ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/385514719

Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядк….

Book · November 2024

CITATIONS
0

READS
167

11 authors, including:



Iryna Basysta
King's Danylo University
44 PUBLICATIONS **15** CITATIONS
SEE PROFILE



Alina Hutnyk
17 PUBLICATIONS **0** CITATIONS
SEE PROFILE

All content following this page was uploaded by Alina Hutnyk on 04 November 2024.

The user has requested enhancement of the downloaded file.

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ (ПРОТОКОЛ БЕРКЛІ)

НАУКОВО-ПРАКТИЧНИЙ ПОРАДНИК



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ (ПРОТОКОЛ БЕРКЛІ)

Науково-практичний порадник

За загальною редакцією доктора юридичних наук, професора, заслуженого юриста України М. С. Цуцкіридзе

Київ – 2024

УДК 343.14:343.3/.4
В43

Рекомендовано до друку рішенням Вченої ради
Державного науково-дослідного інституту
МВС України (протокол № 5 від 23 липня 2024 р.)

Авторський колектив:

Гаврилюк Л. В., кандидат юридичних наук, старший дослідник (передмова; підрозд. 5.1.1, 5.2.2, 5.2.2.1 (у співав.), 5.2.2.2, 5.2.2.3 (у співав.), глосарій, додаток), (ДНДІ МВС України); **Басиста І. В.,** доктор юридичних наук, професор (передмова, розд. 1-4 (у співав.), підрозд. 5.3 (у співав.), глосарій), (ЛьвДУВС); **Афонін Д. С.,** кандидат юридичних наук, доцент (підрозд. 5.1.2), (ОДУВС); **Шевчишен А. В.,** доктор юридичних наук, професор, заслужений юрист України (підрозд. 4.2, 4.3 (у співав.)), (ГСУ НПУ); **Хитра А. Я.,** кандидат юридичних наук, доцент (розд. 1–4 (у співав.)), (ЛьвДУВС); **Лісніченко Д. В.,** кандидат юридичних наук, доцент (підрозд. 5.1.3), (ОДУВС); **Гутник А. В.,** доктор філософії у галузі права (розд. 1–4 (у співав.), глосарій), (ЛьвДУВС); **Биков І. О.,** кандидат юридичних наук (підрозд. 5.2.1, 5.2.2.1 (у співав.)), (ОДУВС); **Бурлака В. В.,** кандидат юридичних наук (підрозд. 5.2.2.3 (у співав.), додаток), (ГСУ НПУ); **Дрозд В. Г.,** доктор юридичних наук, професор, заслужений юрист України (підрозд. 5.3 (у співав.)), (ДЗДГ НПУ); **Корнійко С. М.,** кандидат юридичних наук (підрозд. 5.2.2, 5.2.2.1 (у співав.)), (ДНДІ МВС України); **Пелехатий В. Т.** (підрозд. 5.2.2.3 (у співав.), додаток), (ГСУ НПУ)

Рецензенти:

Капліна О. В. – завідувач кафедри кримінального процесу Національного юридичного університету ім. Я. Мудрого, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України

Топчій В. В. – директор навчально-наукового Інституту права Державного податкового університету, доктор юридичних наук, професор, заслужений юрист України

Тітко І. А. – завідувач кафедри кримінального права та кримінально-правових дисциплін Полтавського юридичного інституту Національного юридичного університету ім. Я. Мудрого, доктор юридичних наук, професор

В43 **Використання** електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкіридзе. – Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. – 196 с.

ISBN 978-966-990-133-0

Розкрито сутність цифрової інформації з відкритих джерел. Визначено порядок збирання цифрових матеріалів з відкритих джерел, порядок огляду вебсторінки, на якій вони розміщені, а також особливості роботи з цифровими матеріалами з відкритих джерел.

Для використання слідчими, дізнавачами, прокурорами, працівниками суду та іншими зацікавленими особами у збиранні та використанні цифрових матеріалів з відкритих джерел мережі «Інтернет» з метою протидії злочинам проти миру, безпеки людства та міжнародного правопорядку та іншим видам злочинів. Може бути корисний для науковців, викладачів, аспірантів, студентів закладів вищої освіти, а також для тих, хто цікавиться питаннями збирання та використання електронних доказів у кримінальному провадженні.

УДК 343.14:343.3/.4

ISBN 978-966-990-133-0

© Державний науково-дослідний інститут МВС України,
Львівський державний університет внутрішніх справ,
Одеський державний університет внутрішніх справ,
Головне слідче управління Національної поліції України, 2024

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
STATE RESEARCH INSTITUTE
LVIV STATE UNIVERSITY OF INTERNAL AFFAIRS
ODESA STATE UNIVERSITY OF INTERNAL AFFAIRS
CENTRAL INVESTIGATION DEPARTMENT
OF THE NATIONAL POLICE OF UKRAINE

USE OF ELECTRONIC EVIDENCE DURING THE PRE-TRIAL INVESTIGATION OF CRIMES AGAINST PEACE, HUMAN SECURITY AND INTERNATIONAL LEGAL ORDER (THE BERKELEY PROTOCOL)

Scientific-and-practical guidelines

Under the general editorship of Doctor of Legal Sciences, Professor, Honoured Lawyer of Ukraine M. S. Tsutskiridze

Kyiv – 2024

UDC 343.14:343.3/.4
B43

Recommended for publication by the decision of the Academic Board of the State Research and Development Institute of the Ministry of Internal Affairs of Ukraine (Protocol № 5 of July 23, 2024)

Authors:

Havryluk L. V., PhD in Law, senior researcher (Introduction; 5.1.1, 5.2.2, 5.2.2.1 (co-auth.), 5.2.2.2, 5.2.2.3 (co-auth.); Glossary; Appendix), (SRI MIA Ukraine); **Basysta I. V.,** D.J.S., professor (Introduction; Sections 1-4 (co-auth.); 5.3 (co-auth.); Glossary), (LvSUIA); **Afonin D. S.,** PhD in Law, associate professor (5.1.2), (OSUIA); **Shevchyshen A. V.,** D.J.S., professor, Honored Lawyer of Ukraine (4.2–4.3 (co-auth.)), (MID NPU); **Khytra A. Ya.,** PhD in Law, associate professor (Sections 1–4 (co-auth.)), (LvSUIA); **Lisnichenko D. V.,** PhD in Law, associate professor (5.1.3), (OSUIA); **Hutnyk A. V.,** PhD in Law (Sections 1–4 (co-auth.); Glossary), (LvSUIA); **Bykov I. O.,** PhD in Law (5.2.1; 5.2.2.1 (co-auth.)), (OSUIA); **Burlaka V. V.,** PhD in Law (5.2.2.3 (co-auth.); Appendix), (MID NPU); **Drozd V. G.,** D.J.S., professor, Honored Lawyer of Ukraine(5.3 (co-auth.)), (DEAH NPU); **Korniiko S. M.,** PhD in Law (5.2.2, 5.2.2.1 (co-auth.)), (SRI MIA Ukraine); **Pelekhatyi V. T.** (5.2.2.3 (co-auth.); Appendix), (MID NPU)

Reviewers:

Kaplina O. V. – Head of the Department of Criminal Procedure of Yaroslav Mudryi National University of Law, D.J.S., Corresponding Member of the National Academy of Legal Sciences of Ukraine

Topchii V. V. – Director of the Educational and Scientific Institute of Law of the State Tax University, D.J.S., Professor, an Honored Lawyer of Ukraine

Titko I. A. – Head of the Department of Criminal Law and Criminal Law disciplines of Poltava Law Institute Yarosav Mydryi National Law University, D.J.S., professor

B43 Use of Electronic Evidence during the Pre-Trial Investigation of Crimes Against Peace, Human Security and International Legal Order (The Berkeley Protocol) : Scientific-and-practical guidelines / L. V. Havryluk, I. V. Basysta, D. S. Afonin, A. V. Shevchyshen et al. ; under the general editorship of M. S. Tsutskiridze. – Kyiv : State Research Institute Ministry of Internal Affairs of Ukraine, Publishing House "Polytechnica", 2024. – 196 p.

ISBN 978-966-990-133-0

The book outlines the essence of digital information from open sources. The procedure for collecting digital materials from open sources, the methods for viewing the web page on which they are uploaded, as well as specificity of dealing with digital materials from open sources are defined.

The scientific and practical guidelines are intended for the use by investigators, prosecutors, court officials and other persons interested in the collection and application of digital materials from the Internet open sources to counter crimes against peace, human security, international legal order and other types of crimes. The book can also be of use to scientists, lecturers, postgraduate students, and students of higher education institutions, as well as to those who are interested in the issues of collecting and using electronic evidence in criminal proceedings.

UDC 343.14:343.3/.4

ISBN 978-966-990-133-0

© State Research and Development Institute of the Ministry of the Interior of Ukraine, Lviv State University of Internal Affairs, Odesa State University of Internal Affairs, Central Investigation Department of the National Police of Ukraine, 2024

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ І ПОЗНАЧЕННЯ 11

ПЕРЕДМОВА 13

РОЗДІЛ 1
КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ 14

1.1. Характеристика понять «цифровість», «цифрові дані і відомості» та «цифрова інформація». Передавання цифрових сигналів 14
1.2. Цифрова інформація та цифрові докази: ознаки, поняття та відмінності 16
1.3. Сутність «відкритих джерел мережі «Інтернет» та «інформації з відкритих джерел мережі «Інтернет». Види відкритих джерел цифрової інформації 19
1.4. Кримінальні процесуальні основи та механізми «роботи» з відкритими джерелами цифрової інформації. Типові помилки в їх обранні 31

РОЗДІЛ 2
ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ 35

2.1. Поняття кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку. Проблеми кваліфікації та кримінальної відповідальності, застосовність давності 35
2.2. Значення інформації у відкритому доступі мережі «Інтернет» для міжнародних та національних розслідувань. Дотримання вимог міжнародного публічного права. Мінімальні стандарти безпеки за Протоколом Берклі 39
2.3. Проблемні питання, які виникають під час розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (визначення підслідності, застосування особливого порядку in absentia тощо). Рекомендації щодо їх вирішення 41

2.4. Заочне судочинство у міжнародному праві
та у процесуальному праві інших країн 57
2.5. Потенційні порушення, які можуть бути допущені у перебігу
«роботи» з відкритими джерелами. Заходи на їх випередження....59

РОЗДІЛ 3
ЦИФРОВІ ВІДОМОСТІ У ДОКАЗУВАННІ: РІШЕННЯ ЄСПЛ, МКС ТА НАЦІОНАЛЬНИХ СУДІВ 69

3.1. Практика ЄСПЛ щодо використання цифрових даних
з відкритих джерел як доказу у кримінальному провадженні... 69
3.2. Наявні підходи у рішеннях міжнародних кримінальних
трибуналів та Міжнародного кримінального суду 72
3.3. Оцінка національними суддями цифрових
даних у сукупності з іншими доказами.....74

РОЗДІЛ 4
СТАНДАРТИ ЦИФРОВИХ ДОКАЗІВ З ВІДКРИТИХ ДЖЕРЕЛ 76

4.1. Вимоги чинного КПК та правова позиція об'єднаної палати
Касаційного кримінального суду Верховного Суду щодо
такого різновиду доказів (кримінальні процесуальні умови
набуття інформацією з відкритих джерел статусу доказу;
недопустимість ототожнення електронного доказу як засобу
доказування та матеріального носія тощо) 76
4.2. Алгоритм аналізу відомостей, які отримані у перебігу
опрацювання цифрової інформації у відкритому доступі
з відкритих джерел.....81
4.3. Стандарти цифрових доказів з відкритих джерел
за Протоколом Берклі 82

РОЗДІЛ 5
ПОШУК, ЗБИРАННЯ ТА ВИКОРИСТАННЯ ЦИФРОВИХ МАТЕРІАЛІВ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ 84

5.1. Підготовка до пошуку, огляду та фіксації цифрових матеріалів
з відкритих джерел у мережі «Інтернет».....84

5.1.1. Процесуальні та організаційно-тактичні основи підготовки до пошуку, огляду та фіксації цифрових матеріалів з відкритих джерел у мережі «Інтернет» 84
5.1.2. Технічне та техніко-криміналістичне забезпечення роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет» 95
5.1.3. Основи безпеки роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет» (тактичні й технічні аспекти) 101

5.2. Пошук, аналіз, виявлення, фіксація та збирання цифрових матеріалів з відкритих джерел у мережі «Інтернет» та їх використання 114

5.2.1. Особливості пошуку, аналізу та виявлення цифрових матеріалів з відкритих джерел у мережі «Інтернет» 114
5.2.2. Процесуальні, тактичні та технічні основи збирання цифрових матеріалів з відкритих джерел у мережі «Інтернет» .. 129

5.2.2.1. Збереження цифрових матеріалів з відкритих джерел у мережі «Інтернет» 131
5.2.2.2. Порядок огляду, фіксації цифрових матеріалів з відкритих Джерел 139
5.2.2.3. Відображення послідовності дій, фіксування інформації, яка міститься в оглянутих цифрових матеріалах з відкритих джерел мережі «Інтернет» 143

5.3. Аналіз, перевірка та оцінка інформації, отриманої із відкритих джерел, під час розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку 151

***СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ* 156**

ГЛОСАРІЙ 178

Додаток. БЛАНК ПРОТОКОЛУ ОГЛЯДУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ МЕРЕЖІ «ІНТЕРНЕТ» 190

CONTENTS

LIST OF CONVENTIONAL ABBREVIATIONS 11

INTRODUCTION 13

CHAPTER 1
CONCEPTUAL APPROACHES TO THE USE OF
DIGITAL INFORMATION FROM OPEN SOURCES 14

1.1. Characteristics of the concepts “digital”, “digital data and information” and “digital information”. Transmission of digital signals 14
1.2. Digital information and digital evidence: features, concepts and differences 16
1.3. The essence of “the Internet open sources” and “information from the Internet open sources”. Types of open sources of digital information 19
1.4. Criminal procedural bases and mechanisms of the “activity” with open sources of digital information. Typical mistakes in their selection 31

CHAPTER 2
USE OF DIGITAL INFORMATION FROM OPEN
SOURCES DURING A CRIMINAL INVESTIGATION OF
OFFENSES AGAINST PEACE, HUMAN SECURITY AND
INTERNATIONAL LEGAL ORDER 35

2.1. The concept of criminal offenses against peace and security, humanity and international legal order. Qualification and criminal liability problems, the applicability of the limitation of action 35
2.2. The value of information in the Internet open access for international and national investigations. International public law compliance Minimum safety standards for The Berkeley Protocol.....39
2.3. Problematic issues that arise during the investigation of crimes against peace, human and international security legal order (determination of investigative jurisdiction, special order in absentia’s application, etc.). Recommendations for their solution 41

2.4. Absentee proceeding in the international law and other countries 57
2.5. Potential violations that may happen in the course "dealing" with open sources. Measures for their prevention 59

CHAPTER 3
DIGITAL INFORMATION IN EVIDENCE: ECHR, ICC AND NATIONAL COURTS' FINDINGS..... 69

3.1. The ECHR's practice regarding the use of digital data from open sources as evidence in criminal proceedings 69
3.2. Existing approaches in findings of international criminal tribunals and the ICC.....72
3.3. Evaluation of digital data by national judges in combination with other evidence 74

CHAPTER 4
OPEN SOURCE DIGITAL EVIDENCE STANDARDS 76

4.1. The requirements of the current CPC and the joint chamber of the Criminal Court of Cassation of the Supreme Court's Cassational Criminal Court's legal position regarding such types of evidence (criminal procedural conditions of acquisition of the status of evidence by information from open sources; inadmissibility of electronic evidence's identification as a means of proof and material carrier, etc.) 76
4.2. Algorithm of the analysis of information obtained during processing digital information in public access from open sources ..81
4.3. Standards for digital evidence from open sources under the Berkeley Protocol.....82

CHAPTER 5
SEARCH, COLLECTION AND USE OF DIGITAL OPEN-SOURCE MATERIALS DURING PRE-TRIAL, INVESTIGATION OF CRIMES AGAINST PEACE, SECURITY OF HUMANITY AND INTERNATIONAL LEGAL ORDER..... 84

5.1. Preparation for search, review, and recording of digital materials from the Internet open sources 84

5.1.1. Procedural and organizational-tactical foundations of preparation for search, review, and recording of digital materials from the Internet networks' open sources 84
5.1.2. Technical and technical forensic support for activity with digital materials from the Internet open sources 95
5.1.3. Basics of security of dealing with digital materials from the Internet open sources (tactical and technical aspects) ... 101
5.2. Search, analysis, detection, recording and evaluation of digital materials from the Internet network's open sources and their further use in proving crimes against peace, human security, and international legal order 114
5.2.1. Features of search, analysis, and detection of digital materials from the Internet open sources 114
5.2.2. Procedural, tactical, and technical foundations of gathering digital materials from the Internet open sources 129
5.2.2.1. Storage of digital materials from the Internet network's open sources 131
5.2.2.2. The procedure for reviewing and recording digital materials from open Sources 139
5.2.2.3 Displaying the sequence of actions, recording information contained in reviewed digital materials from the Internet network's open-source 143
5.3. Analysis, verification, and assessment of information obtained from open sources in the investigation of crimes against peace, human security and international legal order 151

REFERENCES 156

GLOSSARY 178

Appendix. OPEN SOURCE DIGITAL MATERIALS REVIEW'S PROTOCOL 190

УМОВНІ СКОРОЧЕННЯ І ПОЗНАЧЕННЯ

БЕБ	–	Бюро економічної безпеки України
ВРУ	–	Верховна Рада України
ВС	–	Верховний Суд
ГСУ	–	Головне слідче управління Національної поліції України
ГУР МО	–	Головне управління розвідки Міністерства оборони України
ГШ ЗСУ	–	Генеральний штаб Збройних сил України
ДБЖ	–	джерело безперебійного живлення, джерело безперервного живлення (UPS)
ДБР	–	Державне бюро розслідувань
Директива № 2016/680	–	Директива Європейського Парламенту та Ради ЄС про захист фізичних осіб щодо обробки їх персональних даних компетентними органами в цілях попередження, розслідування, виявлення та переслідування кримінальних правопорушень чи виконання кримінальних покарань, а також вільної передачі таких даних, № 2016/680 від 27.04.2016 р.
ДПСУ	–	Державна прикордонна служба України
ЄСПЛ	–	Європейський суд з прав людини
ЖК	–	Женевські конвенції
КК України	–	Кримінальний кодекс України
КПК України	–	Кримінальний процесуальний кодекс України
МВС України	–	Міністерство внутрішніх справ України
МКС	–	Міжнародний кримінальний суд
НАБУ	–	Національне антикорупційне бюро України
ОГП	–	Офіс Генерального прокурора
ООН	–	Організація Об’єднаних Націй
ОП	–	Офіс Президента України
ПК	–	персональний комп’ютер
ППВСУ	–	Постанова Пленуму Верховного Суду України
Протокол Берклі	–	Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової

		інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права
СБУ	–	Служба безпеки України
СРД	–	слідчі (розшукові) дії
США	–	Сполучені Штати Америки
ФРН	–	Федеративна республіка Німеччина
ЦК України	–	Цивільний кодекс України
ШІ	–	штучний інтелект
DSLR (Digital Single Lens Reflex Cameras)	–	цифрові дзеркальні фотоапарати
GDPR	–	Регламент Європейського Парламенту і Ради ЄС про фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, № 2016/679 від 27.04.2016 р.
in absentia	–	кримінальне провадження за відсутності підозрюваного або обвинуваченого
OSINT (Open source intelligence)	–	пошук та аналіз інформації з відкритих джерел
RAM	–	оперативна пам'ять комп'ютера
UPS (Uninterruptible Power Supply)	–	джерело безперебійного живлення, джерело безперервного живлення (ДБЖ)
рф	–	російська федерація
Ⓑ	–	цитата з Протоколу Берклі

ПЕРЕДМОВА

Інформація з відкритих джерел на сьогодні займає вагоме місце у процесі розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку. Робота з цифровими матеріалами потребує спеціальних знань, тому для слідчих робота з такою інформацією під час досудового розслідування є своєрідним викликом, що обумовлено відсутністю універсальних стандартів, як вітчизняних, так і міжнародних, щодо збирання та використання цифрових матеріалів з відкритих джерел як доказів у кримінальному провадженні. Мінімальні стандарти для пошуку, збирання, зберігання, перевірки та аналізу таких матеріалів окреслено у Протоколі Берклі, який на сьогодні є практичним посібником з ведення розслідування з використанням відкритих цифрових даних. У Протоколі Берклі визначено особливості пошуку, збирання цифрового матеріалу з відкритих джерел, а також властивості цифрового елемента, які потрібно належним чином захищати й зберігати протягом певного часу, що дасть можливість їх використовувати як докази у кримінальному провадженні й вітчизняними судами, і Міжнародним кримінальним судом та підвищує ймовірність визнання їх допустимими.

Водночас застосування слідчими положень цього протоколу під час роботи з цифровими матеріалами з відкритих джерел має узгоджуватися з нормами національного законодавства. Лише за таких умов зможемо говорити про наявне підґрунтя для належного документування тяжких міжнародних злочинів і можливість притягнення причетних осіб до відповідальності.

Підготовка науково-практичного порадника обумовлена потребами слідчої діяльності щодо належного документування злочинів проти миру, безпеки людства та міжнародного правопорядку, а також необхідністю вироблення універсального підходу зі збирання та використання цифрових матеріалів з відкритих джерел мережі «Інтернет» під час досудового розслідування таких протиправних дій. Саме на вирішення цих проблемних питань він і спрямований.

Науково-практичний порадник є прикладним кроком на шляху до формування концепції інформації з відкритих джерел. Призначений для використання слідчими, дізнавачами, прокурорами, працівниками суду та іншими особами, які цікавляться питаннями збирання та використання цифрових матеріалів з відкритих джерел мережі «Інтернет» у кримінальному провадженні.

РОЗДІЛ 1. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

Використання цифрової інформації у кримінальному процесуальному доказуванні має низку проблем, зокрема, немає уніфікованого підходу законодавця до вживаної термінології, і як наслідок – терміновжиток різний.

1.1. Характеристика понять «цифровість», «цифрові дані і відомості» та «цифрова інформація». Передавання цифрових сигналів

Чому у професійному вжитку оптимальним є використання таких термінів, як «цифровість», «цифрові дані і відомості» та «цифрова інформація», коли йдеться про відкриті джерела?

У чинному КПК України законодавець не виділяє такого різновиду доказів, як «електронні». При цьому у ЦПК України йде мова про «електронні докази», «електронні документи та документообіг»[1] тощо, а його ст. 100 містить вказівку, що варто розуміти під таким різновидом доказів, який порядок їх подання та як засвідчити «електронні копії електронного доказу»[2]. Українські науковці також вживають термін «електронні докази» на позначення подібного їх різновиду за умов чинного КПК[3; 4; 5; 6; 7]. Нині поняття «електронні» й «цифрові» вживають як синоніми[8]. Судді Верховного Суду допускають вживання

---

[1] Цивільний процесуальний кодекс України. Закон від 18.03.2004. 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11

[2] Там само.

[3] Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні: дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 648 с.

[4] Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні: автореф. дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 42 с.
URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/auto/20/3.pdf

[5] Столітній А. В. Електронне кримінальне провадження: передумови виникнення, сучасний стан та перспективи розвитку: монографія. Київ: Вид. дім «АртЕк», 2016. 724 с.

[6] Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

[7] Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. Львів: ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725

[8] Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісн. ХНУВС–Bulletin of KhNUIA*. 2023. № 3 (102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43

обох термінів[9], хоча окремі представники Феміди оперують виключно поняттям «цифрові докази»[10], а судові рішення різних інстанцій рясніють обома видами терміновживання, хоча у переважній більшості йдеться про електронний доказ у розумінні електронного документа. І хоча такий підхід до вживання термінів не є коректним, все ж він логічно слідує із недосконалих положень чинного КПК України.

Радимо виокремлювати саме **цифрові докази**, **цифрові відомості**, **цифрову інформацію**, що отримана з відкритих джерел. Такий терміновжиток є цілком прийнятним за чинного КПК України та інших національних, чинних у цій сфері нормативно-правових актів: у національному стандарті України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»[11] йдеться саме про цифрові докази; термін зі словом «цифровий» вжито у листі-орієнтуванні Офіса Генерального прокурора щодо збереження цифрової інформації з відкритих джерел від 28 серпня 2021 року[12]). Дороговказом також маємо український неофіційний переклад Протоколу Берклі з ведення розслідування з використанням відкритих цифрових даних[13].

З огляду на зазначене варто розуміти, що «цифрова інформація» існує в «електронно-цифровому» середовищі[14; 15], для її відтворення потрібні апаратні й програмні умови[16], а «через певний проміжок часу

---

[9] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний суд:* вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

[10] Там само.

[11] ДСТУ ISO/IEC 27037:2017. «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». Вид. офіц. Київ: УкрНДНЦ, 2018. VI. 31 с.

[12] Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел: лист-орієнтування Офіса Генерального прокурора від 28.08.2021 № 18/1-386 вих. – 515окв – 21.

[13] Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

[14] Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. С. 36.

[15] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 74–75, 94.

[16] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 94–97.

можуть з'явитися як нові види пристроїв, так і нові типи запису інформації»[17].

Як здійснюється передавання цифрових сигналів? Що таке «носії» та «накопичувачі»?

Для позначення технічних засобів, що призначені для передавання цифрових сигналів у часі й просторі, доцільно застосовувати такий перелік: машинні носії, накопичувачі цифрових даних, носії для збереження цифрових даних, носії цифрових даних[18].

Наприклад, якщо аналізувати публікацію у Телеграм-каналі – фото українських військових у полоні та допис до нього, – то цифрова інформація слідує як із тексту, так і з фото – зовнішні риси військових, формений одяг, знаки розрізнення, приміщення та інші деталі; носієм такої цифрової інформації у цьому випадку буде текст та фотографія, накопичувачем – сервер месенджера (така цифрова інформація поки ще не є доказом у кримінальному провадженні).

Носієм цифрової інформації також може бути **файл**,
а накопичувачем – **машинний носій**[19].

1.2. Цифрова інформація та цифрові докази: ознаки, поняття та відмінності

Якими є характеристики й ознаки цифрової інформації?

Цифрова інформація існує в «електронно-цифровому» середовищі та не завжди набуде характеру, статусу й ознак доказу у кримінальному провадженні. **Вона характеризується** наявністю метаданих (англ. «дані про дані»), її створюють разом із кожним файлом: 1) автоматично програма або 2) автор цифрової інформації[20; 21]. Не абсолютно притаманною їй є ознака позбавлення суб'єктивності[22], адже авторство належить

[17] Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісн. ХНУВС–Bulletin of KhNUIA*. 2023. № 3 (102). С. 209–210. DOI: https://doi.org/10.32631/v.2023.3.43

[18] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 84–85; 86; 88; 98.

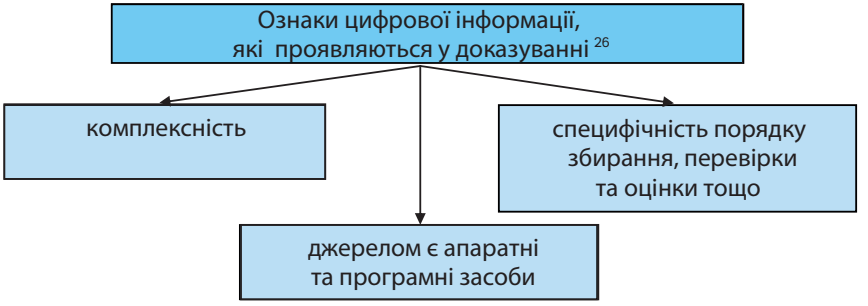
[19] Там само. С. 84–86.

[20] Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. С. 36.

[21] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 74–75, 94.

[22] Там само. С. 74–75, 94.

людині[23; 24]. **Іншими ознаками є такі:** можливість існування у статичній та динамічній формах; закодованість (через що є потреба у перетворенні у таку форму, яка може бути сприйнята людиною); мобільність; тиражованість; «невловимий характер інформації» та легкість внесення змін або знищення. Для відтворення цифрової інформації потрібні апаратні і програмні умови[25].



Чому на етапі збирання відомостей із відкритих джерел слід оперувати такими категоріями, як «цифрова інформація», а не «цифрові докази»?

Відмінності між **цифровою інформацією** та **цифровими доказами** пояснені у Протоколі Берклі (підкреслено, що термін «докази» слід відрізняти від «інформації»[27]).

Цифрова інформація, що отримана з відкритих джерел (цифрова інформація у відкритому доступі) – інформація, що є у відкритому доступі в Інтернеті, до якої можна отримати доступ, наприклад, на загальнодоступних вебсайтах, в Інтернет-базах даних або на платформах соціальних медіа[28].

---

[23] Басиста І. В., Удовенко Ж. В., Кулинич М.-М. А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Наук. вісн. Ужгород. нац. ун-ту*. Сер. ПРАВО. 2024. Вип. 80. Ч. 3. С. 19–38. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf

[24] Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості*: матеріали кругл. столу. 15 берез. 2024. Львів: ЛьвДУВС, 2024.

[25] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 94–97.

[26] Там само. С. 99–101.

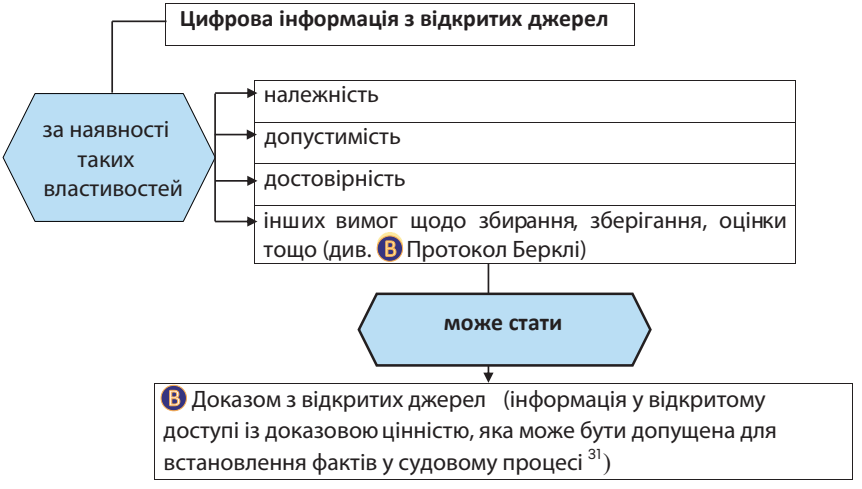
[27] Протокол Берклі ... . С. 27.

[28] Там само. С. 25, 27.

Також у Ⓑ Протоколі Берклі як синонім до поняття «цифрова інформація у відкритому доступі» вжито й такі терміни: «онлайн-контент», «онлайн-матеріал» або «онлайн-дані»[29].

Важливо не зловживати терміном «докази», посилаючись на інформацію взагалі, зокрема й із відкритих джерел. Ⓑ Докази зазвичай визначаються як доказ факту(ів), який використо вується під час розслідування і/або подається на судовому слуханні[30].

Переконані у необхідності оперувати терміном «цифрова інформація з відкритих джерел» щодо якої існує ймовірність набуття статусу цифро вого доказу.



Отож, якщо говоримо про **цифровий доказ** (digital evidence), то йдеться про відомості, факти чи обставини (фактичні дані)[32], що отримані у передбаченому КПК України порядку, збережені (передані) в бінарному вигляді, на які можна (оскільки вони відповідають таким властивостям, як належність, допустимість, достовірність) посилатися як на докази.

[29] Там само. С. 25.
[30] Там само. С. 27.
[31] Там само. С. 27.
[32] Кримінальний процес України: Академічний курс. У 3 т. Т. 1: Загальна частина / В. Т. Нор, Н. Р. Бобечко, М. В. Багрій та ін.; за ред. акад. НАПрН України, д-ра юрид. наук, проф. В. Т. Нора та д-ра юрид. наук, проф. Н. Р. Бобечка. Львів: ЛНУ ім. Івана Франка, 2021. С. 417.

1.3. Сутність «відкритих джерел мережі «Інтернет» та «інформації з відкритих джерел мережі «Інтернет». Види відкритих джерел цифрової інформації

Є проблема з різним розумінням поняття «відкриті джерела» та переліком відкритих джерел. Частково таку прогалину усуває підхід, пропонований у Ⓑ Протоколі Берклі[33].

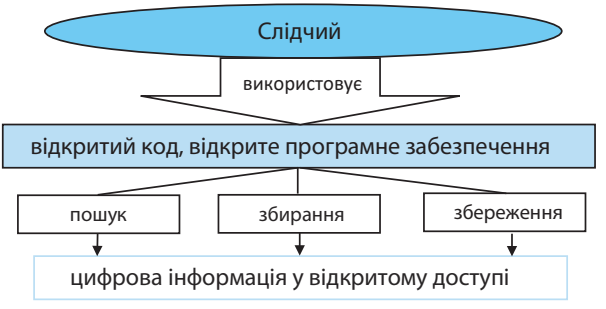
Що таке відкриті джерела цифрової інформації («відкриті джерела мережі «Інтернет»)?

Відкриті джерела цифрової інформації – це медіа, соціальні медіа, вебсайти, геопросторові платформи, бази даних, офіційні дані та інші платформи, на яких можна спостерігати, купувати або запитувати загальнодоступну інформацію[34].

Які «інструменти» для пошуку, збирання та збереження цифрової інформації у відкритому доступі пропонує Протокол Берклі?

У Ⓑ Протоколі Берклі зазначено про **відкритий код, відкрите програмне забезпечення** як дозволені «інструменти» для пошуку, збирання, збереження цифрової інформації у відкритому доступі[35].

Радимо алгоритм роботи слідчого з цифровою інформацією з відкритих джерел, виходячи із наведеного вище.



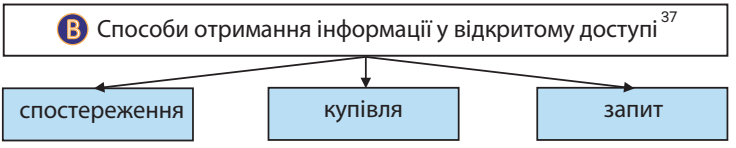
[33] Протокол Берклі … .

[34] Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час досудового розслідування кримінальних правопорушень: окремі аспекти. *Наук. вісн. Ун-ту Короля Данила.* Вип. 17 (29), 2024. С. 227–243.

[35] Протокол Берклі … . С. 25, 27.

Відкритий код, відкрите програмне забезпечення – побудоване з вихідного коду, який кожний, хто має доступ, може перевірити, змінити чи покращити. Код не бачать користувачі, але він підпадає під вказані маніпуляції, які може виконати програміст. На відкрите програмне забезпечення не поширюються авторські права, патенти чи інші юридичні засоби контролю[36].

Які способи отримання інформації у відкритому доступі передбачені у Протоколі Берклі?



Розвідка за відкритими джерелами не виконує функції збору інформації, пов'язаної із процесами розслідування, встановлення елементів різних злочинів[38].

Звісно, що розвідка за відкритими джерелами може бути застосовною для вирішення питання про вжиття заходів забезпечення безпеки (захисту свідків) та як довідкова інформація для прийняття рішень тощо.

Хоча автори й розглядають «розвідку» дещо спрощено, зокрема як «інформацію, яку можна зрозуміти та яка була оцінена у контексті її джерела та надійності»[39], наділяючи OSINT, на відміну від інших розвідок (як от HUMINT, SIGINT, IMINT або PHOTINT чи GEOINT, MASINT[40] тощо), придатністю використання її інструментарію для розслідування злочинів, зокрема й воєнних[41], все ж маємо певні власні аргументи з огляду саме на такий спрощений і буквальний авторський підхід.

Сучасна практика розслідувань використовує методику OSINT для відшукання прихованих активів, таких, що мали б бути обкладені,

---

[36] Там само. С. 25, 27.
[37] Там само. С. 25–26.
[38] Там само. С. 26.
[39] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса: Вид-во «Юридика», 2024. С. 7.
[40] Там само. С. 8–9.
[41] Там само. С. 164–173.

приміром, санкціями тощо. Поділяємо й підхід про придатність інструментарію OSINT для виявлення порушень у різних сферах, про що автори детально зазначають у матеріалах або публікаціях[42]. Є й протилежна мета використання – «…кіберзлочинці з публічних даних складають портрет потенційної жертви»[43].

У рішеннях суддів також згадується OSINT – в них методи названо «аналітичним дослідженням» чи «пошуком» («…було проведено аналітичне дослідження відкритих джерел інформації методами OSINT», див. ухвала слідчого судді Комунарського районного суду міста Запоріжжя від 01.06.2022 у справі № 333/1938/22. https://reyestr.court.gov.ua/Review/104556752;



Ухвала Комунарського районного суду м. Запоріжжя

«…у зв'язку з чим, було здійснено пошук на основі відкритих джерел (OSINT)», див. ухвала слідчого судді Святошинського районного суду м. Києва від 31.07.2019 у справі № 759/13808/19. https://reyestr.court.gov.ua/Review/83480188 тощо).



Ухвала Святошинського районного суду м. Києва

Автори теж аналізують ці та інші рішення, але під дещо іншим, не критичним, кутом зору[44].

Резюмуємо! Маємо власне бачення щодо «режиму» здобутої інформації та способів і шляхів її використання у національних розслідуваннях, з огляду на дотримання вимог до доказів та доказування, як і запобігання порушенням конституційних, процесуальних та конвенційних прав учасників кримінального провадження тощо. Окремі рекомендації наведено у наступних підрозділах.

Очевидно, що результати розвідки повинні оформлюватися належним чином, як от «легалізовуватися» у передбачений законом спосіб як отримані у результаті ОРД матеріали[45].

---

[42] Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. 19.07.2022. *Софтліст:* вебсайт. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/; OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса: Вид-во «Юридика», 2024. 180 с.

[43] Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. 19.07.2022. *Софтліст:* вебсайт. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/

[44] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса: Вид-во «Юридика», 2024. 180 с.

[45] Схожий умовивід також сформулював й у перебігу власної презентації д-р юрид. наук О. О. Торбас під час VI Харківського кримінального процесуального полілогу на тему «КРИМІНАЛЬНИЙ ПРОЦЕС: СУЧАСНИЙ ВИМІР ТА ПРОСПЕКТИВНІ ТЕНДЕНЦІЇ», 17 квіт. 2024 р.

Важливо! Цитата у Протоколі Берклі, у котрій йдеться, що «…розвідка за відкритими джерелами є підмножиною тієї інформації, яка «збирається, використовується та поширюється своєчасно серед відповідної аудиторії з метою задоволення конкретних вимог до розвідки»[46], судячи зі шпальт наявного неофіційного перекладу Протоколу та його викладу англійською мовою[47], взята авторами Протоколу зі с. 8. Директиви про розвідувальну спільноту № 301, 11 липня 2006 р.[48] (про це значиться у присторінковій виносці № 15 Протоколу. Також див. оригінал Протоколу – «15. National Open Source Enterprise, Intelligence Community Directive. No. 301, 11 July 2006, p. 8 (footnote omitted)»[49]). Упродовж ознайомлення зі згаданою Директивою № 301 стало очевидно, що, крім наявних глобальних сформованих підходів щодо отриманої із відкритих джерел цифрової інформації, яка збирається, використовуються та поширюються, відповідно, й правила поводження з нею[50]. Також маємо й неоднаковий у різні часові періоди підхід МКС, про який йтиметься згодом у відповідному підрозділі.

Які є види відкритих джерел цифрової інформації та яку інформацію з них можна використовувати у кримінальному провадженні?

Акумулювавши перелік відкритих джерел, який пропонується у Протоколі Берклі[51], публікаціях дослідників[52; 53], врахувавши особливості кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку, пропонуємо такі види відкритих джерел цифрової інформації.

---

[46] Протокол Берклі ... . С. 26.

[47] Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

[48] INTELIGENCE COMMUNITY DIRECTIVE NUMBER 301. NATIONAL OPEN SOURCE ENTERPRISE. ‘‘‘EFFECTIVE: JULY 11, 2006. URL: https://irp.fas.org/dni/icd/icd-301.pdf

[49] Berkeley Protocol on Digital Open Source Investigations … .

[50] Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час досудового розслідування кримінальних правопорушень: окремі аспекти. *Наук. вісн. Ун-ту Короля Данила*. Вип. 17 (29). 2024. С. 227–243.

[51] Протокол Берклі … . С. 20, 25 та ін.

[52] Gill R. What is Open-Source Intelligence? 23.02.2023.

URL: https://www.sans.org/blog/what-is-open-source-intelligence/; Open-source intelligence. 02.05.2022. European Union. URL: https://data.europa.eu/en/publications/datastories/open-source-intelligence

[53] Кваліфікація та розслідування порушення законів і звичаїв війни: наук.-практ. посіб. / А. А. Вознюк, І. В. Жук, О. В. Таран, С. С. Чернявський та ін.; за заг. ред. М. С. Цуцкірідзе, В. В. Чернея, А. А. Вознюка. Київ: Норма права, 2023. С. 195.

Види відкритих джерел цифрової інформації

МЕДІА	
Матеріали (стаття, фоторепортаж, відео, аудіо), які створені чи отримані *під час журналістської діяльності*. Журналістські проєкти, спрямовані на розслідування злочинів під час російсько-української війни. Можуть бути опубліковані на вебсайтах, у «*Telegram*», «*Youtube*», «*Twitter*», «*Facebook*», «*Instagram*».	
Журналістські проєкти, які розслідують факти депортації дітей з окупованих територій, знищення об'єктів критичної інфраструктури, факти екоциду, вивезення культурних цінностей, фіксують випадки катування та вбивства цивільного населення та ідентифікують російських військових і їх командирів.	
Global Investigative Journalism Network[54]	
Bihus.Info[55]	
Слідство.Інфо[56]	
Схеми[57]	

СОЦІАЛЬНІ МЕДІА	
Платформи, створені для комунікації між користу вачами, які включають обмін повідомленнями, зображеннями, фото, відео, аудіо та іншими творами.	
Різновиди соцмедіа[58]	**Приклади**
Блоги	«*LiveJournal*», «*Blogger*» та ін.

[54] Global Investigative Journalism Network. URL: https://gijn.org/ua/
[55] Bihus.Info. URL: https://bihus.info/
[56] Слідство.Інфо. URL: https://www.slidstvo.info/
[57] Схеми. URL: https://www.radiosvoboda.org/skhemy
[58] Chauhan S., Panda N. K. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Elsevier Science & Technology Books, 2015. P. 31.

СОЦІАЛЬНІ МЕДІА		
Соціальні мережі	*«Telegram», «Youtube», «Twitter», «Facebook», «Instagram»; у т.ч. заборонені в Україні «Вконтакте», «Одноклассники»* та ін.	
	Телеграм-канали для пошуку інформації про громадян рф[59]	
	DataLeakBot[60]	
	CyberSec's Bot[61]	
	Глаз Бога[62]	
	OSINTFLOW bot[63]	
	Телеграм-канали ворога	
	Герои спецоперации Z[64]	
	СОЛДАТСКАЯ ПРАВДА КРП(б)[65]	
Медіаплатформи	*«YouTube», «Skype», «Livestream», «SoundCloud», «Pinterest», «SlideShare»* та ін.	

[59] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 195.
[60] DataLeakBot. *Telegram*: вебсайт. URL: https://telegram.im/@safe_search_bot
[61] CyberSec's Bot. URL: https://t.me/cybersecs
[62] Глаз Бога. *Telegram*: вебсайт. URL: https://telegram.im/@eyegodsbot?lang=ru
[63] OSINTFLOW bot. *Telegram*: вебсайт. URL: https://t.me/osintflow_find_bot
[64] Герои спецоперации Z. *Telegram*: вебсайт. URL: https://t.me/s/heroesofZ
[65] СОЛДАТСКАЯ ПРАВДА КРП(б). *Telegram*: вебсайт. URL: https://t.me/Soldiers_truth

<table>
<tr><td colspan="3">ВЕБСАЙТИ[66]</td></tr>
<tr><td>Інформаційні</td><td colspan="2">Призначені для інформування відвідувачів, поширення новин, тематичні сайти, енциклопедії, словники тощо[67]. Наприклад, Херсонський обласний краєзнавчий музей на своєму сайті публікує зображення та опис викрадених історичних цінностей[68]; чи сайт незалежного експерта з захисту, який проводить огляди безпілотників, човнів, їх озброєння[69].</td></tr>
<tr><td>Бізнес-сайти</td><td colspan="2">Сайти, що містять інформацію про компанії та їхні послуги, здійснюють функцію електронної торгівлі[70]. Наприклад, сайти, які пропонують продаж зброї.</td></tr>
<tr><td rowspan="5">Сайти сервісів</td><td colspan="2">Пошукові сторінки</td></tr>
<tr><td colspan="2">Сайти, які допомагають знайти інформацію в Інтернет-мережі за ключовими словами («Google», «Yandex», «Yahoo» і под.).</td></tr>
<tr><td colspan="2">Вебархіви і цифрові бібліотеки</td></tr>
<tr><td colspan="2">Сховища, в яких зберігаються вебсайти, здійснені у них зміни, видалення інформації у певний час.</td></tr>
<tr><td>«The Internet Archive Wayback Machine»[71]</td><td></td></tr>
<tr><td>Для зберігання інформації про війну в Україні створено «Ukraine War Archive»[72]</td><td></td></tr>
</table>

[66] Поняття, структура та різновиди вебсайтів. Автоматизоване розроблення вебсайтів. URL: http://www.ndu.edu.ua/liceum/web.pdf

[67] Там само.

[68] Цифрова колекція. Викрадена історія. Херсонський обласний краєзнавчий музей. URL: https://hokm.ks.ua/category/czyfrova-kolekcziya/vykradena-istoriya/

[69] Covert Shores: H I Sutton. URL: http://www.hisutton.com/

[70] Поняття, структура та різновиди вебсайтів. Автоматизоване розроблення вебсайтів. URL: http://www.ndu.edu.ua/liceum/web.pdf

[71] The Internet Archive Wayback Machine. URL: https://help.archive.org/

[72] Ukraine War Archive. URL: https://ukrainewararchive.org/

ГЕОПРОСТОРОВІ ПЛАТФОРМИ		
Супутникові знімки	*Google Earth Pro*[73]	
	NASA Earthdata Search[74]	
	USGS Earth Explorer[75]	
Карти	*Google Maps*[76]	
	Wikimapia[77]	
	LiveUAMap[78]	
	Bing Maps[79]	

БАЗИ ДАНИХ		
Державні (адміністратором є державна установа)	*Державний реєстр санкцій*[80]	
	Воєнні злочинці рф (ГУР МО)[81]	

[73] Google Earth Pro. URL: https://www.google.com/intl/ru/earth/about/
[74] NASA Earthdata Search. URL: https://search.earthdata.nasa.gov/search
[75] USGS Earth Explorer. URL: https://earthexplorer.usgs.gov/
[76] Google Maps. URL: https://www.google.com.ua/maps/
[77] Wikimapia. URL: https://wikimapia.org/
[78] LiveUAMap. URL: https://liveuamap.com/uk
[79] Bing Maps. URL: https://www.bing.com/maps
[80] Державний реєстр санкцій. URL: https://drs.nsdc.gov.ua/
[81] Воєнні злочинці рф (ГУР МО). URL: https://gur.gov.ua/content/war-criminals-rf.html

<table>
<tr><th colspan="3">БАЗИ ДАНИХ</th></tr>
<tr><td>Державні
(адміністратором є державна установа)</td><td>Особи, які переховуються від органів влади (МВС)[82]</td><td></td></tr>
<tr><td rowspan="3">Приватні
(адміністраторами є приватні особи чи установи)</td><td>Clarity Project[83]</td><td></td></tr>
<tr><td>Опендатабот[84]</td><td></td></tr>
<tr><td>YouControl[85]</td><td></td></tr>
<tr><td colspan="3">Реєстри, адміністраторами яких є незалежні, недержавні, волонтерські, журналістські організації або ж адміністратор невідомий</td></tr>
<tr><td colspan="2">Центр «Миротворець»[86] – пошук інформації за анкетними даними про зрадників Батьківщини, бойовиків, найманців та терористів, російських військовослужбовців – військових злочинців[87].</td><td></td></tr>
<tr><td colspan="2">Онлайн-реєстр «Російські військові злочинці»[88] (спільний проєкт Антикорупційного штабу та «Слідство.Інфо») – пошук за анкетними даними військових російської армії, ідентифікованих осіб полонених росіян, а також вбитих під час війни в Україні росіян або докази присутності в Україні (у профайлі кожного військового зазначається лінк на доказову базу).</td><td></td></tr>
<tr><td colspan="2">База російських військових, які причетні до вчинення воєнних злочинів «КНИГА КАТІВ УКРАЇНСЬКОГО НАРОДУ»[89] – інформація про воєнних злочинців рф та їхні злочини, можливий пошук осіб за анкетними даними, віком, а також за місцем вчинення злочину[90].</td><td></td></tr>
</table>

[82] Особи, які переховуються від органів влади (МВС). URL: https://wanted.mvs.gov.ua/searchperson/

[83] Clarity Project. URL: https://clarity-project.info/

[84] Опендатабот. URL: https://opendatabot.ua/

[85] YouControl. URL: https://youcontrol.com.ua/

[86] Центр «Миротворець». URL: https://myrotvorets.center/

[87] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 196.

[88] Онлайн-реєстр «Російські військові злочинці» (спільний проєкт Антикорупційного штабу та «Слідство.Інфо»). URL: https://rwc.shtab.net/troopers

[89] База російських військових, які причетні до вчинення воєнних злочинів «КНИГА КАТІВ УКРАЇНСЬКОГО НАРОДУ». URL: https://russian-torturers.com/

[90] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 195.

БАЗИ ДАНИХ	
Вебсайт «ОПРИЧНИКИ»[91] – інформація про російських військових, які беруть участь у війні проти України. Можливий пошук інформації за анкетними даними або ключовими словами[92].	
Реєстри «Вороги України» (проєкт від OSINT-спільноти MOLFAR)[93] – список ведеться за різними категоріями, наприклад «Книга орків», «ФСБ рф», «ФСБ рф: прифронтові області», «ГРУ рф: російські розвідники», «Пілоти російської авіабази «Енгельс». Можливість пошуку інформації про осіб, які брали участь у збройній агресії, а також основні ресурси, які використовують в OSINT-розвідці[94].	
Сайт «Потерь.НЕТ»[95] – інформація про загиблих російських військових в Україні. Можливість пошуку інформації за анкетними даними[96].	
Проєкт «Кто воюет в Украине»[97] – інформація про російські підрозділи та їх керівництво, які беруть участь у збройній агресії. Пошук за напрямком наступу підрозділу, видом військ, регіоном дислокації[98].	
База даних записів із даними росіян (проєкт від OSINTFLOW)[99] – інформація про росіян із закритих та відкритих ресурсів, додатків та програмного забезпечення. Можливий пошук за анкетними даними, номером телефону.	
Реєстр російських окупантів, які воювали на Миколаївщині (проєкт центру журналістських розслідувань Nikcenter)[100] – ідентифіковані російські військові, причетні до злочинів на Миколаївщині. Пошук неможливий. Список осіб в алфавітному порядку.	

[91] Вебсайт «ОПРИЧНИКИ». URL: https://www.oprichniki.org/

[92] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 196.

[93] Реєстри «Вороги України» (проєкт від OSINT-спільноти MOLFAR). URL: https://molfar.com/enemies

[94] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 195.

[95] Сайт «Потерь.НЕТ». URL: https://poternet.site/ua

[96] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 196.

[97] Проєкт «Кто воюет в Украине». URL: https://war-proekt.media/base/voiska/

[98] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 196.

[99] База даних записів із даними росіян (проєкт від OSINTFLOW). URL: https://search.osintflow.com/search

[100] Реєстр російських окупантів, які воювали на Миколаївщині (проєкт центру журналістських розслідувань Nikcenter). URL: https://invaders.nikcenter.org/

БАЗИ ДАНИХ	
Бази даних доказів воєнних злочинів рф (проєкт міжнародної розвідувальної спільноти InformNapalm)[101] – включає кілька баз: базу даних російських підрозділів, задіяних до повномасштабного вторгнення у 2022 році; Інтерактивну базу даних російської агресії; Кадрову російську армію в Україні; Базу даних і відеографіка новітнього озброєння ЗС рф на Донбасі; Нагородне тавро воєнних злочинців. Бази постійно оновлюються.	
Увага! *Бази даних, які наповнюють приватні особи, можуть містити інформацію від анонімних джерел, «злиті дані», тому їх слід ретельно перевіряти й підкріплювати іншими доказами.*	

ОФІЦІЙНІ ДАНІ		
Міжнародних організацій	«UNICEF»[102], «IOM»[103], «Red Cross Society»[104] та ін.	
Органів державної влади та місцевого самоврядування	**Українські**	
	ОП[105], ОГП[106], МВС[107], обласних державних адміністрацій, обласних військових адміністрацій, територіальних громад та ін.	
	Варто виокремити ресурси офіційних установ[108]	
	Телеграм-канал СБУ[109]	
	Телеграм-канал ГУР МО[110]	

[101] Бази даних доказів воєнних злочинів рф (проєкт міжнародної розвідувальної спільноти InformNapalm). URL: https://informnapalm.org/ua/bazy-danyh/
[102] UNICEF. URL: https://www.unicef.org/ukraine/
[103] IOM. URL: https://ukraine.iom.int/uk
[104] Red Cross Society. URL: https://redcross.org.ua/
[105] Офіс Президента. URL: https://www.president.gov.ua/
[106] Офіс Генерального прокурора. URL: https://www.gp.gov.ua/
[107] Міністерство внутрішніх справ України. URL: https://mvs.gov.ua/
[108] Кваліфікація та розслідування порушення законів і звичаїв війни … . С. 196–197.
[109] СБУ. *Telegram*: вебсайт. URL: https://t.me/SBUkr
[110] ГУР МО. *Telegram*: вебсайт. URL: https://t.me/s/DIUkraine

<table>
<tr><th colspan="3">ОФІЦІЙНІ ДАНІ</th></tr>
<tr><td rowspan="5">Органів державної влади та місцевого самоврядування</td><td colspan="2">Російські, проросійські, окупаційної влади, наприклад Телеграм-канали</td></tr>
<tr><td>Маргарита Симоньян[111]</td><td></td></tr>
<tr><td>Мария Львова-Белова[112]</td><td></td></tr>
<tr><td>Владимир Соловьёв[113]</td><td></td></tr>
<tr><td>Рамзан Кадиров[114]</td><td></td></tr>
<tr><td>ПВК «Вагнер»[115]</td><td></td></tr>
<tr><td>Незалежних та приватних організацій</td><td colspan="2">Благодійних фондів та громадських організацій, правозахисних організацій ЦГП «Альменда»[116], Фундація DEJURE[117], Платформа прав людини[118] тощо.</td></tr>
</table>

Зазначений у таблиці перелік відкритих джерел не є вичерпним[119]. Пропонований перелік Телеграм-каналів, вебсайтів сформовано станом на 10.07.2024.

[111] Маргарита Симоньян. *Telegram*: вебсайт. URL: https://t.me/s/margaritasimonyan
[112] Мария Львова-Белова. *Telegram*: вебсайт. URL: https://t.me/s/malvovabelova
[113] Владимир Соловьёв. *Telegram*: вебсайт. URL: https://t.me/s/SolovievLive
[114] Рамзан Кадиров. *Telegram*: вебсайт. URL: https://t.me/s/RKadyrov_95/4699
[115] ПВК «Вагнер». *Telegram*: вебсайт. URL: https://t.me/s/wagnernew
[116] ЦГП «Альменда». URL: https://almenda.org/
[117] Фундація DEJURE. URL: https://dejure.foundation/
[118] Платформа прав людини. URL: https://ppl.org.ua/
[119] Протокол Берклі … . Приторінкове посилання № 1 на С. 20.

1.4. Кримінальні процесуальні основи та механізми «роботи» з відкритими джерелами цифрової інформації. Типові помилки в їх обранні

*Заходи, завдяки яким **вже здійснюється** встановлення (ідентифікація) воєнних злочинців та які пов'язані з роботою з відкритими джерелами та використанням цифрової інформації :*

- Розпізнавання злочинців за допомогою систем, які включають мережу з-понад 30 мільярдів зображень облич, отриманих з відкритих джерел в мережі «Інтернет».
- Верифікація воєнних злочинців у соціальних мережах, у тому числі за допомогою інструментів пошуку акаунтів соцмереж за фото Clearview та інструмента ідентифікації в соцмережах Artellence.
- Використання можливостей супутникового зв'язку та аналізу відео- і фотоматеріалів, отриманих з вилучених мобільних терміналів, камер відеоспостережень, камер відеоспостережень системи «Безпечне місто» тощо.
- Проведення OSINT-досліджень (фото- і відеоматеріали, отримані у глобальній мережі)[120]. Нагадуємо, що мета доказування в OSINT-розвідках не може переслідуватися [121].
- Використання міжвідомчої бази даних «Воєнний злочинець».

База даних **«Воєнний злочинець»** містить відомості про 550 000 воєнних злочинців, факти скоєння воєнних злочинів та докази, виявлені під час військової агресії рф[122].

Ця база даних **не є відкритою**, до неї мають доступ тільки працівники певних служб: СБУ, ГШ ЗСУ, ДПСУ, НАБУ, БЕБ, ДБР, ОГП та ін.

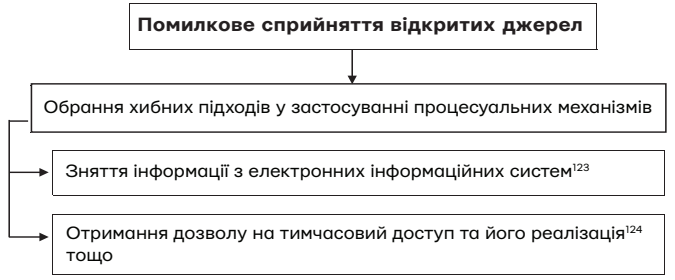
[120] Краєвська Т. Українські правоохоронці представили в Гаазі результати розслідування воєнних злочинів. УНН. 11.03.2024. *ІА «УНН»:* вебсайт. URL: https://unn.ua/news/ukrainski-pravookhorontsi-predstavyly-v-haazi-rezultaty-rozsliduvannia-voiennykh-zlochyniv

[121] Протокол Берклі … . С. 26.

[122] Краєвська Т. Українські правоохоронці представили в Гаазі результати розслідування воєнних злочинів. УНН. 11.03.2024. *ІА «УНН»:* вебсайт. URL: https://unn.ua/news/ukrainski-pravookhorontsi-predstavyly-v-haazi-rezultaty-rozsliduvannia-voiennykh-zlochyniv; У МВС ідентифікували понад 232 тисячі військових злочинців та зрадників. *Урядовий портал:* вебсайт. 03.08.2023. URL: https://www.kmu.gov.ua/news/u-mvs-identyfikuvaly-ponad-232-tysiachi-viisko vykh-zlochyntsiv-ta-zradnykiv

Чому важлива правильна оцінка джерела як відкритого?

Правильна оцінка джерела як відкритого передбачає, окрім іншого, задіяння належних процесуальних механізмів.



Для прикладу, у справі № 953/1240/23 проводилися «...зняття та огляд інформації з електронних інформаційних систем (мережі «Інтернет»), доступ до яких не обмежується її власником та не пов'язаний з подоланням системи логічного захисту, а саме інформації з офіційного сайту Управління культури, освіти та спорту Великобурлуцької селищної ради»[125], що начебто не суперечить положенням чинного КПК України (на перший погляд це випадок, який не потребує дозволу слідчого судді для отримання інформації з електронної інформаційної системи[126]). Утім, якщо доступ до вебресурсу не обмежується його власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, такі дії є некоректними[127]. Крім того, безпідставно

[123] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний суд:* вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/; Вирок колегії суддів Київського районного суду м. Харкова від 02.03.2023 у справі № 953/1240/23. URL: https://reyestr.court.gov.ua/Review/109609026

[124] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 149; Постанова колегії суддів Другої судової палати Касаційного кримінального суду Верховного Суду від 30.04.2020 у справі № 640/19897/16-к (провадження № 51-6241км19). URL: https://reyestr.court.gov.ua/Review/89034985

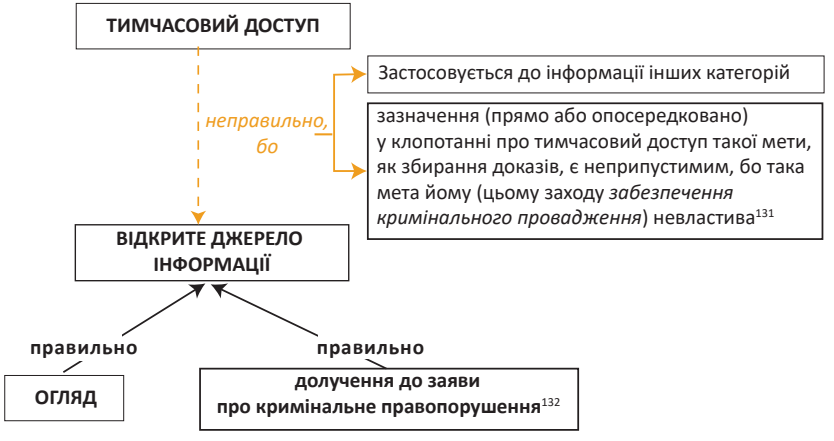
[125] Вирок колегії суддів Київського районного суду м. Харкова від 02.03.2023 у справі № 953/1240/23. URL: https://reyestr.court.gov.ua/Review/109609026

[126] Басиста І. В. Зняття інформації з електронних інформаційних систем. Велика українська юридична енциклопедія. У 20 т. Харків: Право, 2016. Т. 19. Кримінальний процес, судоустрій, прокуратура та адвокатура / редкол. В. Т. Нор (голова) та ін. Нац. акад. прав. наук України; Ін-т держави і права ім. В. М. Корецького НАН України; Нац. юрид. ун-т ім. Ярослава Мудрого. 2020. С. 348.

[127] Коваленко А. В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки*: зб. тез Міжнар. наук.-практ. конф. (22–23 лют. 2024 р.) / упор. У. О. Цмоць. Львів: Львів. держ. ун-т внутр. справ, 2024. С. 413–417. (Також презентація виступу). URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html

витрачаються людський ресурс та час (що порушує принцип процесуальної економії) через обрання такого неправильного підходу до роботи із «відкритим джерелом», що також могло б унеможливити подальше безпосереднє дослідження судом цього цифрового доказу з відкритого джерела, як і перевірку його достовірності через стирання (зміну, корегування тощо) інформації із згаданого офіційного сайту. Про цю практичну проблему із належною архівацією даних, які містяться у відкритих джерелах, вже вели мову як судді Верховного Суду , вказуючи, що іноді засад безпосередності «…взагалі неможливо дотриматися, оскільки перехід за відповідним посиланням в інтернеті не дає результату або ж за таким посиланням розміщена вже інша інформація»[128], так і науковці[129].

Важливо! Не слід забувати, що Інтернет «пам'ятає все»! Користуючись у вільному доступі цифровими бібліотеками[130] можна побачити архів Інтернет-сторінки: додавання, зміну чи видалення цифрової інформації тощо.



[128] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний суд:* вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

[129] Коваленко А. В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. … . С. 413– 417.

[130] Наприклад цифрова бібліотека Internet Archive. URL: https://archive.org/about/

[131] Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження, проведене Вищим спеціалізованим судом України з розгляду цивільних і кримінальних справ від 07.02.2014, підп. 9, п. 2.5. URL: https://zakon.rada.gov.ua/laws/show/n0001740-14#Text

[132] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 149–150; Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. Львів: ЛьвДУВС, 2022. С. 105, 130–132. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725

Утім, навіть за стану справ, коли проводяться *огляди загальнодоступної цифрової інформації*, є чимало питань щодо їх перебігу, інформативності та збереження інформації, отриманої з відкритих джерел, як і долучення до матеріалів провадження, і цьому свідченням є наявні судові рішення[133], є й такі кінцеві процесуальні рішення судів, які успішно «встояли» у касації[134]. Суди також мають процесуальний клопіт із правовою оцінкою скріншотів, співвідношенням оригіналу доказу та його копії тощо[135].

Чому потрібний алгоритм дій для всіх залучених у кримінальне провадження уповноважених суб'єктів, які «працюють» з відкритими джерелами цифрової інформації?

Концепція цифрової інформації з відкритих джерел як глобальне утворення, як вже йшлося, потребує вироблення алгоритму дій для всіх залучених у кримінальне провадження уповноважених суб'єктів, які «працюють» з відкритими джерелами цифрової інформації. Інакше не буде єдиного розуміння та підходу в оперативного працівника, слідчого, дізнавача, прокурора, слідчого судді та суду, як «поводитися» з цифровою інформацією з відкритих джерел, що негативно впливатиме на дотримання конституційних і конвенційних прав учасників такого кримінального провадження. Алгоритм має відповідати як чинному кримінальному процесуальному законодавству, так і застосовним міжнародно-правовим рамкам та стандартам щодо цифрових доказів з відкритих джерел, поняття яких поки у чинному КПК України не сформульовано, як і основи «процесуальної поведінки» з таким різновидом даних.

---

[133] Вирок Київського районного суду м. Харкова від 14.08.2023 у справі № 953/2635/23 (н/п 1-кп/953/807/23). URL: https://reyestr.court.gov.ua/Review/112892204; Вирок Хмельницького міськрайонного суду Хмельницької області у справі № 686/3769/23 (провадження № 1-кп/686/745/23). URL: https://reyestr.court.gov.ua/Review/113906215

[134] Постанова Третьої судової палати Касаційного кримінального суду Верховного Суду від 28.02.2024 у справі № 753/14148/21 (провадження № 51-6134 км 23). URL: https://reyestr.court.gov.ua/Review/117442733

[135] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний суд:* вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/; Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28.10.2021. *Верховний суд:* вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

РОЗДІЛ 2. ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ

2.1. Поняття кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку. Проблеми кваліфікації та кримінальної відповідальності, застосовність давності

Про які кримінальні правопорушення йде мова та до чого зобов'язує правозастосовувача міжнародно-правова бланкетність окремих із таких норм?

До цих кримінальних правопорушень належать ті, які передбачені у розділі XX Кримінального кодексу України. Серед них такі, на жаль, актуальні на сьогодні:

– пропаганда війни (ст. 436 КК України);

– виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436-2 КК України);

– планування, підготовка, розв'язування та ведення агресивної війни (ст. 437 КК України);

– порушення законів та звичаїв війни (ст. 438 КК України);

– екоцид (ст. 441 КК України, «Станом на грудень 2023 року процесуальне керівництво забезпечувалося у 25 кримінальних провадженнях, з них 14 пов'язані зі збройною агресією рф»[136]);

– геноцид (ст. 442 КК України) та ін.

Автори слушно підкреслюють міжнародно-правову бланкетність окремих із названих норм[137], що зобов'язує правозастосовувача звертатися до норм міжнародного права, зокрема міжнародного гуманітарного права, міжнародного кримінального права тощо.

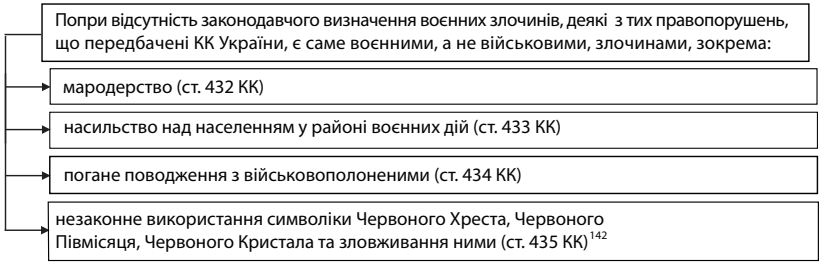
---

[136] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України:* вебсайт. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

[137] Пам'ятка для випускників закладів вищої освіти МВС України з документування злочинів, пов'язаних зі збройною агресією рф проти України: [практ. посіб.] / кол. авт.-уклад.: В. М. Василенко, А. І. Кисько, О. М. Музичук, В. В. Романюк та ін.; упоряд. С. Є. Абламський; за заг. ред. В. В. Сокуренка; МВС України, Харків. нац. ун-т внутр. справ. Вид. 2-ге, доп. і перероб. Харків: ХНУВС, 2024. С. 7–8.

«…в українському законодавстві немає таких понять, як «воєнний злочин» (хоча значна кількість авторів оперують саме такою термінологією, ведучи мову як про кваліфікацію, так і про розслідування[138]) або «злочин проти людяності»[139].

Воєнні злочини – порушення законів та звичаїв війни – належать до сфери виключно міжнародного кримінального права. Загальний перелік воєнних злочинів закріплений у Статуті Міжнародного кримінального суду (Римський статут)[140], який Україна на серпень 2024 року не ратифікувала[141].



Важливо! Ст. 6 Римського статуту МКС передбачає відповідальність за вчинення такого міжнародного злочину, як геноцид. При цьому порівняно з її викладом чинна ст. 442 КК України потребує приведення у відповідність з положеннями міжнародного права.

Ч. 2 ст. 442 КК України нерелевантна із її назвою та ч. 1. Через таку структуру норми, до тієї, поки що мізерної, статистики щодо облікованих актів злочину геноциду автоматично потрапляють і публічні заклики до геноциду, а також виготовлення матеріалів із закликами до геноциду, *які не є міжнародним злочином геноциду*, але відповідальність за вчинення яких передбачена ч. 2 ст. 442 КК України[143].

---

[138] Там само.

[139] Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані. 21.09.2023. *Радіо Свобода:* вебсайт. URL: https://www.radiosvoboda.org/a/doslidzhennia-rozsliduvannia-voiennyh-zlochyniv-v-ukraini/32602285.html

[140] Римський статут Міжнародного кримінального суду від 17 липня 1998 р. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text

[141] Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані ... .

[142] Там само.

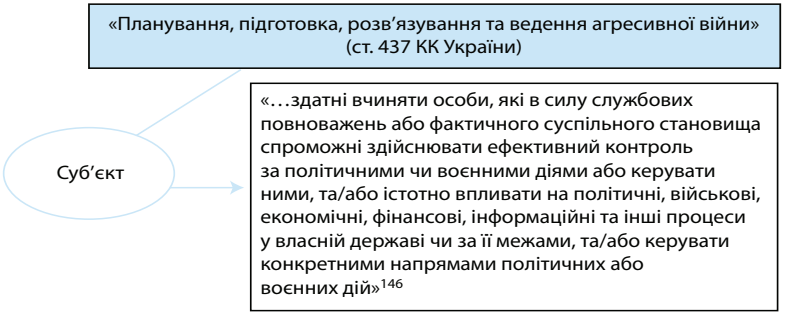
[143] Басиста І. В. Насильницька передача українських дітей – акт геноциду чи воєнний злочин? *Українська воєнна та повоєнна кримінальна юстиція:* матеріали IX (XXII) Львівськ. форуму кримін. юстиції (м. Львів, 26–27 жовт. 2023 р.) / упоряд. І. Б. Газдайка-Василишин. Львів: ЛьвДУВС, 2023. С. 18–64. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html; Басиста І. В. Притягнення до кримінальної відповідальності

Чи застосовується «давність» у разі вчинення цих злочинів?

Важливо! Схожим чином (але не аналогічним), як і в Римському статуті, національний законодавець унормував, що давність (у розумінні звільнення від кримінальної відповідальності у зв'язку із закінченням строків давності (ст. 49 КК України); звільнення від відбування покарання у зв'язку із закінченням строків давності виконання обвинувального вироку (ст. 80 КК України)) не застосовується, серед іншого, й у разі вчинення злочинів проти миру та безпеки людства, передбачених у ст. 437–439 і ч. 1 ст. 442 КК України (ч. 5 ст. 49 КК України та ч. 6 ст. 80 КК України)[144].

Чи наявні проблеми, які пов'язані із кваліфікацією та кримінальною відповідальністю?

Щодо проблем кваліфікації за чинним КК України, то наявні ґрунтовні наукові напрацювання із цього приводу, а окремі, в яких ще й узагальнені ті із них, які дотичні до процесуального права, вже вийшли друком у 2024 році[145]. Особливої уваги варта та обставина, що Велика Палата Верховного Суду сформулювала правовий висновок щодо суб'єкта за ст. 437 КК України.



за геноцид за чинним КК України: окремі проблеми. *Процесуальне та криміналістичне забезпечення досудового розслідування*: тези доп. учасників наук.-практ. семінару (01 груд. 2023 р.) / упор. А. Я. Хитра. Львів: ЛьвДУВС. 2023. С. 10–17. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html; Басиста І. В. Викрадення українських дітей як різновид геноцидної політики росії. *Військові кримінальні правопорушення та особливості їх розслідування*: матеріали кругл. столу, проведеного в межах Днів науки на ф-ті правн. наук Нац. ун-ту «Києво-Могилянська академія» (26 січ. 2024 р.). Київ: НаУКМА, 2024. С. 6–22; Бабін Б. В. Категорія геноциду та поточна правова система України. *Війна в Україні: зроблені висновки та незасвоєні уроки*: зб. тез міжнар. наук.-практ. конф. (22–23 лют. 2024 р.) / упор. У. О. Цмоць. Львів: Львівськ. держ. ун-т внутр. справ, 2024. С. 66–70. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html

[144] Кримінальний кодекс України від 05.04.2001 № 4651-VI (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/2341-14?f

[145] Пам'ятка для випускників закладів вищої освіти МВС України з документування злочинів, пов'язаних із збройною агресією рф проти України … . С. 7–8.

[146] Постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22). URL: https://reyestr.court.gov.ua/Review/117373993

Більш детально: постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22)[147].

Огляд судової практики ВС щодо кримінальних правопорушень, пов'язаних з війною

Важливо! Наявні невирішені питання щодо «…співвідношення складів кримінальних правопорушень, передбачених ч. 1 ст. 111-1 КК України та ст. 436-2 КК України»[148]. Звісно, на цьому перелік не вичерпується, актуальну судову практику Верховного Суду можна переглянути за посиланням https://supreme.court.gov.ua/supreme/pres-centr/info_anons_daidgest_oglyad/1590735/ (Огляд судової практики ВС щодо кримінальних правопорушень, пов'язаних з війною). Радимо також звернутися до напрацювань процесуалістів, які під своїм кутом зору виклали складові проблематики кваліфікації злочинів проти миру, безпеки людства та міжнародного правопорядку у перебігу їх розслідування[149].

Маємо й непросту ситуацію, що є наслідком застарілих правових рамок окремих формулювань статей ЖК. Так, «…застаріла правова рамка ст. 147 ЖК IV, на яку спирається § 2441 КЗ США, яка не дозволяє назвати речі своїми іменами, однак з погляду Римського статуту ці дії становлять окремий воєнний злочин – сексуальне насильство (ст. 8 (2) (b) (xxii))»[150].

Наявна також проблема у дещо іншій площині, зокрема з тим, як правильно зазначають правозахисники, що до початку повномасштабного вторгнення більшість злочинів, пов'язаних з порушенням міжнародного гуманітарного права, кваліфікувалися як загальні кримінальні правопорушення[151]. Тому й постає питання щодо відмінностей у «режимах» кваліфікації та й загалом розслідування, яке поки що залишається без відповіді.

[147] Там само.

[148] Судді ВС розповіли про останні тенденції у сфері кримінального права України. 28.12.2023. *ТОВ «ІА «БОРГ.ЕКСПЕРТ»*: вебсайт. URL: https://borgexpert.com/news/suddi-vs-rozpovily-pro-ostanni-tendentsii-u-sferi-kryminalnoho-prava-ukrainy

[149] Головюк І. В. Вироки за ст. 438 КК України: порушення законів та звичаїв війни (з 24 лютого 2022 року). *Вища школа адвокатури*: вебсайт. URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/porusennia-zakoniv-ta-zvicayiv-viini-st-438-kk-mezi-ta-pidstavi-kriminalizaciyi; Головюк І. В. Порушення законів та звичаїв війни: про особливості кваліфікації злочину. *Вища школа адвокатури:* вебсайт. URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/porusennia-zakoniv-ta-zvicayiv-viini-pro-osoblivosti-kvalifikaciyi-zlocinu-rozpovila-advokat-irina-gloviuk; Serhii Ablamskyi, Volodymyr Galagan, Iryna Basysta, Zhanna Udovenko Detention of a person suspected of committing a criminal offense during martial law in Ukraine (Detenção de uma pessoa suspeita de cometer um crime durante a lei marcial na Ucrânia). *Revista Brasileira de Políticas Públicas*. 2023. Vol. 13. N. 3. P. 452–467. DOI: https://doi.org/10.5102/rbpp.v13i3.9129

[150] Задоя К. Перше кримінальне провадження в США щодо воєнних злочинів, вчинених в Україні. 01.02.2024. *Глобальна ініціатива T4P (Трибунал для Путіна):* вебсайт. URL: https://t4pua.org/2281

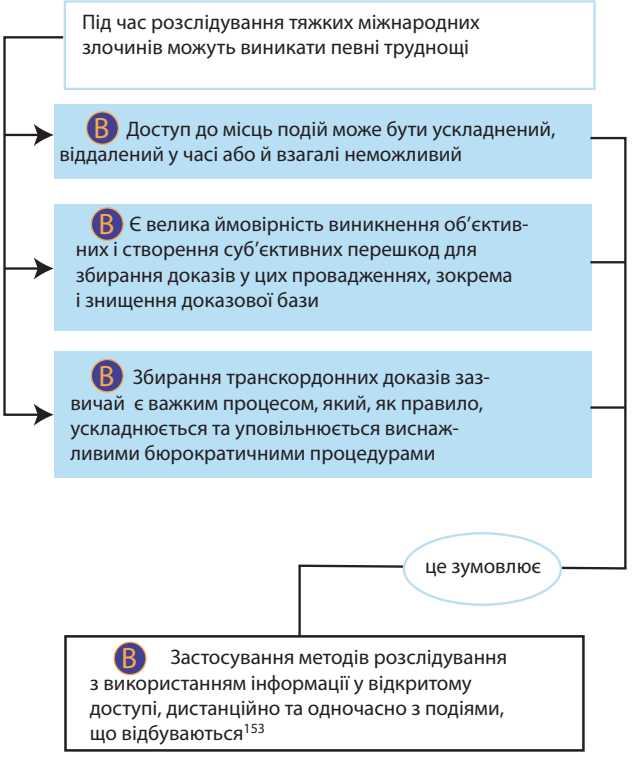
[151] Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані … .

2.2. Значення інформації у відкритому доступі мережі «Інтернет» для міжнародних та національних розслідувань. Дотримання вимог міжнародного публічного права. Мінімальні стандарти безпеки за Протоколом Берклі

Чому інформація у відкритому доступі мережі «Інтернет» важлива як для міжнародних, так і для національних розслідувань?

З аналізу положень Протоколу Берклі слідує, що:

> «Оскільки розслідування тяжких міжнародних злочинів пов'язані з багатьма правовими та політичними процесами, які й дозволяють їх проводити чи блокують провадження у певний період часу, а лише згодом настає така нагода реалізації, то й логічно, що вони віддалені від самих подій кримінальних правопорушень у просторі та часі»[152].



[152] Протокол Берклі … . С. 22.
[153] Там само.

Як «співдіють» вимоги міжнародного гуманітарного права, міжнародного кримінального права та міжнародного права у сфері прав людини під час розслідування цих злочинів?

Дотримання вимог міжнародного публічного права передбачає одночасне дотримання вимог міжнародного гуманітарного права, міжнародного права у сфері прав людини, міжнародного кримінального права.

> Застосування міжнародного гуманітарного права та/або міжнародного кримінального права не звільняє держави від виконання своїх зобов'язань за міжнародним правом у сфері прав людини. Щодо застосовності цих положень див. п. 42–47 Протоколу Берклі[154].

Чому важливо, щоб національна криміналізація тяжких міжнародних злочинів та «правила» національних розслідувань відповідали міжнародному праву прав людини, міжнародному гуманітарному праву та міжнародному кримінальному праву?

У наших розслідуваннях маємо бути дотичними до ситуацій та тих проваджень, які вже здійснює МКС, Міжнародний Суд ООН, ЄСПЛ та суди в інших країнах, зокрема й за принципом універсальної юрисдикції. Також прогнозованим та обговорюваним є створення трибуналів, зокрема й щодо вчиненої російської агресії.

> У Протоколі Берклі зазначено: «…коли слідчі, які ведуть розслідування з використанням даних у відкритому доступі, не знають (обєктивно. – Авт.) конкретного механізму чи юрисдикції, вони повинні прагнути збирати та зберігати інформацію таким чином, щоб максимально використовувати її у найширшому діапазоні потенційно релевантних юрисдикцій. Якщо слідчі знають про відповідні вимоги до місця, де врешті-решт буде розглядатися справа, вони повинні адаптувати свої процеси до тих конкретних вимог»[155].

Важливо! Щоб працівники-практики глибше зрозуміли сучасні процеси, пропонуємо приклад реалізації юрисдикції за принципом пасивної правосуб'єктності, як от щодо висунення в США обвинувачення російським військовим щодо подій, які трапилися на території України[156].

[154] Там само.

[155] Там само. С. 44.

[156] Задоя К. Перше кримінальне провадження в США щодо воєнних злочинів, вчинених в Україні. 01.02.2024. *Глобальна ініціатива T4P (Трибунал для Путіна):* вебсайт. URL: https://t4pua.org/2281

Що таке «оцінка ризиків» та «мінімальні стандарти безпеки» під час роботи з відкритими джерелами цифрової інформації?

Мінімальні стандарти безпеки є основоположними під час роботи з відкритими джерелами задля виявлення та збирання цифрової інформації, а оцінка ризиків та безпеки є глибинним завданням.

(Детальніше див. Додаток II до Ⓑ Протоколу Берклі «Шаблон оцінки цифрових загроз та ризиків»[157]). Розлогіше їх описано у п. 67–93 Ⓑ Протоколу Берклі[158]. Їх дотримання упродовж діяльності з пошуку детально відображено у підрозд. 5.1 (п. 5.1.3) цього Порадника.

2.3. Проблемні питання, які виникають під час розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (визначення підслідності, застосування особливого порядку in absentia тощо). Рекомендації щодо їх вирішення

Що слід розуміти під розслідуванням з використанням даних у відкритому доступі за Протоколом Берклі?

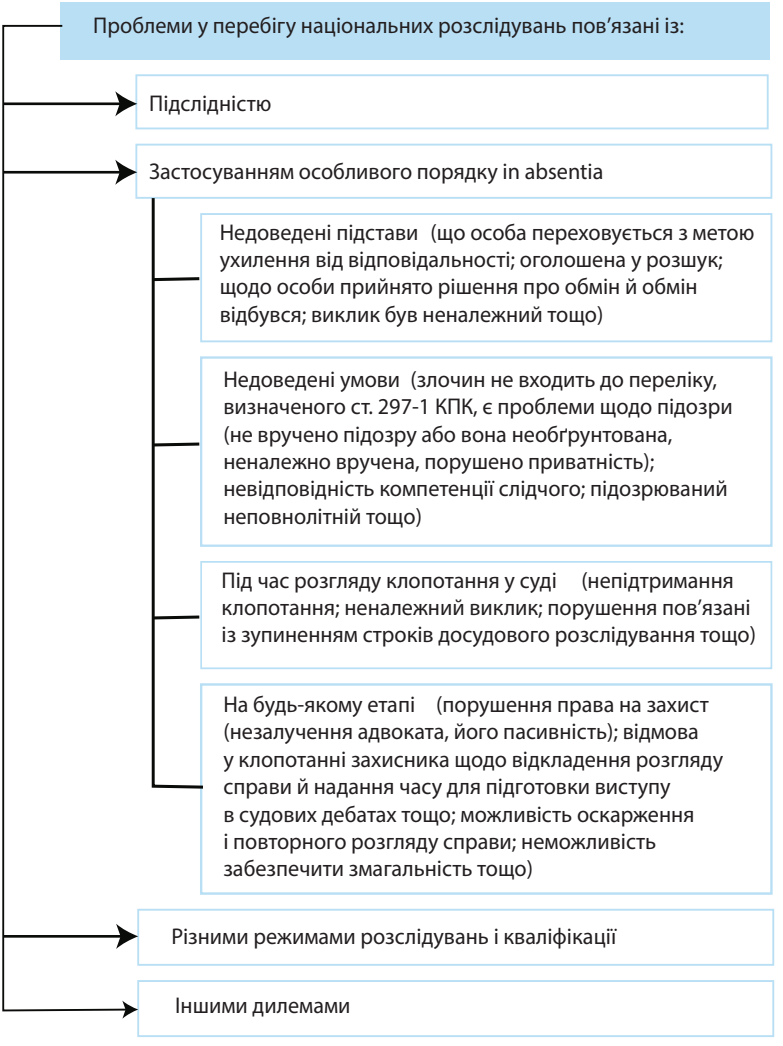
Ⓑ У Протоколі Берклі запропоновано таке визначення: «…розслідування з використанням даних у відкритому доступі стосується використання інформації у відкритому доступі для функцій збирання інформації та доказів»[159].

Які узагальнені проблеми наявні у перебігу національних розслідувань?

Певна кількість проблем, які наявні у перебігу національних розслідувань, є наслідком відсутнього аналогічного досвіду в інших країнах, який ми б могли запозичити (Україна працює над притягненням до відповідальності винних у міжнародних злочинах ще до завершення війни, залучаючи власних прокурорів, слідчих і суддів[160]).

---

[157] Протокол Берклі … . С. 115.
[158] Там само. С. 55–62.
[159] Там само. С. 27.
[160] Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані … .



Яка ситуація із підслідністю та допустимістю зібраних доказів у разі її недотримання?

Ч. 2 ст. 216 КПК України унормовано, що всі кримінальні правопорушення, що передбачені у розділі XX «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку» чинного КК України, за винятком тих, які визначені ст. 436-1 та 445 КК, підслідні слідчим органів безпеки, які й мали б здійснювати досудове розслідування у цих кримінальних провадженнях.

Важливо! Так склалося, що «…слідчі СБУ об'єктивно не можуть розслідувати таку кількість воєнних злочинів, тому до розслідування цієї категорії злочинів залучаємо слідчих ще двох органів…», «…обов'язково на початковому етапі, якомога раніше, залучаємо слідчих СБУ, які певний час розслідують кримінальне провадження»[161].

***Увага*!** Національна судова практика, яка існувала та існує (хоча вона має тенденцію змінюватися), здебільшого вважає доказ, зібраний з «порушенням правил підслідності», недопустимим.

Чи маємо проблеми із цими кримінальними провадженнями через їх «заочність»?

У питаннях здійснюваних та триваючих розслідувань, як і судових розглядів, маємо і суттєву дилему із застосуванням особливого порядку in absentia.

Важливо! Попри те, що це «…полістадійна ускладнена форма кримінального провадження, яка зумовлена специфічними фактичними та юридичними підставами його здійснення, містить додаткові гарантії дотримання прав осіб, які беруть участь у кримінальному провадженні, та відрізняється особливостями реалізації окремих засад кримінального провадження»[162], на жаль, у практичній діяльності цим усім складовим не приділяють належної уваги, а окремі з них взагалі нівельовані.

Розуміння глибини та розмаху проблематики у перебігу цієї «ускладненої форми кримінального провадження»[163] слідує із таких оприлюднених у 2023 році начальником Департаменту війни ОГП даних, що є «…велике провадження щодо злочину агресії відносно вищого військово-політичного керівництва російської федерації. У ньому маємо 639 підозрюваних осіб…», «…у більшості випадків наші розслідування здійснюються за заочною процедурою…»[164]. Зі слів

---

[161] Рік розслідування воєнних злочинів. Інтерв'ю з Юрієм Бєлоусовим, начальником Департаменту війни ОГП [текстова версія]. 02.03.2023. *Justtalk:* вебсайт. URL: https://justtalk.com.ua/post/rik-rozsliduvannya-voennih-zlochiniv-intervyu-z-yuriem-belousovim-nachalnikom-departamentu-vijni-ogp-tekstova-versiya

[162] Дроздов О. Глава 8. Кримінальне провадження за відсутності підозрюваного, обвинуваченого (in absentia) у підручнику «Особливі порядки кримінального провадження». С. 172–206. [О. В. Капліна, О. І. Марочкін, М. І. Демура та ін.]; за ред. О. В. Капліної; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2024. 366 с.

[163] Там само.

[164] Рік розслідування воєнних злочинів. Інтерв'ю з Юрієм Бєлоусовим, начальником Департаменту війни ОГП [текстова версія]. 02.03.2023. *Justtalk:* вебсайт. URL: https://justtalk.com.ua/post/rik-rozsliduvannya-voennih-zlochiniv-intervyu-z-yuriem-belousovim-nachalnikom-departamentu-vijni-ogp-tekstova-versiya

керівника ГСУ Національної поліції України вже станом на 31.01.2024 йдеться про 2 тис. 400 підозр[165].

Які питання виникають під час застосування процедури in absentia у цих кримінальних провадженнях та як їх вирішувати?

Щоб звернути увагу слідчих на прогнозовані порушення та проблемні питання, які виникають під час застосування процедури in absentia, ми сформували таблицю, в якій їх узагальнили та відобразили окремі пропозиції, як їх уникнути.

В основі таблиці використано:

– підстави та умови здійснення спеціального досудового розслідування, а також особливості доказування, які систематизовані І. Гловюк та М. Стояновим[166];

– узагальнення судової практики, що проведене авторами курсу УГСПЛ «Колабораційна діяльність: кримінальний та цивільний аспекти»[167];

– огляд судової практики ККС ВС щодо здійснення спеціальної процедури кримінального провадження (досудового розслідування та судового розгляду) за відсутності обвинуваченого (in absentia)[168];

– узагальнення судової практики щодо відмов слідчими суддями в задоволенні клопотання про здійснення спеціального досудового розслідування, яке провів І. Калька[169];

– судові рішення з пошуку в ЄДРСР, а також наукові розвідки інших авторів, на яких наявні релевантні посилання у тексті таблиці.

---

[165] Геронтьєва О. Проблеми з безпекою через зброю в країні не бачу, загрози громадянам немає – керівник Головного слідчого управління Нацполіції. 31.01.2024. *ІА «Інтерфакс-Україна»:* вебсайт. URL: https://interfax.com.ua/news/interview/963982.html

[166] Гловюк І., Стоянов М. Особливості доказування у спеціальному досудовому розслідуванні: окремі питання. *Право України*. 2017. № 12. С. 19–26.

[167] ILIA (International Law in Advocacy) is a collaborative platform, developed organically by Human Rights House Foundation and Houses over the course of over a decade. URL: https://ilia.humanrightshouse.org/course/view.php?id=430

[168] Огляд судової практики Касаційного кримінального суду щодо здійснення спеціальної процедури кримінального провадження (досудового розслідування та судового розгляду) за відсутності обвинуваченого (in absentia). Рішення, внесені до ЄДРСР з 2018 року по серпень 2022 року / упоряд.: заст. голови Касаційного кримінального суду у складі Верховного Суду, канд. юрид. наук В. В. Щепоткіна, правове управління (ІІІ) департаменту аналітичної та правової роботи апарату Верховного Суду. Київ, 2022. 23 с. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1344119/

[169] Калька І. З. Реалізація прав підозрюваного, обвинуваченого в спеціальному кримінальному провадженні (in absentia): дис. … д-ра філос. за спец. 081 – Право. Нац. акад. внутр. справ. Київ, 2023. 265 с.

Окремі проблеми та порушення під час досудового розслідування та судового розгляду у перебігу застосування процедур in absentia

1. Недоведені підстави для здійснення спеціального досудового розслідування	
1.1. Не надано доказів, що особа переховується від органів слідства та суду на тимчасово окупованій території України, на території держави, визнаної Верховною Радою України державою-агресором, з метою ухилення від кримінальної відповідальності	
Чи перебуває особа на тимчасово окупованій території або території держави-агресора?	⊕ Вказівка у відкритих джерелах (мережі «Інтернет») конкретного місцезнаходження особи за межами підконтрольної Україні території є додатковим підтвердженням перебування особи на цій території[170].
Чи особа справді ухиляється від кримінальної відповідальності?	⊕ Сам факт перебування підозрюваного на тимчасово окупованій території не може свідчити про його бажання та спроби уникнення кримінальної відповідальності, оскільки, в даному випадку є очевидним факт непереборної сили у вигляді воєнних подій, у зв'язку з чим підозрюваний навіть будучи обізнаним про необхідність явки до слідчого, не може виконати свій обов'язок з огляду на обставини, які від нього не залежать[171].
Чи було здійснено виклики належним чином не менш ніж три рази[172]?	⊕ Належним є виклик особи, який відповідає ст. 135, 297-5 КПК України.
	⊕ Направлення повідомлення про підозру та повісток підозрюваному, який перебуває на тимчасово окупованій території України, за допомогою месенджера «Viber» на номер телефону, яким користувався підозрюваний, і підтвердження того, що він переглянув ці повідомлення, відповідає положенням КПК та є додатковим заходом до основних способів інформування підозрюваного, передбачених КПК[173].
	⊖ Виклик підозрюваного із застосуванням месенджерів є неналежним повідомленням учасника кримінального провадження про виклик, оскільки такого порядку повідомлення процесуальним законом не передбачено[174].

[170] Постанова ВС від 04.11.2021 у справі № 326/1385/18 (провадження № 51-2018км21). URL: https://reyestr.court.gov.ua/Review/101100299

[171] Ухвала Дніпровського апеляційного суду від 29.06.2023 у справі № 932/3698/22. URL: https://reyestr.court.gov.ua/Review/111950943

[172] Гловюк І., Стоянов М. Особливості доказування у спеціальному досудовому розслідуванні: окремі питання. *Право України*. 2017. № 12. С. 19–26.

[173] Постанова ВС від 04.11.2021 у справі № 326/1385/18 (провадження № 51-2018км21). URL: https://reyestr.court.gov.ua/Review/101100299

[174] Ухвала Орджонікідзевського районного суду м. Запоріжжя від 16.09.2022 у справі № 335/1262/19. URL: https://reyestr.court.gov.ua/Review/106354358

Також треба з'ясувати, чи були причини неявки підозрюваного на виклик поважними не менш ніж три рази[175]?

1.2. Не надано доказів, що особа оголошена у міжнародний розшук

 Жодних даних про оголошення особи у міждержавний та/або міжнародний розшук або переховування понад шість місяців від органів слідства та суду з метою ухилення від кримінальної відповідальності, та/або стосовно якої наявні фактичні дані, що вона перебуває за межами України, на тимчасово окупованій території України або в районі проведення антитерористичної операції, органом досудового розслідування не надано, а тому підстави для здійснення спеціального судового провадження немає[176].

 Належними доказами оголошення у міжнародний розшук є наявність постанови про оголошення розшуку, а також особу поставлено на облік в Інтерполі[177].

 Утім, підтримуємо позицію, що на підтвердження оголошення особи у міжнародний розшук слід **сукупно подавати такі документи**:

1) постанову про оголошення у міжнародний розшук;
2) витяг з ЄРДР про внесення відомостей про міжнародний розшук;
3) запит до НЦБ Інтерполу в Україні;
4) витяг з бази даних Інтерполу про перебування особи у розшуку[178].

1.3. Не доведено, що уповноваженим органом прийнято рішення про передачу підозрюваного для обміну як військовополоненого та такий обмін відбувся

 «У судовому засіданні з'ясувалося що у прокурора фактично відсутнє відповідне рішення відповідного координаційного штабу щодо засудженого… У зв`язку з тим, що прокурором до клопотання не долучено зазначених доказів в обґрунтування клопотання, суд вважає за необхідне повернути без розгляду відповідне клопотання з роз'ясненням, що це не перешкоджає повторному зверненню з клопотанням після усунення обставин, що стали підставою для повернення»[179].

 «У судовому засіданні прокурором було долучено до матеріалів справи роздруківки статей із ЗМІ РФ, у яких зазначено, що особа 07.09.2019 року була обміняна за формулою «35 на 35», однак жодної офіційної інформації, чи дійсно останній був обміняний, якщо так, то в якості кого (для спеціального судового провадження важливий статус військовополоненого), прокурором не надано»[180].

---

[175] Там само.

[176] Ухвала Слов'янського міськрайонного суду Донецької області від 15.06.2020 у справі № 243/3303/20. URL: https://reyestr.court.gov.ua/Review/89806902

[177] Постанова Касаційного кримінального суду у складі Верховного суду від 07.12.2022 у справі № 385/619/16. URL: https://reyestr.court.gov.ua/Review/107834205

[178] Федоренко І. Л. Міжнародний розшук, процедура in absentia в українському законодавстві. Презентація. 9 с. *Асоціація правників України*: вебсайт. URL: https://uba.ua/documents/events/2020/Kate/UBA%20Knowledge%20Hub/%D0%A4%D0%B5%D0%B4%D0%BE%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%86%D0%B3%D0%BE%D1%80.pdf

[179] Ухвала Вільнянського районного суду Запорізької області від 08.04.2024 у справі № 314/1565/24. URL: https://reyestr.court.gov.ua/Review/118189336

[180] Ухвала Дарницького районного суду м. Києва від 08.11.2023 у справі № 753/12538/16-к. URL: https://reyestr.court.gov.ua/Review/114779246

До матеріалів справи слід додавати документи, які підтверджують: 1) рішення про передачу військовополоненого (протокол[181] чи «витяг з протоколу»[182] Координаційного штабу з питань поводження з військовополоненими); 2) факт обміну (наприклад «відповідь»[183], «повідомлення»[184], «інформація»[185] з Координаційного штабу з питань поводження з військовополоненими).
2. Недоведені умови для здійснення спеціального досудового розслідування
2.1. Злочин не входить до переліку, визначеного ч. 2 ст. 297-1 КПК
Ст. 146 КК України не входить до переліку статей, що містяться в ч. 2 ст. 297-1 КПК України, за вчинення яких може здійснюватися спеціальне досудове розслідування[186].
Злочин, передбачений ч. 3 ст. 365 КК України, належить до злочинів, до яких можливе встановлення спеціального судового розгляду, однак злочин, передбачений ч. 1 ст. 307 КК України, не входить до переліку злочинів, передбачених ч. 2 ст. 297-1 КПК України, що виключає в цьому випадку спеціальний судовий розгляд[187].
Обґрунтувати необхідність розслідування злочину, який не входить до переліку, визначеному у ч. 2 ст. 297-1 КПК, в одному кримінальному провадженні зі злочинами, які зазначені у цій частині, та неможливість виділення матеріалів через можливий негативний вплив на повноту досудового розслідування та судового розгляду відповідно до абз. 3 ч. 2 ст. 297 КПК.
2.2. Проблеми щодо підозри (обґрунтування, вручення тощо)
2.2.1. Особі не повідомлено про підозру, підозра не обґрунтована
Враховуючи, шо особу про підозру у вчиненні кримінального правопорушення не повідомлено та у міждержавний та міжнародний розшук не оголошено, слідчий суддя дійшов висновку про відсутність підстав, встановлених ст. 297-1 КПК України, для здійснення спеціального досудового розслідування, у зв`язку з чим у задоволенні клопотання слід відмовити[188].

[181] Про утворення Координаційного штабу з питань поводження з військовополоненими: Постанова КМУ від 11.03.2022 № 257. Абз. 3. П. 9. URL: https://zakon.rada.gov.ua/laws/show/257-2022-%D0%BF#Text

[182] Ухвала Личаківського районного суду м. Львова від 10.11.2022 у справі № 463/1712/22. URL: https://reyestr.court.gov.ua/Review/107356174

[183] Там само.

[184] Ухвала Галицького районного суду м. Львова від 31.03.2023 у справі № 461/2055/23. URL: https://reyestr.court.gov.ua/Review/109924830

[185] Ухвала Галицького районного суду м. Львова від 12.12.2023 у справі № 461/10189/23. URL: https://reyestr.court.gov.ua/Review/115578469

[186] Ухвала слідчого судді Печерського районного суду м. Києва від 08.10.2020 у справі № 757/42166/20-к. URL: https://reyestr.court.gov.ua/Review/92178885

[187] Київський районний суд м. Харкова від 15.09.2022 у справі № 953/4064/22. URL: https://reyestr.court.gov.ua/Review/106252541

[188] Ухвала Апеляційного суду Житомирської області від 09.12.2016 у справі № 295/15419/16-к. URL: https://reyestr.court.gov.ua/Review/63335901

2.2.2. Неналежне вручення особі повідомлення про підозру

У царині недотримання належного порядку повідомлення про підозру за умов порядку in absentia є сутнісні ризики порушення конституційних, процесуальних та конвенційних прав. І ця «процесуальна біда» мала місце[189], як до затвердження «Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження (у газеті «Урядовий кур'єр») та на офіційному вебсайті Офіса Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування»[190] (далі – Порядок), так і є, із частково «мінімалізованими» ризиками, й сьогодні[191]. Доволі низька ймовірність того, що підозрюваний, обвинувачений прочитає документи, які публікують на вебсайті Офіса Генерального прокурора та газеті «Урядовий кур'єр», про що неодноразово наголошували науковці[192]. Отож, маємо цілу низку невирішених ситуацій із вжиттям всіх належних заходів щодо вручення (доведення) особі повідомлення про підозру, серед яких й належне виконання п. 4 Розділу III Порядку[193].

⛔ «…повідомлення про підозру було вручено директору ЖЕО КП «КОМСЕРВІС» за місцем проживання особи. Однак жодних доказів, що саме це ЖЕО здійснює обслуговування будинку за місцем проживання особи, та взагалі, що така організація існувала та здійснювала свою діяльність на момент вручення підозри, суду надано не було»[194].

⛔ «…відсутні беззаперечні (недвозначні) докази, що підтверджують факт інформування особи про притягнення її до кримінальної відповідальності (повідомлення про підозру), а також доказів, з яких можна зробити висновок, що обвинувачений намагався ухилитися від суду чи недвозначно відмовився від свого права прибути на судове засідання»[195].

---

[189] Жидков В. Л., Жила О. Б. Застосування спеціальної процедури притягнення до кримінальної відповідальності (in absentia) за колабораційну діяльність (публікація стала можливою завдяки щедрій підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID) в рамках Програми «Права людини в дії», яка виконується Українською Гельсінською спілкою з прав людини). Київ, 2023. С. 5. URL: https://www.helsinki.org.ua/wp-content/uploads/2023/06/Zastosuvannia-spetsialnoi-protsedury-prytiahnennia-do-kryminalnoi-vidpovidalnosti-in-absentia-za-kolaboratsiynu-diialnist.pdf

[190] Про затвердження Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження та на офіційному вебсайті Офіса Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування: Наказ Офіса Ген. прокурора від 30.05.2023 р. № 141. URL: https://zakon.rada.gov.ua/laws/show/v0141905-23#Text

[191] Гутник А. В. Забезпечення права на захист персональних даних підозрюваного у кримінальному провадженні: проблеми та шляхи їх розв'язання. *Бізнес і права людини в Україні: проблеми та рішення під час війни й повоєнного відновлення*: зб. матеріалів III Всеукр. конкурсу наук. робіт; за заг. ред. В. А. Устименка; ред.-упоряд. А. Є. Санченко. Київ: Компанія «ВАІТЕ», 2024. С. 174–182.

[192] Корякін Р. О., Яковенко М. О. Актуальні проблеми спеціального досудового розслідування кримінальних правопорушень. *Вісн. Луганськ. держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. 2016. № 2. С. 115; Кримчук С. Г. Окремі аспекти здійснення повідомлення про підозру у спеціальному досудовому розслідуванні. *Юрид. бюлетень*. 2019. Вип. 11. Ч. 2. С. 274. URL: http://www.lawbulletin.oduvs.od.ua/archive/2019/11/part_2/37.pdf; Атаманов О. М. Повідомлення про підозру особі, місцезнаходження якої не встановлено або яка перебуває за межами України: дис. … д-ра філос. за спец. 081 – Право / Нац. акад. внутр. справ.

⛔ «…жодних доказів того, що дане повідомлення було вручено особисто, чи у разі неможливості такого вручення, іншим особам, визначеним ст. 135 КПК, суду надано не було»[196]
⛔ Надсилання судових повісток і викликів під час спеціального досудового розслідування та судового провадження, а також публікування вказаних викликів у засобі масової інформації загальнодержавного значення обвинуваченому, який проживає на тимчасово окупованій території України, із вказівкою на іншу адресу проживання, ніж та, що зазначена в матеріалах кримінальної справи, вважається неналежним повідомленням обвинуваченого про день, час та місце розгляду справи[197].
✅ **Належне вручення повідомлення про підозру:** 1) надсилати повідомлення про підозру відповідно до вимог ч. 1, 2, 4, 5, 6, 7 КПК; 2) якщо обґрунтовано неможливо вручити у спосіб, зазначений у п. 1, то: а) зазначити про це у клопотанні; б) додати відповідні докази неможливості такого вручення; в) вручити повідомлення відповідно до ч. 8 ст. 135 КПК (вебсайт ОГП + газета «Урядовий кур'єр») та додатково надіслати за допомогою соцмереж; г) зазначити інформацію про публікації та дати їх у клопотанні; д) додати докази публікації до клопотання; 3) зазначити правильну адресу проживання. **Див. про належне вручення повісток про виклик у цій таблиці – блок 1.1.**

Київ, 2021. С. 152; Тимофеєв А. О. Проблеми практичної реалізації процедури спеціального досудового розслідування (in absentia) в Україні. *Наук. записки НаУКМА. Юрид. науки*. 2021. Т. 8. С. 64. URL: http://nrplaw.ukma.edu.ua/article/view/254047; Гутник А., Коць Є. Проблемні аспекти вручення процесуальних документів особі, яка перебуває на тимчасово окупованій території або на території держави-агресора. *Наук. вісн. Дніпропетров. держ. ун-ту внутр. справ*. 2023. № 2. С. 272–273. DOI: 10.31733/2078-3566-2023-2-271-279.

[193] Про затвердження Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження та на офіційному вебсайті Офіса Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування: Наказ Офіса Ген. прокурора від 30.05.2023 р. № 141. URL: https://zakon.rada.gov.ua/laws/show/v0141905-23#Text

[194] Ухвала Красногвардійського районного суду м. Дніпропетровська від 31.10.2022 у справі № 204/8858/22. URL: https://reyestr.court.gov.ua/Review/107362235

[195] Ухвала Ленінського районного суду м. Кіровограда від 21.01.2022 у справі № 405/8268/21. URL: https://reyestr.court.gov.ua/Review/102696510

[196] Ухвала Красногвардійського районного суду м. Дніпропетровська від 31.10.2022 у справі № 204/8856/22. URL: https://reyestr.court.gov.ua/Review/107401003

[197] Постанова ВС від 13.06.2019 у справі № 607/9498/16-к (провадження № 51-2422км18). URL: http://reyestr.court.gov.ua/Review/82492181; Огляд судової практики Касаційного кримінального суду щодо здійснення спеціальної процедури кримінального провадження (досудового розслідування та судового розгляду) за відсутності обвинуваченого (in absentia). Рішення, внесені до ЄДРСР, з 2018 року по серпень 2022 року / упоряд.: заступник голови Касаційного кримінального суду у складі Верховного Суду, канд. юрид. наук В. В. Щепоткіна, правове управління (III) департаменту аналітичної та правової роботи апарату Верховного Суду. Київ, 2022. 23 с. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1344119/

Додатковий спосіб інформування. «Письмове повідомлення про підозру скеровано … в «Instagram»… у віповідь на яке він повідомив «Приеду скоро на танке! обязательно жди» (мова оригіналу. – Авт.) … підозрюваний висловив слідчому намір з'явитися у спосіб (на танку), який за реальних обставин виключає його явку та можливість вчинення за його участю процесуальних дій (принаймні тих, які слідчий мав намір провести), що вказує на небажання підозрюваного виконувати свій процесуальний обов`язок»[198]. Таке повідомлення є підтвердженням отримання повідомлення про підозру чи повістки про виклик[199]

2.2.3. Порушення права на приватність особи під час публікації повідомлення про підозру на вебсайті ОГП та у газеті «Урядовий кур'єр»

Виявлені порушення щодо роботи із персональними даними[200]: надмірне збирання, безстрокове зберігання, розголошення.

Щодо підозрюваного

Оприлюднено надмірну кількість персональних даних: інформацію про національність, місце народження, сімейний стан, судимість, місце роботи, реєстраційний номер облікової картки платника податків, наявність статусу особи, щодо якої здійснюється особливий порядок кримінального провадження[201], дані паспорта громадянина України та паспорта для виїзду за кордон[202].

Неприховано персональні дані дітей підозрюваного, які перебувають на його утриманні[203].

Щодо потерпілого та свідків

Неприховано прізвища, імена та по батькові, дати народження осіб, у яких підозрювана відбирала заяви та пояснення[204].

[198] Ухвала Корольовського районного суду м. Житомира від 31.03.2023 у справі № 296/2927/23. URL: https://reyestr.court.gov.ua/Review/110121449

[199] Гутник А., Коць Є. Проблемні аспекти вручення процесуальних документів особі, яка перебуває на тимчасово окупованій території або на території держави-агресора. *Наук. вісн. Дніпропетров. держ. ун-ту внутр. справ*. 2023. № 2. С. 275.

[200] Гутник А. В. Забезпечення права на захист персональних даних підозрюваного у кримінальному провадженні: проблеми та шляхи їх розв'язання. *Бізнес і права людини в Україні: проблеми та рішення під час війни й повоєнного відновлення*: зб. матеріалів III Всеукр. конкурсу наук. робіт; за заг. ред. В. А. Устименка; ред.-упоряд. А. Є. Санченко. Київ: Компанія «ВАІТЕ», 2024. С. 177–188.

[201] Гутник А. В. Порушення Закону України «Про захист персональних даних» на вебсайті Офіса Генерального прокурора. *«Наукова весна» 2023*: матеріали XIII Міжнар. наук.-техн. конф. студ., аспірантів та мол. вчених (м. Дніпро, 1–3 бер. 2023 р.). Дніпро: НТУ «ДП», 2023. С. 352.

[202] Гутник А. В. Повідомлення про підозру у вчиненні ідеологічного та культурно-освітнього колабораціонізму: аналіз дотримання вимог ст. 277 КПК. Military offences and war crimes: background, theory and practice: collective monograph; ed. by V. M. Stratonov. Riga, Latvia: «Baltija Publishing», 2023. P. 260.

[203] Повідомлення про підозру Мусієнку Д. М. та повістки про виклик на 01.11.2023, 02.11.2023, 03.11.2023. *Офіс Генерального прокурора:* вебсайт. URL: https://www.gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-musijenku-dm-ta-povistki-pro-viklik-na-01112023-02112023-03112023; Повідомлення про підозру та повістки про виклик Хитун Л. В. на 01.11.2023, 02.11.2023, 03.11.2023. *Офіс Генерального прокурора: вебсайт*. URL: https://www.gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-xitun-lv

[204] Повідомлення про підозру Кусік Маргариті Вікторівні, пам'ятка про процесуальні права та обов'язки підозрюваного та повістки про виклик підозрюваної Кусік М. В. на 25.10.2023, 26.10.2023, 27.10.2023. *Офіс Генерального прокурора:* вебсайт. URL: https://www.

Цих порушень можна уникнути, якщо: 1) дотримуватися вимог ст. 277 КПК щодо змісту письмового повідомлення про підозру; 2) дотримуватися вимог Порядку[205] щодо приховування персональних даних потерпілого, свідка; 3) Перевіряти публікацію на вебсайті ОГП після публікації.
2.2.4. Невідповідність компетенції слідчого
2.2.5. Особа є неповнолітньою (наявна заборона у КПК)
3. Проблеми, які виникають під час розгляду клопотання в суді
3.1. Непідтримання клопотання в суді
«Прокурор та слідчий в судове засідання неодноразово не з'являлися та клопотання не підтримали. Тому слідчий суддя вважає, що клопотання не підлягає задоволенню, що не позбавляє їх права в подальшому звернутися з аналогічним клопотанням»[206].
Прибувати на засідання для підтримання клопотання або подавати клопотання про розгляд клопотання без участі сторони обвинувачення.
3.2. Неналежний виклик у суд
Особу вважають належним чином ознайомленою зі змістом судових повісток, а отже, обізнаною про здійснюване судом щодо неї кримінальне провадження в порядку ч. 3 ст. 323 КПК (in absentia), якщо місцевий суд повідомляв їй про судові засідання (у тому числі про судове засідання, на якому було проголошено вирок) шляхом розміщення оголошення на вебпорталі «Судова влада України» та в газеті «Урядовий кур'єр»[207].
Про належний виклик також див. цю таблицю вище – блоки 1.1. та 2.2.2.
3.3. Порушення, пов'язані із зупиненням строку досудового розслідування
«досудове розслідування зупинене та на час розгляду цього клопотання не було відновлено, а проведення будь-яких слідчих дій після зупинення досудового розслідування прямо заборонено нормами КПК»[208].

gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-kusik-mv-pamyatka-pro-procesualni-prava-ta-obovyazki-pidozryuvanoyi-kusik-mv-ta-povistki-pro-viklik-na-25102023-26102023-27102023

[205] Про затвердження Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження та на офіційному вебсайті Офіса Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування: Наказ Офіса Ген. прокурора від 30.05.2023 р. № 141. URL: https://zakon.rada.gov.ua/laws/show/v0141905-23#Text

[206] Ухвала Новомосковського міськрайонного суду Дніпропетровської області від 05.12.2022 у справі № 183/6587/22. URL: https://reyestr.court.gov.ua/Review/107959506

[207] Постанова ВС від 01.04.2021 у справі № 759/2992/17 (провадження № 51-3360км20). URL: https://reyestr.court.gov.ua/Review/95946565

[208] Ухвала Красногвардійського районного суду м. Дніпропетровська від 20.10.2022 у справі № 204/8197/22. URL: https://reyestr.court.gov.ua/Review/107223204#

«виклик підозрюваного здійснений неналежним чином, його неявка … під час зупиненого досудового розслідування не може вважатися ухиленням від явки на виклик до слідчого»[209].

«Аналізуючи наведені норми та враховуючи, що клопотання надійшло після закінчення строку досудового розслідування, слідчий суддя взагалі позбавлений можливості вирішувати поставлені слідчим питання поза межами, встановленими Законом (КПК. – Авт.), строку досудового розслідування»[210].

Важливо дотримуватися глави 23 КПК «Зупинення досудового розслідування».

4. Проблеми, які можуть виникнути на будь-якому етапі кримінального провадження (у тому числі у судовому розгляді)

4.1 Порушення права на захист

Незалучення захисника[211]

В ухвалі суду[212] немає жодної згадки про захисника (чи було його залучено? коли та ким? чи брав він участь у засіданні під час розгляду клопотання про здійснення спеціального досудового розслідування?).

Пасивність адвоката

«Пасивна участь захисника у кримінальному провадженні за процедурою «in absentia» є істотним порушенням кримінального процесуального закону, порушенням права на захист, що перешкоджає суду ухвалити законне й обґрунтоване судове рішення. Пасивною участю захисника, зокрема, можна вважати незаявлення ним жодних заяв чи клопотань, спрямованих на захист обвинуваченого, згода з усіма клопотаннями сторони обвинувачення, відсутність інформації про зустрічі з обвинуваченим, неузгодження з ним лінії захисту від обвинувачення»[213].

1. Надання професійної правової допомоги та реалізації права на захист від кримінального обвинувачення є конституційним професійним обов'язком адвоката.

2. У провадженнях «in absentia» адвокат зобов'язаний виходити із необхідності забезпечити клієнту право на захист, а також із пріоритетності інтересів такого підзахисного.

3. Неможливість виконувати при цьому інші правила адвокатської етики (наприклад, інформування адвокатом клієнта щодо ведення дорученої йому справи) не зумовлює обов'язкової неможливості здійснювати захист особи від кримінального обвинувачення за її відсутності.

---

[209] Ухвала Шепетівського міськрайонного суду від 28.04.2022 у справі № 688/3180/21. URL: https://reyestr.court.gov.ua/Review/104146087

[210] Ухвала Печерського районного суду м. Києва від 13.01.2022 у справі № 757/63763/21-к. URL: https://reyestr.court.gov.ua/Review/104512262

[211] Коць Є. П. Проблемні аспекти залучення та участі захисника під час спеціального досудового розслідування (in absentia). *Аналітично-порівняльне правознавство*: електрон. наук. видання. 2023. № 2. С. 345. DOI: https://doi.org/10.24144/2788-6018.2023.02.59

[212] Ухвала Комунарського районного суду м. Запоріжжя від 03.04.2023 у справі № 333/2408/23. URL: https://reyestr.court.gov.ua/Review/109981556

[213] Постанова ВС від 13.06.2019 р. у справі № 607/9498/16-к (провадження № 51-2422км18). URL: http://reyestr.court.gov.ua/Review/82492181

4. Можливість надання правової (правничої) допомоги адвокат визначає виходячи з конкретних обставин справи та інтересів клієнта у ній[214].
Відмова у клопотанні захисника щодо відкладення розгляду справи й надання часу для підготовки виступу в судових дебатах
⛔ Якщо у спеціальному судовому провадженні (in absentia) суд відмовив задовольнити клопотання сторони захисту про відкладення розгляду справи й надання часу для підготовки виступу в судових дебатах для належної організації та непорушення права на захист його підзахисного без належного і розумного обґрунтування своєї відмови, посилаючись виключно на необхідність забезпечення безперервності судового розгляду (ст. 322 КПК) і недоцільність витрачання прокурором бюджетних коштів на розміщення оголошення, він порушив принципи юридичної рівності, змагальності та справедливості судового розгляду, що не узгоджується зі ст. 6 Конвенції про захист прав людини і основоположних свобод[215].
4.2. Оскарження рішення, повторний розгляд справи
⛔ В українському законодавстві досі не врегульовано питання надання обвинуваченому реальної можливості скористатися наданим законодавцем правом на оскарження вироку у справі, розглянутій за його відсутності[216].
➕ У КПК України слід передбачити обов'язкову вимогу щодо виклику обвинуваченого у підготовче судове засідання, публікації кінцевого судового рішення у справі (in absentia), розширенні можливості, умови, підстави та процедуру повторного розгляду судової справи в загальному порядку, або відновлення провадження по справі судом першої інстанції[217].
4.3. «Зазіхання» на принцип змагальності

Важливо! Попри усі наявні практичні проблеми, які у значній кількості трапляються у перебігу in absentia та описані вище, все ж практики цілком слушно стверджують про те, що:

1) злочини продовжують вчинятися на окупованих територіях, до яких немає доступу;

---

[214] Про затвердження роз'яснення щодо участі адвокатів у кримінальних провадженнях за відсутності підозрюваного, обвинуваченого: рішення Ради адвокатів України від 27.12.2022 № 183. *Національна асоціація адвокатів України*: вебсайт. URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2022-12-27-r-shennya-rau-183_63d129b90a174.pdf

[215] Постанова ВС від 19.07.2022 у справі № 727/13085/18 (провадження № 51-10250км18). URL: https://reyestr.court.gov.ua/Review/105359481

[216] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 08.06.2023. *JustTalk: вебсайт*. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

[217] Жидков В. Л., Жила О. Б. Застосування спеціальної процедури притягнення до кримінальної відповідальності (in absentia) за колабораційну діяльність (публікація стала можливою завдяки щедрій підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID) в рамках Програми «Права людини в дії», яка виконується Українською Гельсінською спілкою з прав людини). Київ. 2023. С. 5. URL: https://www.helsinki.org.ua/wp-content/uploads/2023/06/Zastosuvannia-spetsialnoi-protsedury-prytiahnennia-do-kryminalnoi-vidpovidalnosti-in-absentia-za-kolaboratsiynu-diialnist.pdf

2) є загроза втрати доказової бази, тому «…необхідні слідчі дії здійснюються відразу»… Дистанційне збирання доказів забезпечується, серед іншого, й отриманням інформації з відкритих джерел. Також така діяльність дозволяє «запускати певні компенсаційні механізми для потерпілої особи»[218].

Застосування процедури in absentia, зокрема у провадженнях щодо злочинів проти миру, безпеки та міжнародного правопорядку, має здійснюватися у чіткій відповідності до вимог чинного КПК України. *Формувати доказову базу слід лише із належних та допустимих доказів*[219]. Крім того,

> «…процедури in absentia можуть вважатися законними та справедливими, лише якщо вони передбачають гарантії, визначені міжнародним правом»[220].

Про дотримання яких обов'язкових гарантій та умов йдеться?



[218] Рік розслідування воєнних злочинів. Інтерв'ю з Юрієм Бєлоусовим, начальником Департаменту війни ОГП [текстова версія]. 02.03.2023. *Justtalk:* вебсайт. URL: https://justtalk.com.ua/post/rik-rozsliduvannya-voennih-zlochiniv-intervyu-z-yuriem-belousovim-nachalnikom-departamentu-vijni-ogp-tekstova-versiya

[219] Пріхно А. «Немає жодного сенсу в сотнях вироків без належних доказів», – суддя про воєнні злочини РФ. 14.11.2022. *Судова влада України:* вебсайт. URL: https://court.gov.ua/press/publications/1345639/

[220] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 08.06.2023. *JustTalk:* вебсайт. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

	В іншому випадку є велика ймовірність, що доведеться вести мову про порушення конвенційних прав.

	В українському законодавстві досі не врегульоване питання забезпечення обвинуваченому реальної можливості скористатися наданим законодавцем правом на оскарження судового рішення і мова не лише про вирок у справі, розглянутій за його відсутності.

Важливо! Судове рішення підлягає врученню обвинуваченому (розсилається через органи Мін'юсту), чим начебто *створюється можливість його оскарження* (див. Інструкцію[224]), але *чи справді забезпечується така можливість*? Очевидно, що не завжди, чим «спричиняються додаткові ризики визнання порушення прав сторони процесу, що є ключовим і має особливості у справах, які розглядаються в спеціальному провадженні»[225]. У Резолюції Комітету Міністрів Ради Європи № (75) 11 від 19 січня 1973 року йдеться про важливість саме «*забезпечення оскарження вироку*»[226].

---

[221] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України:* вебсайт. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

[222] Рішення ЄСПЛ «Сейдович проти Італії» (Sejdovic v. Italy). Заява № 56581/00 від 01.03.2006. *Інформац. бюлетень з практики суду 84*. Берез. 2006. Український переклад зроблено в рамках проекту Ради Європи «Подальша підтримка реформи кримінальної юстиції в Україні», за фінансового сприяння уряду Данії. URL: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-179185&filename=CASE%20OF%20SEJDOVIC%20v.%20ITALY%20-%20%5BUkrainian%20Translation%5D%20legal%20summary%20by%20the%20CoE%20Project%20%22Continued%20support%20to%20the%20criminal%20justice%20reform%20in%20Ukraine%22.pdf&logEvent=False

[223] Рішення ЄСПЛ «Санадер проти Хорватії» (Sanader v. Croatia). Заява № 66408/12 від 12.02.2015. Information Note on the Court's case-law 182. February 2015. URL: https://hudoc.echr.coe.int/fre?i=002-10371

[224] Про затвердження Інструкції про порядок здійснення міжнародного співробітництва з питань взаємної правової допомоги, видачі правопорушників (екстрадиції), передачі (прийняття) засуджених осіб, виконання вироків та інших питань міжнародного судового співробітництва у кримінальному провадженні під час судового провадження: Наказ Міністерства юстиції України від 19.08.2019 р. № 2599/5. URL: https://zakon.rada.gov.ua/laws/show/z0956-19#Text

[225] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 08.06.2023. *JustTalk:* вебсайт. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

[226] Резолюція № (75) 11 Комітету Міністрів Ради Європи «Про критерії, які регламентують розгляд, що проводиться за відсутності обвинуваченого» від 19.01.1973. URL: https://rm.coe.int/09000016804f7581

Важливо! Дотримання такого із стандартів Резолюції Комітету Міністрів Ради Європи № (75) 11, як:

> «…період часу для оскарження не повинен починатися раніше, ніж особа, щодо якої винесено вирок, не отримає ефективного повідомлення про винесене судове рішення, якщо тільки не буде встановлено, що особа навмисно прагнула уникнути правосуддя»[227].

Однією зі складових забезпечення загальної справедливості провадження є **забезпечення права на захист.**

Відкритим залишається питання дотримання стандарту Резолюції Комітету Міністрів Ради Європи № (75) 11 від 19 січня 1973 року «Про критерії, які регламентують розгляд, що проводиться за відсутності обвинуваченого», зокрема такого із них: наскільки реально захист «впливає на процес збору доказів?».

Констатуємо ряд правильних та своєчасних ініціатив для роз'яснення адвокатам особливостей їх участі у цій категорії проваджень[228] та підкреслення розуміння того, що «…надання професійної правничої допомоги є їх обов'язком через ексклюзивний конституційний статус»[229].

Аналіз судової практики за наслідком розгляду клопотання про здійснення спеціального досудового розслідування підтверджує пасивність адвокатів під час розгляду клопотань без участі підозрюваного. Допускаються й інші порушення права на захист: не вживаються заходи щодо залучення захисника або ж захисник підтримує позицію сторони обвинувачення тощо[230].

Важливо! Є ймовірність, що опоненти будуть проводити активну кампанію задля обґрунтування власних контраргументів.

---

[227] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 8.06.2023. *JustTalk: вебсайт*. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

[228] Про затвердження роз'яснення щодо втручання органів БПД до правової позиції адвоката при розгляді клопотання про обрання запобіжного заходу: рішення Ради адвокатів України від 08.08.2022 № 70. *Нац. асоціація адвокатів України*: вебсайт. URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2022-08-02-r-shennya-rau-70_62fcfd46cb86e.pdf; Про затвердження роз'яснення щодо участі адвокатів у кримінальних провадженнях за відсутності підозрюваного, обвинуваченого: рішення Ради адвокатів України від 27.12.2022 № 183. *Нац. асоціація адвокатів України:* вебсайт. URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2022-12-27-r-shennya-rau-183_63d129b90a174.pdf

[229] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України: вебсайт*. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

[230] Коць Є. П. Проблемні аспекти залучення та участі захисника під час спеціального досудового розслідування (in absentia). *Аналітично-порівняльне правознавство*: електрон. наук. видання. 2023. № 2. С. 345. DOI: https://doi.org/10.24144/2788-6018.2023.02.59

Отож закликаємо дотримуватися рекомендації «…застосовувати особливий порядок **«in absentia»** під час досудового розслідування і в ході судового розгляду **«лише у виключних випадках і за наявності потужної доказової бази»**[231].

2.4. Заочне судочинство у міжнародному праві та у процесуальному праві інших країнах

«…міжнародне право з обережністю ставиться до заочного судочинства»[232].

Чи допустимі заочні провадження щодо найтяжчих міжнародних злочинів?

Важливо! «На міжнародній арені після Другої світової війни, Нюрнберзького міжнародного військового трибуналу такі заочні провадження не застосовувалися. Заочне судочинство було заборонено у справах колишньої Югославії та Руанди, у Спеціальному суді по Сьєрра-Леоне, а також у МКС. Заочне судочинство було відновлено під час Спеціального трибуналу по Лівану, який відкрився у 2009 році»[233].

Про міжнародний досвід африканських держав та інших країн, як і про особливості притягнення до відповідальності за найтяжчі міжнародні злочини див. рекомендації африканських організацій громадянського суспільства та експертів із правових питань[234], аналітичні та інформаційні матеріали щодо цього питання[235], а також в українському перекладі «Options for justice a handbook for designing accountability mechanisms for grave crimes» = «Вибір заради справедливості: посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини. Т. 2…»[236].

[231] Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані … .

[232] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України*: вебсайт. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

[233] Там само.

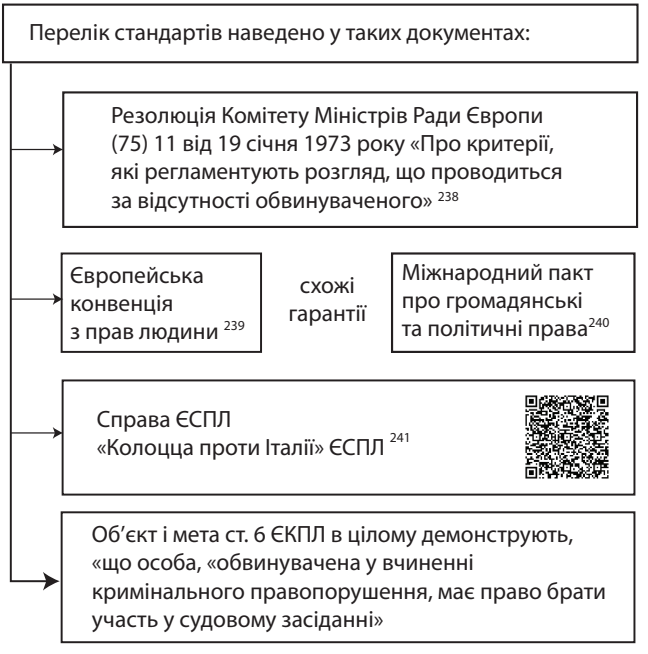
[234] Наприклад, рекомендації зустрічі 24 експертів у жовтні 2013 року для обговорення «Просування відповідальності за міжнародні злочини в Африці», у: Всеафриканський союз адвокатів, «Аналітична записка № 5, Міжнародне кримінальне правосуддя в Африці». 17 лип. 2013 р. С. 1–2.

[235] Seeking Justice or Shielding Suspects? An analysis of the Malabo Protocol on the African Court. 23.11.2016. *Kenyans for Peace with Truth and Justice (KPTJ):* вебсайт. С. 18. URL: http://kptj.africog.org/seeking-justice-or-shielding-suspects-an-analysis-of-the-malabo-protocol-on-theafrican-court; Max du Plessis Implications of the AU Decision to Give the African Court Jurisdiction Over International Crimes. *Institute for Security Studies:* вебсайт. № 235. URL: https://issafrica.s3.amazonaws.com/site/uploads/Paper235-AfricaCourt.pdf

[236] Вибір заради справедливості: посіб. зі створення механізмів притягнення до відповідальності за найтяжчі злочини. Т. 2 / пер. О. Бондаренко; заг. ред. Р. Мартиновського, Л. Мороз. Переклад та видання здійснене за підтримки Програми «Права людини і правосуддя» Міжнародного фонду «Відродження». 2018. С. 13. URL: https://www.irf.ua/wp-content/uploads/2020/06/tom_ii_web.pdf

Які встановлено міжнародні стандарти розслідування, що застосовні також до заочних проваджень щодо найтяжчих міжнародних злочинів?

Міжнародно-правові рамки слідують із положень «...статті 14 (3) (d) Міжнародного пакту про громадянські та політичні права...» і «...передбачають, що особа, якій висунуто кримінальне обвинувачення, має право бути поінформованою про обвинувачення і бути судимою у власній присутності. Ці права є мінімальною гарантією справедливості й застосовуються на всіх стадіях судового розгляду»[237].



[237] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України:* вебсайт. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

[238] Резолюція № (75) 11 Комітету Міністрів Ради Європи «Про критерії, які регламентують розгляд, що проводиться за відсутності обвинуваченого» від 19.01.1973. URL: https://rm.coe.int/09000016804f7581

[239] Європейська конвенція про захист прав людини і основоположних свобод: міжнар. докум. 04.11.1950. URL: http://zakon4.rada.gov.ua/laws/show/995_004

[240] Міжнародний пакт про громадянські і політичні права: міжнар. докум. 19.10.73. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

[241] Рішення ЄСПЛ у справі «Колоцца проти Італії («Colozza v. Italy». Заява № 9024/80 від 12.02.1985. URL: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-57462&filename=CASE%20OF%20 COLOZZA%20v.%20ITALY.docx&logEvent=False

> «Міжнародні суди одностайно наголошують, що держава зобов'язана застосувати всі наявні засоби, щоб підозрюваний був належним чином поінформований про кримінальне провадження проти нього. Це відображено в рішеннях Європейського суду з прав людини (Sanader v. Croatia, Sejdovic v. Italy, Stoyanov v. Bulgaria), Комітету ООН з прав людини (Мбенге проти Заіру) та МКС (справа проти Саіфа Аль-Іслама Гаддафі)»[242].

Яким є заочне судочинство в інших країнах?

«…Згідно з позицією Верховного суду США заочний розгляд справи *неможливий* без присутності обвинуваченого на початку судового розгляду»[243]. Заочне судочинство допускається й у інших країнах, але *з обмеженими варіаціями щодо покарань* і, як правило, йдеться про невеликі терміни позбавлення волі, або ж таке покарання взагалі не прийнятне у цій категорії проваджень[244]. Отож, на часі є впровадження необхідних стандартів правосуддя[245].

2.5. Потенційні порушення, які можуть бути допущені у перебігу «роботи» з відкритими джерелами. Заходи на їх випередження

Порушення через нерозуміння «меж» відкритих джерел

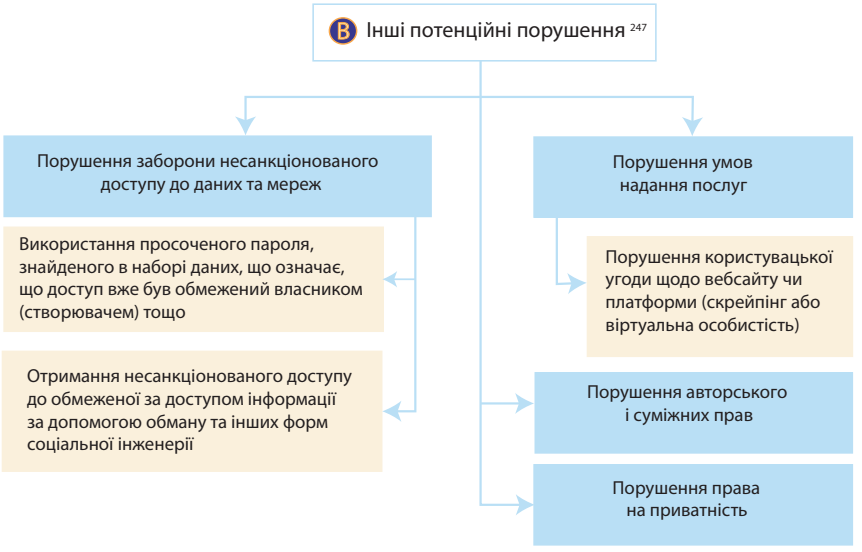
«Межі» відкритих джерел[246]

Джерело є відкрите	Не належить до відкритих джерел
Є можливість за допомогою безплатних веббраузерів переходити на відповідний сайт, і такі процеси відкриті для всіх користувачів у юрисдикціях, в яких доступ є законним й під час доступу до нього чи перегляду не порушуються заходи конфіденційності та безпеки	Конфіденційна, засекречена чи іншим чином захищена законом інформація у вільному (відкритому) доступі
Онлайн-контент купили для цілей розслідування (отримали як платну послугу, яка доступна для всіх представників громадськості)	Послуга, доступ до якої мають лише певні групи (правоохоронні органи, приватні слідчі)
Надсилання запитів та отримання відповіді	Взаємодія із зовнішніми джерелами (сервіс обміну повідомленнями, чат, форум, електронна пошта)

[242] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 08.06.2023. *JustTalk:* вебсайт. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

[243] Задоя К. Перше кримінальне провадження в США щодо воєнних злочинів, вчинених в Україні. 01.02.2024. *Глобальна ініціатива T4P (Трибунал для Путіна):* вебсайт. URL: https://t4pua.org/2281

[244] Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13.12.2023. *Нац. асоціація адвокатів України:* вебсайт. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html



Чи буде за Протоколом Берклі порушенням використання інформації із тіньового Інтернету у сферу «відкритого доступу»?

Цифрова інформація може бути доступною для тих, хто має спеціалізовані технічні навички та пройшов навчання, які можуть отримати доступ до мереж і даних, недоступних для звичайної людини, або доступ до яких вона навряд чи матиме[248]. Мова йде про те, що Інтернет складається з відкритої (Surface Web, або «поверхневий веб») та прихованої (Deep Web, який включає Dark Web) частин[249]. Surface Web доступний всім, у ньому здійснюють пошук Google та інші популярні пошукові сервіси, натомість Deep Web не проіндексована стандартними пошуковими системами. Dark Web – це частина Deep Web, але доступ до нього можливий тільки через спеціальні браузери (наприклад, Tor, I2P), які забезпечують анонімність та невідстежуваність користувача[250].

---

[245] Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 8.06.2023. *JustTalk*: вебсайт. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

[246] Протокол Берклі … . С. 25, 26.

[247] Там само. С. 51, п. 63. С. 52, п. 65.

[248] Там само. С. 25, п. 14.

[249] Савчук Т. Dark Web: прихована сторона інтернету, яка поширена в Україні. 07.10.2017. *Радіо Свобода:* вебсайт. URL: https://www.radiosvoboda.org/a/28778448.html

[250] Chris Hoofnagle. Dark Web Intelligence: Methods & Legal Issues. *BCLT Research2Practice*. July 16, 2020. Presentation. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/darknet_intel.pdf

Так, Протокол Берклі включає можливість використання інформації із тіньового Інтернету у сферу «відкритого доступу», доки не відбувається несанкціонованого доступу до інформації[251], наприклад, використання вразливості або викрадених облікових записів[252].

Чи забороняє Протокол Берклі скрейпінг або віртуальну особистість?

Важливо! Порушення умов надання послуг, як от користувацької угоди щодо вебсайту або платформи (скрейпінг або віртуальна особистість тощо)[253] матиме вплив на можливість використовувати у доказуванні отриманої у його перебігу інформації, якщо це передбачено у конкретній юрисдикції (тому потрібно завчасно визначитися з юрисдикцією та з'ясувати стан справ із цим). Варто також завчасно ознайомитися із умовами використання (як от Facebook тощо).

Чи є ймовірність порушення авторських прав під час роботи з відкритими джерелами цифрової інформації?

> **Захист авторських прав** посідає у царині розслідувань з використанням відкритих цифрових даних не останнє місце, а порушення авторських прав є високоймовірним.

Під час досудового розслідування може збиратися цифровий контент, інформація з баз даних, вебсайтів, творів, у тому числі створених із використанням ШІ, та інша інформація, на яку поширюється сфера авторського права та/або суміжних прав.

Важливо! Україна – п'ятнадцята країна, що приєдналася до ініціативи WIPO (йдеться про наповнення платформи WIPO ALERT для протидії роботі вебсайтів, на яких порушуються права інтелектуальної власності)[254], 21 березня 2024 року Мінекономіки ухвалило відповідний Наказ[255].

---

[251] Протокол Берклі … . С. 25, п. 14.

[252] Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources. Cybersecurity Unit. Computer Crime & Intellectual Property Section. Criminal Division U.S. Department of Justice. February 2020. P. 3. URL: https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl

[253] Протокол Берклі … . С. 52, п. 65.

[254] Україна розширила інструменти захисту авторських прав в інтернет-просторі. 30.03.2024. URL: https://yaizakon.com.ua/ukrayina-rozshirila-instrumenti-zahistu-avtorskih-prav-v-internet-prostori/

[255] Там само.

Важливо! «У багатьох країнах оригінальні твори, зафіксовані на матеріальних носіях, автоматично захищаються авторським правом… Твір має бути *оригінальним* і *зафіксованим* на фізичному носії»[256]. Варто констатувати, що є кардинально протилежні прецеденти із таких вигранних позовів[257].

В Україні ж наявний базовий Закон[258], яким, серед іншого контекстуально важливого, у п. 3 ч. 1 ст. 22 передбачено, що до випадків вільного використання творів (без дозволу суб'єктів авторського права, безоплатно та без зазначення імені автора і джерела запозичення) належить і такий, як відтворення творів для забезпечення судового, адміністративного, кримінального провадження в обсязі, що відповідає поставленій меті»[259]. Поряд з таким станом справ авторське право та суміжні права підпадають під правову охорону, а у разі їх порушення настає кримінальна відповідальність, а «…також фінансування таких дій, якщо це завдало матеріальної шкоди у значному розмірі» (ст. 176 КК України[260]). Аналізом п. 31 ППВСУ № 5 від 04.06.2010 «Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав»[261] встановлено, що розміщення творів у мережі «Інтернет» у вигляді, доступному для публічного використання, є правомірним лише з дозволу автора чи іншої особи, яка має авторське право; відтворенням є виготовлення одного або більше примірників твору, відеограми, фонограми в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер[262]. Касаційний цивільний суд Верховного Суду буквально

[256] Що таке авторське право? Довідковий центр. Youtube. Довідка. URL: https://support.google.com/youtube/answer/2797466?sjid=6449976278248575575-EU#zippy=%2Cякі-типи-творів-захищаються-авторським-правом

[257] Петрів О., Спесивцева О. Автори проти штучного інтелекту: на чийому боці суд? 15.12.2023. *ЦЕДЕМ*: вебсайт. URL: https://cedem.org.ua/news/avtory-proty-shi-na-chyjomu-botsi-cud/; Деґе Ш. Чи може штучний інтелект конкурувати з митцями? 06.02.2023. *Deutsche Welle*: вебсайт. URL: https://www.dw.com/uk/ci-moze-stucnij-intelekt-konkuruvati-z-mitcami/a-64602090; Басиста І. В., Удовенко Ж. В., Кулинич М.-М. А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Наук. вісн. Ужгород. нац. ун-ту*. Сер. ПРАВО. 2024. Вип. 80. Ч. 3. С. 19–38. https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf; Кішка, що прославилася в інтернеті завдяки своєму знаменитому похмурому вигляду, отримала 710 тисяч доларів США у справі про захист авторських прав у федеральному суді штату Каліфорнія. 25.01.2018. *BBC Україна*: вебсайт. URL: https://www.bbc.com/ukrainian/other-news-42815049

[258] Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-20 (редакція від 15.04.2023). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

[259] Там само.

[260] Кримінальний кодекс України від 05.04.2001 № 4651-VI (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/2341-14?f

[261] Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав: Постанова Пленуму Верховного суду України від 04.06.2010 № 5. URL: https://zakon.rada.gov.ua/laws/show/v0005700-10#Text

[262] Там само.

17 січня 2024 року розглядав справу авторки автореферату дисертації, який без її дозволу розмістив університет (справа № 308/7570/18-ц, провадження № 61-7051св23[263]). У коментарі слушно зазначено, що серед іншого Судом також було підкреслено про те, що «...використання об'єкта права інтелектуальної власності іншою особою здійснюється з дозволу особи, яка має виключне право дозволяти використання об'єкта права інтелектуальної власності, *крім випадків правомірного використання без такого дозволу, передбачених цим Кодексом та іншим законом* (ч. 3 ст. 426 ЦК України)...»[264]. «Як виняток допускається правомірне використання твору як об'єкта права інтелектуальної власності без дозволу особи, яка має виключне право дозволяти використання об'єкта права інтелектуальної власності, у разі, якщо це передбачено відповідною нормою закону»[265].

Як названо аналогічний «блок» у Протоколі Берклі та де шукати його вимоги?

У Протоколі Берклі такий блок отримав назву «Закони про інтелектуальну власність» (п. 66).

Важливо! Слідчі повинні знати про всі дозволи на інтелектуальну власність щодо тієї інформації, яку вони зібрали під час розслідування. У юрисдикціях такі вимоги можуть варіюватися. Принаймні всі дотримуються однієї – *захист авторських прав для творця контенту*, який і має надати відповідну згоду на використання. Юрисдикції нерідко встановлюють і виняток для «добросовісного використання» або «торгової чесності»[266].

Якщо до контенту застосовуються безкоштовні ліцензії, то слід дотримуватися їхніх умов, бо такий контент для власного використання виробив певні дозвільні умови[267].

---

[263] Постанова Другої судової палати Касаційного цивільного суду Верховного Суду від 17.01.2024 у справі № 308/7570/18-ц, провадження № 61-7051св23. URL: https://reyestr.court.gov.ua/Review/117473137

[264] Наталя Мамченко. Цитування чи плагіат: Верховний Суд розглянув справу авторки автореферату дисертації, який без її дозволу розмістив університет. 11.03.2024. *Судово-юридична газета*. URL: https://sud.ua/uk/news/publication/295198-tsitirovanie-ili-plagiat-verkhovnyy-sud-rassmotrel-delo-avtora-avtoreferata-dissertatsii-kotoryy-bez-ee-razresheniya-razmestil-universitet?fbclid=IwAR29XWWUrQFRC7Flx6IfwVaTrUQue_t1PjeJJyHQf8WBZD06iplJCAc0X7E

[265] Постанова Другої судової палати Касаційного цивільного суду Верховного Суду від 17.01.2024 у справі № 308/7570/18-ц, провадження № 61-7051св23. URL: https://reyestr.court.gov.ua/Review/117473137

[266] Протокол Берклі … . С. 53.

[267] Там само. С. 53.

Перед *констатацією порушення авторських прав* насамперед треба з'ясувати, чи на такий контент поширюється принцип «добросовісного використання». Ще на етапі досудового оскарження порушення авторських прав низка компаній (Instagram[268], Facebook[269], Tik Tok[270], YouTube[271] тощо) розробили власні правила у випадку встановлення користувачем порушення авторського права[272].

Що слід розуміти під «цифровими правами» та порушенням права на приватність?

> Дотримання цифрових прав. Цифрова техніка – це об'єкт підвищеної «концентрації» прав людини. Декількома простими маніпуляціями з пристроєм можна одночасно обмежити, а то й порушити низку прав. Наявний «електронний (цифровий) імунітет» категорій осіб, традиційно наділених правом на мовчання[273].

У Протоколі Берклі йдеться й про **право на недоторканність приватного життя і захист даних** (зокрема й персональних). Отож, слідчі повинні знати глобальні межі захисту даних, безпеки даних та обміну даними (див. п. 61–63).

Також йдеться й про **інформаційну конфіденційність**, яка охоплює інформацію, що існує або може бути отримана про людину[274].

> Автори вже задавалися питанням про визначення права, яким загалом охороняються цифрові дані, та встановили, що це як право на приватність, так і спеціальне право на гарантування цілісності та конфіденційності *інформаційно-технологічних систем* як результат адаптації традиційного права до особливостей інформаційних технологій[275].

Важливо! На перший погляд у процесі роботи з відкритими джерелами названі права обмежені чи порушені бути не можуть,

[268] Авторське право. Довідковий центр. *Instagram*: вебсайт. URL: https://www.facebook.com/help/instagram/126382350847838

[269] Там само.

[270] Intellectual Property Policy. *Tiktok*: вебсайт. Last updated: June 7. 2021. URL: https://www.tiktok.com/legal/page/global/copyright-policy/en

[271] Правила й вказівки. *YouTube*: вебсайт. URL: https://www.youtube.com/intl/uk_ALL/creators/how-things-work/policies-guidelines/

[272] Як надіслати запит на видалення відео через порушення авторських прав. Довідковий центр. Youtube Довідка. URL: https://support.google.com/youtube/answer/2807622?hl=uk

[273] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 68.

[274] Протокол Берклі … . 2020. С. 50, п. 61.

[275] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 68–69.

але це лише у тому випадку, якщо не було допущено помилок під час розрізнення джерела та інформації та не допущено інших порушень. Отже, розуміння такої межі та її дотримання є надважливим, інакше є очевидна ймовірність порушення означених прав.

> ***Наприклад***, порушення недоторканності приватного життя, яка часто піднімається нагору у контексті цифрової інформації, є однією з небагатьох підстав, за якими судді можуть виключити докази в МКС (див. Римський статут, ст. 69 (7))[276].

Важливо! ЄСПЛ надає певні окремі тлумачення законів про недоторканність приватного життя із швидко зростаючим набором судової практики, що стосується питань цифрових прав[277]. У перебігу навчання на онлайн-курсі «Інтернет і цифрові права людини»[278] для учасників навчання було запропоновано підбірку такої судової практики, з аналізу якої можна констатувати, що особи звертаються до ЄСПЛ переважно з метою захисту порушених прав, які передбачені ст. 8 ЄКПЛ («Право на повагу до приватного і сімейного життя»), або ст. 10 ЄКСПЛ («Свобода вираження поглядів»).

Проблема, яку вирішував ЄСПЛ	**Справа та посилання на неї**	
Застосування заходів блокування доступу до Інтернету	(Ахмет Їлдірім проти Туреччини (Ahmet Yıldırım v. Turkey)[279]	
	Акденіз проти Туреччини (Akdeniz v. Turkey)[280]	
	Ченгіз проти Туреччини (Cengiz and Others v. Turkey)[281]	

[276] Протокол Берклі … . С. 50, п. 62.

[277] Протокол Берклі … . С. 50–51, п. 62.

[278] Створений за підтримки Американської асоціації юристів, Ініціативи з верховенства права (ABA ROLI в Україні) в рамках програми «Сприяння Інтернет-свободі в Україні» (див. https://academy.legalaid.gov.ua/course/view.php?id=166)

[279] Рішення ЄСПЛ у справі «Ахмет Їлдірім проти Туреччини» (Ahmet Yıldırım v. Turkey). Заява № 3111/10 від 18.12.2012. URL: https://hudoc.echr.coe.int/eng-press?i=003-4202780-4985142

[280] Рішення ЄСПЛ у справі «Акденіз проти Туреччини» (Akdeniz v. Turkey). Заява № 20877/10 від 11.03.2014. URL: https://hudoc.echr.coe.int/eng?i=001-142383

[281] Рішення ЄСПЛ у справі «Ченгіз проти Туреччини» (Cengiz and Others v. Turkey). Заява № 48226/10, № 14027/11 від 1.12.2015. URL: https://hudoc.echr.coe.int/eng-press?i=003-5241080-6502267

Застосування заходів блокування доступу до Інтернету	Владімір Харітонов проти Росії (Vladimir Kharitonov v. Russia)[282]	
	«ООО Флавус та інші проти Росії» (OOO Flavus and Others v. Russia)[283]	
	Булгаков проти Росії (Bulgakov v. Russia)[284]	
	Енгельс проти Росії (Engels v. Russia)[285]	
	Вікімедія проти Туреччини (Wikimedia Foundation, Inc. v. Turkey)[286]	
	Таганрог ЛРО проти Росії 2 (Taganrog LRO and Others v. Russia 2)[287]	
Обмеження доступу засуджених до певних сайтів в Інтернеті[288]	Калда проти Естонії (Kalda v. Estonia)[289]	
	Рамазан Демір проти Туреччини (Ramazan Demir v. Turkey)[290]	
	Янковскіс проти Литви (Jankovskis v. Lithuania)[291]	

[282] Рішення ЄСПЛ у справі «Владімір Харітонов проти Росії» (Vladimir Kharitonov v. Russia). Заява № 10795/14 від 23.06.2020. URL: https://hudoc.echr.coe.int/eng?i=001-203177

[283] Рішення ЄСПЛ у справі «ООО Флавус та інші проти Росії» (OOO Flavus and Others v. Russia). Заява № 12468/15 від 23.06.2020. URL: https://hudoc.echr.coe.int/eng?i=001-203178

[284] Рішення ЄСПЛ у справі «Булгаков проти Росії» (Bulgakov v. Russia). Заява № 20159/15 від 23.06.2020. URL: https://hudoc.echr.coe.int/eng?i=001-203181

[285] Рішення ЄСПЛ у справі «Енгельс проти Росії» (Engels v. Russia). Заява № 61919/16 від 23.06.2020. URL: https://hudoc.echr.coe.int/eng?i=001-203180

[286] Рішення ЄСПЛ у справі «Вікімедія проти Туреччини» (Wikimedia Foundation, Inc. v. Turkey). Заява № 25479/19 від 1.03.2022. URL: https://hudoc.echr.coe.int/eng?i=001-216677

[287] Рішення ЄСПЛ у справі «Таганрог ЛРО проти Росії 2» (Taganrog LRO and Others v. Russia 2). Заява № 32401/10 від 7.06.2022. URL: https://hudoc.echr.coe.int/eng?i=001-217535

[288] Access to Internet and freedom to receive and impart information and ideas. Factsheet. September 2022. *European Court of Human Rights*: вебсайт. URL: https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf

[289] Рішення ЄСПЛ у справі «Калда проти Естонії» (Kalda v. Estonia). Заява № 17429/10 від 19.12.2016. URL: https://hudoc.echr.coe.int/eng?i=001-160270

[290] Рішення ЄСПЛ у справі «Рамазан Демір проти Туреччини» (Ramazan Demir v. Turkey). Заява № 68550/17 від 9.02.2021. URL: https://hudoc.echr.coe.int/eng?i=001-207804

[291] Рішення ЄСПЛ у справі «Янковскіс проти Литви» (Jankovskis v. Lithuania). Заява № 21575/08 від 17.12.2017. URL: https://hudoc.echr.coe.int/eng?i=002-11349

Зловживанням правом на свободу вираження поглядів, що полягає у неповазі до жертв збройних конфліктів	Вільямсон проти Німеччини (Williamson against Germany)[292]	
	Пасторс проти Німеччини (Pastörs v. Germany)[293]	
Пошук балансу між захистом приватного життя та свободи вираження поглядів	Фон Ганновер проти Німеччини (Von Hannover v. Germany)[294]	
	Фон Ганновер проти Німеччини (№ 2) (Von Hannover v. Germany (№ 2))[295]	
	Егіль Ейнарссон проти Ісландії (Egill Einarsson v. Iceland)[296]	
	Кудер та Ашет Філіпачі Асосьє проти Франції (Couderc and Hachette Filipacchi Associés v. France)[297]	
	Родіна проти Латвії (Rodina v. Latvia)[298]	
Визначення меж між свободою вираження поглядів та мовою ворожнечі	Санчез проти Франції (Sanchez v. France) [299]	
	Перінчек проти Швейцарії (Perinçek v. Switzerland)[300]	

[292] Рішення ЄСПЛ у справі «Вільямсон проти Німеччини» (Williamson against Germany). Заява № 64496/17 від 31.01.2019. URL: https://www.echr.com.ua/translation/sprava-vilyamson-proti-nimechchini-pres-reliz/

[293] Рішення ЄСПЛ у справі «Пасторс проти Німеччини» (Pastörs v. Germany). Заява № 55225/14 від 03.10.2019. URL: https://www.echr.com.ua/translation/sprava-pastors-proti-nimechchini/

[294] Рішення ЄСПЛ у справі «Фон Ганновер проти Німеччини» (Von Hannover v. Germany). Заява № 59320/00 від 24.06.2004. URL: https://hudoc.echr.coe.int/eng?i=001-61853

[295] Рішення ЄСПЛ у справі «Фон Ганновер проти Німеччини 2» (Von Hannover v. Germany 2)». Заяви № 40660/08 та 60641/08 від 7.02.2012. URL: https://hudoc.echr.coe.int/eng?i=001-109029

[296] Рішення ЄСПЛ у справі «Егіль Ейнарссон проти Ісландії» (Egill Einarsson v. Iceland). Заява № 24703/15 від 07.11.2017. URL: https://hudoc.echr.coe.int/eng?i=001-178362

[297] Рішення ЄСПЛ у справі «Кудер та Ашет Філіпачі Асосьє проти Франції» (Couderc and Hachette Filipacchi Associés v. France). Заява № 40454/07 від 10.11.2015. URL: https://hudoc.echr.coe.int/eng?i=001-158861

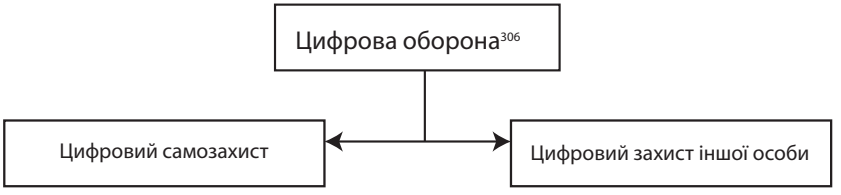
[298] Рішення ЄСПЛ у справі «Родіна проти Латвії» (Rodina v. Latvia). Заяви № 48534/10 та 19532/15 від 14.05.2020. URL: https://hudoc.echr.coe.int/eng?i=001-202437

[299] Рішення ЄСПЛ «Санчез проти Франції» (Sanchez v. France). Заява № 45581/15 від 02.09.21. URL: https://rm.coe.int/affaire-sanchez-c-france-uk-/1680a4df76

[300] Рішення ЄСПЛ у справі «Перінчек проти Швейцарії» (Perinçek V. Switzerland). Заява № 27510/08 від 15.10.2015. URL: https://hudoc.echr.coe.int/eng?i=001-158235

Визначення меж між свободою вираження поглядів та мовою ворожнечі	Стомахін проти Росії (Stomakhin v. Russia)[301]	
	Нікс проти Німеччини (NIX v. GERMANY)[302]	
	Смажич проти Боснії та Герцеговини (Smajic v. Bosnia and Herzegovina)[303]	
	Белькасем проти Бельгії (Belkacem v. Belgium)[304]	
	Лілієнталь проти Ісландії (Lilliendahl v. Iceland)[305]	

Що таке цифрова оборона?



У п. 54 (B) Протоколу Берклі зазначено, що у «…кримінальних справах прокурори зобов'язані розкривати відповідну інформацію (будь-яку інформацію, зібрану в межах розслідування, яка обвинувачує або виправдовує, включаючи інформацію щодо надійності свідків та докази сторони захисту». Із цього правила є й винятки, які розлого за юрисдикціями подано у присторінковій виносці № 76 (B) Протоколу. Берклі. Також слід мати на увазі, що слідчі такі зобов'язання щодо розкриття інформації мають пам'ятати ще на етапі її збору[307], тоді є ймовірність уникнення значної кількості ймовірних порушень у перебігу такої діяльності.

[301] Рішення ЄСПЛ у справі «Стомахін проти Росії» (Stomakhin v. Russia). Заява № 52273/07 від 09.05.2020. URL: https://hudoc.echr.coe.int/eng?i=001-182731
[302] Рішення ЄСПЛ у справі «Нікс проти Німеччини» (Nix v. Germany). Заява № 35285/16 від 13.03.2018. URL: https://hudoc.echr.coe.int/eng?i=001-182241
[303] Рішення ЄСПЛ у справі «Смажич проти Боснії та Герцеговини» (Smajic v. Bosnia and Herzegovina). Заява № 48657/16 від 16.12.2018. URL: https://hudoc.echr.coe.int/eng?i=001-180956
[304] Рішення ЄСПЛ у справі «Белькасем проти Бельгії» (Belkacem v. Belgium). Заява № 34367/14 від 27.06.2017. URL: https://hudoc.echr.coe.int/eng?i=001-175941
[305] Рішення ЄСПЛ У справі «Лілієнталь проти Ісландії» (Lilliendahl vs Iceland). Заява № 29297/18 від 12.05.2020. URL: https://hudoc.echr.coe.int/fre?i=001-203199
[306] Такий підхід запропоновано на С. 142 у власній монографії А. В. Скрипник.
[307] Протокол Берклі … . С. 46.

РОЗДІЛ 3. ЦИФРОВІ ВІДОМОСТІ У ДОКАЗУВАННІ: РІШЕННЯ ЄСПЛ, МКС ТА НАЦІОНАЛЬНИХ СУДІВ

3.1. Практика ЄСПЛ щодо використання цифрових даних з відкритих джерел як доказу у кримінальному провадженні

Яким є чинний підхід ЄСПЛ до цифрових даних з відкритих джерел як форми доказу?

Міжнародний консультант Ради Європи, баристер Джеремі Макбрайд[308] констатував:

> «…Європейському суду ще не довелося розглядати Берклійський протокол… конкретне посилання на концепцію матеріалу з відкритих джерел як форму доказу майже не фігурує в розгляді справ у Європейському суді. Зокрема, такі докази – на відміну від доказів з електронних джерел у цілому – ще не обговорювалися окремо з погляду їхньої прийнятності. Однак у Європейському суді, безсумнівно, є справи, в яких Держави покладаються на соціальні мережі та системи обміну повідомленнями, – які можуть надавати докази, що підпадають під категорію доказів із відкритих джерел, – коли намагаються виправдати дії, які, на думку заявників, порушують їхні права людини. Подібні твердження поки що не увінчалися успіхом, але це пов'язано не з формою, а з їхнім змістом»[309].

В яких рішеннях ЄСПЛ можна відстежити його чинний підхід?

Радимо звернутися до тієї підбірки судових рішень ЄСПЛ, яку здійснив Д. Макбрайд для з'ясування означених ситуацій[310].

---

[308] *Jeremy McBride. Судова палата Монктону у Великій Британії.*

[309] Макбрайд Д. Застосовні міжнародно-правові рамки та стандарти щодо доказів із відкритих та електронних джерел: Європейська конвенція з прав людини. *Council of Europe*: вебсайт. URL: https://rm.coe.int/coe-ukraine-open-uk/1680a6e571

[310] Рішення ЄСПЛ у справі «Монір Лотфі проти Кіпру» (Monir Lotfy v. Cyprus). Заява № 37139/13 від 29.06.2021. URL: https://hudoc.echr.coe.int/eng?i=001-210680; Рішення ЄСПЛ у справі «С. Г. проти Сполученого Королівства» (S. H. v. United Kingdom). Заява № 19956/06 від 15.06.2010. URL: https://www.refworld.org/jurisprudence/caselaw/echr/2010/en/73048; Рішення ЄСПЛ у справі «Айлей та інші проти Росії» (Ayley and Others v. Russia). Заява № 25714/16, № 56328/18 від 03.04.2019. URL: https://hudoc.echr.coe.int/eng?i=001-192578; Рішення ЄСПЛ у справі «Седлецька проти України» (Sedletska v. Ukraine). Заява № 42634/18 від 01.04.2021. URL: https://hudoc.echr.coe.int/eng?i=001-208882; Рішення ЄСПЛ у справі «Шенк проти Швейцарії» (Schenk v. Switzerland) [P]. Заява № 10862/84 від 12.07.1988. URL: https://hudoc.echr.coe.int/eng?i=001-76800

Рішення ЄСПЛ	QR-код
«Монір Лотфі проти Кіпру» (Monir Lotfy v. Cyprus)	
«С. Г. проти Сполученого Королівства» (S. H. v. United Kingdom)	
«Айлей та інші проти Росії» (Ayley and Others v. Russia)	
«Седлецька проти України» (Sedletska v. Ukraine)	
«Шенк проти Швейцарії» (Schenk v. Switzerland)	



«Проте в жодному з випадків не було зроблено припущення, що для національних судів було б принципово недоречним покладатися на докази, отримані із соціальних мереж і систем обміну повідомленнями»[311].

Чи містить ЄКПЛ правила допустимості доказів?

Д. Макбрайд звернув увагу, що ЄКПЛ не містить правил допустимості доказів, а ці питання підпадають під дотримання вимог національного законодавства. Окрему позицію у таких провадженнях посідає роль спеціалістів та експертів, що цей фахівець продемонстрував на прикладі справи «Грузія проти Росії (II)» (Georgia v. Russia (II)[312].

Які складові вже «викликали занепокоєння» в ЄСПЛ та релевантні також щодо цифрових доказів з відкритих джерел?

Серед тієї сукупності складових, які «можуть викликати занепокоєння» у ЄСПЛ і щодо *цифрових доказів з відкритих джерел* Д. Макбрайд виділяє дотримання права на захист, «вагомість» доказів, їх достовірність та надійність, а також наголошується на походженні цих доказів та способах їх отримання, які співвіднесені з автентичністю та надійністю. Підкреслюється, що спосіб отримання може поставити під сумнів надійність доказу[313]. Цей провідний фахівець скеровує нас до наступних рішень ЄСПЛ[314], де всі ці випадки вже мали місце та констатовані як порушення ЄКПЛ.

[311] Макбрайд Д. Зазначений твір.

[312] Там само.

[313] Там само.

[314] Рішення ЄСПЛ у справі «Горватіч проти Хорватії» (Horvatić v. Croatia). Заява № 36044/09 від 17.10.2013. URL: https://hudoc.echr.coe.int/eng?i=001-126915; Рішення ЄСПЛ у справі «Сакіт Західов проти Азербайджану» (Sakit Zahidov v. Azerbaijan). Заява № 51164/07

Рішення ЄСПЛ	QR-код
«Горватіч проти Хорватії» (Horvatić v. Croatia)	
«Сакіт Західов проти Азербайджану» (Sakit Zahidov v. Azerbaijan)	
«Ведува проти Румунії» (Văduva v. Romania)	
«Лопес Рібальда та інші проти Іспанії» (López Ribalda and Others v. Spain)	

Які узагальнені висновки щодо доказування із залученням цифрових даних з відкритих джерел можна сформулювати на підставі аналізу практики ЄСПЛ?

Важливою є наявність чіткої процедури, якої слід дотримуватися під час збирання цифрових доказів з відкритих джерел, включаючи документацію про те, як це відбувається, а також забезпечення того, що ця процедура була дотримана та може бути продемонстрована. Крім того, важливо мати можливість продемонструвати, що немає підстав сумніватися в автентичності матеріалів з відкритих джерел, наприклад через те, що вони були сфабриковані або якимось чином змінені з метою створення очевидно обвинувачувальних доказів[315].



За наявності матеріалів з акаунтів у соціальних мережах однієї чи кількох осіб, які використовуються таким чином, якщо такі особи не дають свідчень особисто, необхідно буде враховувати вимоги, викладені у справі «Шачашвілі проти Німеччини» (Schatschaschwili v. Germany) [ВП], заява № 9154/10 від 15 грудня 2015 року[316], та подальших справах, а саме, що для їхньої неявки має бути поважна причина та наявні достатні врівноважувальні чинники, щоб компенсувати недоліки, за яких захист працював би у разі, якщо показання цих свідків були б єдиною або вирішальною підставою для засудження[317].

від 12.11.2015. URL: https://hudoc.echr.coe.int/eng?i=001-158490; Рішення ЄСПЛ у справі «Ведува проти Румунії» (Văduva v. Romania). Заява № 27781/06 від 25.02.2014. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-141172&filename=001-141172.pdf; Рішення ЄСПЛ у справі «Лопес Рібальда та інші проти Іспанії» (López Ribalda and Others v. Spain). Заява № 1874/13 від 17.10.2019. URL: https://hudoc.echr.coe.int/fre?i=001-197098

[315] Макбрайд Д. Зазначений твір.

[316] Рішення ЄСПЛ у справі «Шачашвілі проти Німеччини» (Schatschaschwili v. Germany) [ВП]. Заява № 9154/10 від 15.12.2015. URL: https://hudoc.echr.coe.int/fre?i=001-159566

[317] Макбрайд Д. Зазначений твір.

3.2. Наявні підходи у рішеннях міжнародних кримінальних трибуналів та Міжнародного кримінального суду

Якими є підходи міжнародних кримінальних трибуналів до доказування із залученням цифрових даних з відкритих джерел?

Що стосується тих справ, які розглядалися в міжнародних кримінальних трибуналах та Міжнародному кримінальному суді (МКС), то радимо вдатися до аналізу вже згадуваного вище другого тому «Options for justice a handbook for designing accountability mechanisms for grave crimes» / «Вибір заради справедливості: посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини»[318]. Сконцентрований у цьому посібнику матеріал здатний пролити світло на концептуальні підходи судів за різних часових рамок.

Чи використовує МКС у доказуванні цифрові дані з відкритих джерел?

Констатуємо, що МКС у своїй практиці оцінював матеріали, отримані з відкритих джерел на предмет їх доказової сили та віднесеності до доказів. «Надмірне використання прокурором таких відомостей в якості прямих доказів призвело до того, що судді, починаючи з 2013 року, почали обмежувати відповідну практику, зазначаючи, що *відомості з відкритих джерел насамперед мають використовуватися як орієнтуюча інформація або разом з іншими доказами*», хоча й у 2016 році ситуація знову почала змінюватися на користь використання цих доказів, але й з «певною долею скептицизму»[319]. МКС довелося констатувати, що стандарт доказування потребує використання певного типу доказів задля формування об'єктивного переконання про факти, які встановлюються, а «…звіти громадських організацій та статті у пресі можуть бути корисними для розуміння історичного контексту конфлікту»[320] (Gbagbo and Blé Goudé Case. International Criminal Court: website. URL: https://www.icc-cpi.int/cdi/gbagbo-goude).

---

[318] Вибір заради справедливості: посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини. Т. 2 / пер. О. Бондаренко; заг. ред. Р. Мартиновський, Л. Мороз. Пер. та видання здійснене за підтримки Програми «Права людини і правосуддя» Міжнар. фонду «Відродження». 2018. 544 с. URL: https://www.irf.ua/wp-content/uploads/ 2020/ 06/tom_ii_web.pdf

[319] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса: Вид-во «Юридика», 2024. С. 176–178.

[320] Там само. С. 177.

Радимо скористатися лапідарним оглядом АНТИРЕЙД з посиланням на «PRAVO», де здійснено аналіз використання панорамних знімків та авіаційної зйомки у справах «Prosecutor v. Mladic, Prosecutor v. Tolimir»[321].

Прокурор проти Младича

Прокурор проти Толіміра

На цей час робота МКС акумулює у своїй практиці сучасні підходи до оцінювання матеріалів, отриманих з відкритих джерел. Наприклад, у справах «Prosecutor v. Mahmoud al-Werfalli» та «Prosecutor v. Ahmad Al Faqi Al Mahdi»[322] щодо ситуації в Малі оцінювалися відео нападів на релігійні об'єкти під час процесу. Справа щодо збиття літака рейсу МН-17 на Донбасі також ґрунтувалася як на фото та відео з відкритого доступу, так і на перехопленнях телефонних розмов. Та будь-який юридичний процес повинен мати чіткі механізми роботи з різними видами доказів, які встановлюють однакові стандарти для всіх справ[323].

Прокурор проти Махмуда Мустафи Бусайф аль-Верфаллі

Прокурор проти Ахмада Аль-Факі Аль-Махді

[321] Рішення МКС у справі «Прокурор проти Младича» (Prosecutor v. Mladic). Заява IT-09-92-T від 22.11.2017. URL: https://www.icty.org/x/cases/mladic/tjug/en/171122-3of5_1.pdf; Рішення МКС у справі «Прокурор проти Толіміра» (Prosecutor v. Tolimir). Заява IT-05-88/2-T від 12.12.2012. URL: https://www.icty.org/x/cases/tolimir/tjug/en/121212.pdf

[322] Рішення МКС у справі «Прокурор проти Махмуда Мустафи Бусайф аль-Верфаллі» (Prosecutor v. Mahmoud al-Werfalli). Заява ICC-01/11-01/17 від 04.07.2018. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2018_03552.PDF; Рішення МКС у справі «Прокурор проти Ахмада Аль-Факі Аль-Махді» (Prosecutor v. Ahmad Al Faqi Al Mahdi) Заява ICC-01/12-01/15 від 27.09.2016. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_07244.PDF

[323] Збір інформації з відкритих джерел як майбутній засіб доказів у найважчих міжнародних злочинах. 07.12.2023. *Antiraid*: вебсайт. URL: https://antiraid.com.ua/news/zbir-informatsii-z-vidkrytykh-dzherel-iak-majbutnij-zasib-dokaziv-u-najvazhchykh-mizhnarodnykh-zlochynakh/

Які новації у цій царині щодо діяльності МКС наявні?

На цьому етапі МКС перейшов на «новий виток роботи». «Так, у 2023 році прокурор МКС оголосив про запуск розширеної платформи для надання доказів OTPLink (https://otplink.icc-cpi.int)»[324].



Для розлогішого сприйняття та розуміння аспектів використання МКС OTPLink радимо скористатися присторінковим посиланням[325] та словником термінів у додатках.

3.3. Оцінка національними суддями цифрових даних у сукупності з іншими доказами

Як оцінюють національні суди цифрові дані?

У тексті попередніх підрозділів першого розділу вже було згадано та проаналізовано певну кількість *рішень українських судів, в яких:*

Цифрові дані судді оцінювали у сукупності з іншими доказами.

Висновок про допустимість електронного документа як доказу[326] зроблено у Постанові об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20)[327].

[324] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса: Вид-во «Юридика», 2024. С. 175.

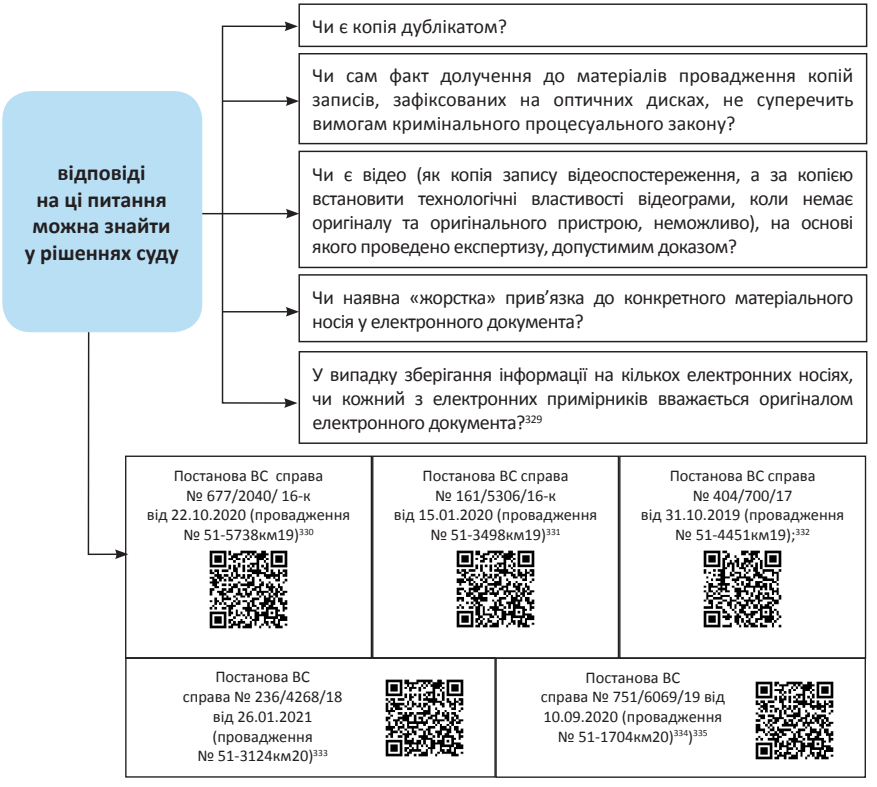
[325] ICC Prosecutor Karim A. A. Khan KC announces launch of advanced evidence submission platform : OTPLink. *International Criminal Court*: website. URL: https://www.icc-cpi.int/ news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submissionplatform-otplink)

[326] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний суд*: вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

[327] Постанова Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). URL: https://reyestr.court.gov.ua/Review/96074938

[328] Судова практика ККС Верховного Суду щодо допустимості електронних доказів: презентація, підготовлена суддею Верховного Суду Надією Стефанів. *Верховний суд*: вебсайт. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

У презентації судді Верховного Суду «Судова практика ККС Верховного Суду щодо допустимості електронних доказів»[328] наведено правові позиції Суду щодо таких питань.



[329] Судова практика ККС Верховного Суду щодо допустимості електронних доказів: презентація, підготовлена суддею Верховного Суду Надією Стефанів. *Верховний суд*: вебсайт. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

[330] Постанова Верховного Суду у справі № 677/2040/16-к від 22.10.2020 (провадження № 51-5738км19). URL: https://reyestr.court.gov.ua/Review/92458395

[331] Постанова Верховного Суду у справі № 161/5306/16-к від 15.01.2020 (провадження № 51-3498км19). URL: https://reyestr.court.gov.ua/Review/87053591

[332] Постанова Верховного суду у справі № 404/700/17 від 31.10.2019 (провадження № 51-4451км19). URL: https://reyestr.court.gov.ua/Review/85390646

[333] Постанова Верховного суду у справі № 236/4268/18 від 26.01.2021 (провадження № 51-3124км20). URL: https://reyestr.court.gov.ua/Review/94905297

[334] Постанова Верховного Суду у справі № 751/6069/19 від 10.09.2020 (провадження № 51-1704км20). URL: https://reyestr.court.gov.ua/Review/91722819

[335] Судова практика ККС Верховного Суду щодо допустимості електронних доказів: презентація, підготовлена суддею Верховного Суду Надією Стефанів. *Верховний суд*: вебсайт. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

РОЗДІЛ 4. СТАНДАРТИ ЦИФРОВИХ ДОКАЗІВ З ВІДКРИТИХ ДЖЕРЕЛ

Протокол Берклі передбачає, що розслідування з використанням даних у відкритому доступі стосується використання інформації у відкритому доступі для функції збирання інформації та доказів[336] Доказами з відкритих джерел у Протоколі Берклі названо інформацію у відкритому доступі з доказовою цінністю, яка може бути допущена для встановлення фактів у судовому процесі[337]. Також у Протоколі Берклі зазначається те, що докази, як правило, визначаються як доказ факту(ів), який використовується під час розслідування і/або подається на судовому слуханні[338].

4.1. Вимоги чинного КПК та правова позиція об'єднаної палати Касаційного кримінального суду Верховного Суду щодо такого різновиду доказів (кримінальні процесуальні умови набуття інформацією з відкритих джерел статусу доказу; недопустимість ототожнення електронного доказу як засобу доказування та матеріального носія тощо)

Якими є способи та шляхи збирання доказів, у тому числі й цифрових доказів з відкритих джерел, за вимогами чинного КПК України?

Ч. 2 ст. 93 КПК України визначає способи та шляхи збирання доказів, які дозволені у кримінальному провадженні, і логічно, що цифрові докази з відкритих джерел слід збирати відповідно до цих вимог.

Так, «…сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом»[339].

---

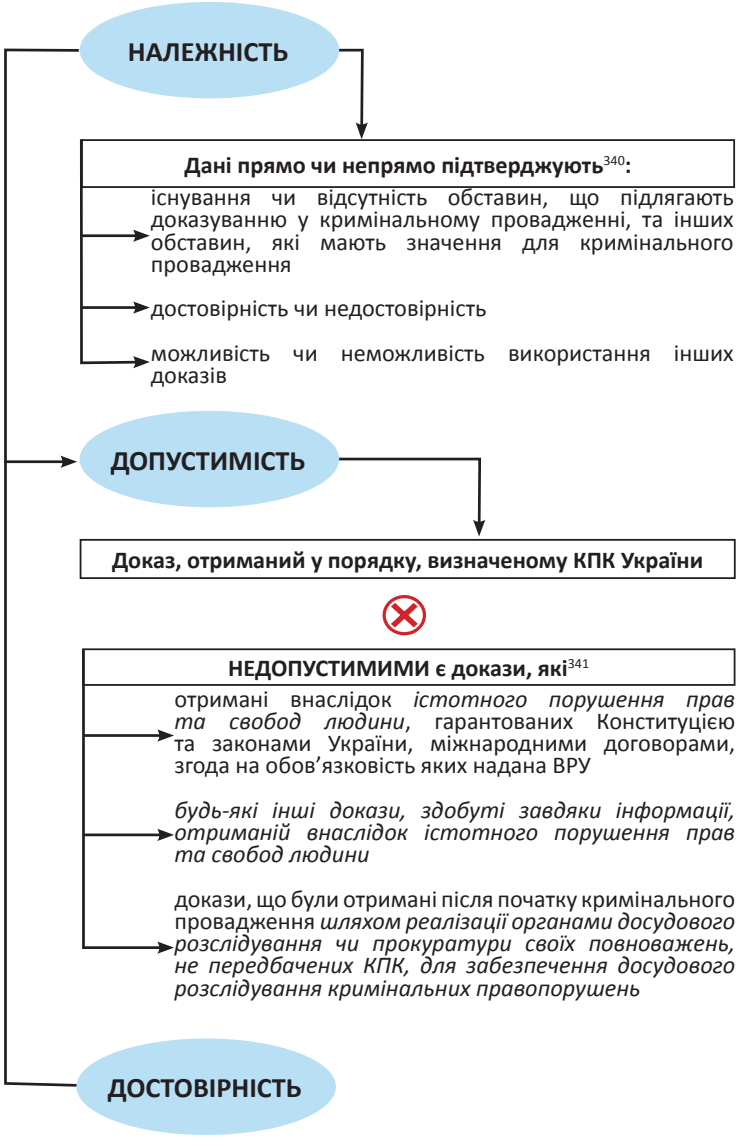
[336] Протокол Берклі … . С. 27, п. 20.

[337] Там само. С. 27.

[338] Там само. С. 27, п. 21.

[339] Кримінальний процесуальний кодекс України: Закон України № 4651-VI від 13.04.2012 (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/4651-17

Інформація з відкритих джерел набуде статусу доказу лише тоді, коли буде відповідати таким вимогам



[340] Там само.
[341] Там само.

Що таке докази за КПК України?

Чинний КПК унормовує, що *доказами у кримінальному провадженні* є «фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів і обставин, що мають значення для кримінального провадження та підлягають доказуванню»[342] (ч. 1 ст. 84 КПК України).

Які джерела інформації належать до процесуальних за КПК України?

Знаходити інформацію, яка може бути визнана доказом, ми можемо з таких процесуальних джерел, як *показання*, *речові докази*, *документи*, *висновки експертів*[343] (ч. 2 ст. 84 КПК України).

Які процесуальні джерела релевантні до цифрової інформації за КПК України?



Щодо *цифрової інформації* релевантними можуть бути такі два процесуальні джерела, як *речові докази* та *документи*, про що вже зазначали науковці[344]. Зокрема, у вже згадуваній постанові об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20)[345] серед іншого, зокрема, *зроблено висновок про допустимість електронного документа як доказу*[346] (хоча, як вже йшлося вище, у межах національного правового поля правильніше вести мову про *цифровий документ*).

---

[342] Кримінальний процесуальний кодекс України … .

[343] Там само.

[344] Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. Львів: ЛьвДУВС, 2022. С. 25. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725

[345] Постанова Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). URL: https://reyestr.court.gov.ua/Review/96074938

[346] Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07.06.2022. *Верховний Суд*: вебсайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

Чи допускається ототожнення електронного доказу як засобу доказування та матеріального носія такого документа?

«…ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Для виконання завдань кримінального провадження, з огляду на положення Закону України «Про електронні документи та електронний документообіг», допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той самий електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами CRC-сума, hash-сума), або, за наявності відповідних підстав, шляхом проведення спеціальних досліджень…»[347].
Постанова об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20).

Що КПК України відносить до документів та їх оригіналів?

Згідно з ч. 2 ст. 99 КПК України до документів, за умови наявності в них відомостей, передбачених ч. 1 цієї статті, можуть належати:

1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані);

2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України;

3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії…

Матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність»,

[347] Постанова Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). URL: https://reyestr.court.gov.ua/Review/96074938

за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази. *Оригіналом електронного документа* є його відображення, якому надається таке саме значення, як документу. Копії інформації, у тому числі комп'ютерних даних, що містяться 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*[348].

Інших конкретизованих та систематизованих стандартів, які релевантні до цифрових доказів з відкритих джерел, у національному кримінальному процесуальному законодавстві поки що немає.

Утім, наявні ґрунтовні наукові рекомендації дослідників, про які йдеться у цьому розділі та підрозділах першого розділу, і практичні дороговкази, які вміщені у Протоколі Берклі[349].

Якими положеннями слід керуватися органу досудового розслідування у національних розслідуваннях?

У національних розслідуваннях слід керуватися:

- Загальними вимогами до доказів, їх джерел, визначених у КПК.
- Постановою Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20) та іншою релевантною судовою практикою, яка постійно оновлюється.
- Усіма іншими дотичними положеннями, з яких складається кримінальне процесуальне законодавство України (див. ч. 2 ст. 1 КПК України).

Більш розлогу інформацію про *стандарти цифрових доказів з відкритих джерел* наведено у Протоколі Берклі.

[348] Кримінальний процесуальний кодекс України: Закон України № 4651-VI від 13.04.2012 (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/4651-17

[349] Протокол Берклі … .

4.2. Алгоритм аналізу відомостей, які отримані у перебігу опрацювання цифрової інформації у відкритому доступі з відкритих джерел

На етапі збирання даних, які отримані у перебігу опрацювання інформації у відкритому доступі, необхідно:

1

з'ясувати, чи справді ця інформація є такою, що перебуває у відкритому доступі

з'ясувати чи належить таке джерело до переліку відкритих

2

Дати відповідь на питання:

Чи ці дані підтверджують (прямо або непрямо) існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів?

Чи відповідає порядок отримання цих даних порядку, який пропонує нам КПК України?

Чи було допущено при їх отриманні істотні порушення прав та свобод людини, котрі гарантовані Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана ВРУ?

Чи мають місце при їх отриманні інші, передбачені ч. 1-3 ст. 87 КПК України, допущені порушення?

Чи після початку кримінального провадження органи досудового розслідування чи (та) прокуратури реалізовували свої повноваження всупереч КПК України чи (та) тим шляхом, який не передбачений КПК України для забезпечення досудового розслідування кримінальних правопорушень?

Чи мають місце ті обставини, які перелічені у ст. 88-88-1 КПК України та чи є ті із них, які перелічені у ч. 2 ст. 88 КПК України, що дозволяють допустимість?

4.3. Стандарти цифрових доказів з відкритих джерел за Протоколом Берклі

Що таке достовірність, надійність та правдивість інформації?

Особи, які мають намір використовувати інформацію з відкритих джерел, повинні першочергово з'ясувати:



Протокол Берклі «розуміє» зазначені терміни таким чином:

- «надійність» – правдоподібність, правдивість;
- «достовірність» – здатність працювати послідовно, надійно, відповідно до очікувань;
- «правдивість» (справжність, дійсність, точність) – відповідність фактам[350].

Яке основне завдання слідчих, які ведуть розслідування з використанням інформації у відкритому доступі?

Основне завдання слідчих, які ведуть розслідування з використанням інформації у відкритому доступі, – збирати *актуальну* та *достовірну інформацію*, щоб її можна було використати для фактичних і юридичних висновків. Слідчі повинні прагнути, щоб сприйняті ними з відкритих джерел дані мали у перспективі доказову силу, а цифрові докази, отримані першопочатково у вигляді інформації з відкритих джерел, були *прийнятними, релевантними, достовірними* та *доказовими. Допустимість таких доказів має на меті убезпечення належного процесу та права на справедливий судовий розгляд.* Попри те, що у міжнародних кримінальних судах і трибуналах планка допустимості доказів зазвичай нижча, ніж у національних судах, все ж *методи збирання доказів важливі скрізь*[351].

[350] Протокол Берклі … . С. 27–28, п. 23.
[351] Там само. С. 47, п. 55.

Отже, **резюмуємо**!

Слідчий під час роботи з відкритими джерелами

Ⓑ Оцінює ризики, безпеку та вживає належних заходів задля забезпечення такої безпеки та уникнення (мінімізації) ризиків[352]

❗ Ⓑ **План стійкості та турбота про себе передовсім**[353]

Перед початком розслідування з використанням даних у відкритому доступі *слід* ***створити план онлайн-розслідування*** (див. дод. І до Ⓑ Протоколу Берклі[354]), який має охоплювати загальну стратегію розслідування та конкретні операції з розсліду-вання в Інтернеті[355]. Ⓑ *План онлайн-розслідування має стосуватися тих тем, які визначені п. 116–121*[356]*, і він підлягає регулярному перегляду та, за потреби, слід вносити затребувані зміни до нього*[357]

Ⓑ З'ясовує, чи є інформація *актуальною* та *достовірною* (чи є змога встановити або спростувати її з достатньою точністю)[358]

Додаткові критерії достовірності[359]
- автентифікованість
- ідентифікованість
- верифікованість
- незмінність
- відтворюваність

З'ясовує, чи не є ця інформація Ⓑ *неправдивою* (недостовірна інформація, що не призначена для заподіяння шкоди. Наприклад, люди, не знаючи про її неправдивість та маючи на меті бути корисними, поширюють таку інформацію в Інтернеті, соціальних мережах)[360] чи Ⓑ *дезінформацією* (неправдива інформація, яка навмисно створюється та поширюється з явною метою заподіяння шкоди)[361]

Ⓑ Великий обсяг зібраної інформації може бути обтяжливим або навіть неможливим для огляду. Збереження та зберігання масово зібраної інформації теж будуть такими самими[362].

[352] Там само. С. 55–62, п. 67–93.
[353] Там само. С. 74–75, п. 123–126.
[354] Там само. С. 113.
[355] Там само. С. 72, п. 115.
[356] Там само. С. 72–74.
[357] Там само. С. 74, п. 122.
[358] Там само. С. 47, п. 55.
[359] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2022. С. 100–101.
[360] Протокол Берклі … . С. 47, п. 55; присторінкове посилання № 81.
[361] Там само.
[362] Там само. С. 46–47.

РОЗДІЛ 5. ПОШУК, ЗБИРАННЯ ТА ВИКОРИСТАННЯ ЦИФРОВИХ МАТЕРІАЛІВ З ВІДКРИТИХ ДЖЕРЕЛ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ

5.1. Підготовка до пошуку, огляду та фіксації цифрових матеріалів з відкритих джерел у мережі «Інтернет»

5.1.1. Процесуальні та організаційно-тактичні основи підготовки до пошуку, огляду та фіксації цифрових матеріалів з відкритих джерел у мережі «Інтернет»

У кримінальному процесі України одним зі способів виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення є проведення передбаченого ст. 237 КПК України СРД-огляду.

На думку науковців, зокрема А. В. Коваленко, «ця слідча (розшукова) дія зазвичай спрямована на дослідження та фіксування матеріальної обстановки і є незамінним процесуальним засобом отримання доказової й орієнтуючої інформації від об'єктів матеріального світу. Проте з поступальним рухом науково-технічного прогресу та поширенням комп'ютерної техніки все частіше постає потреба в межах кримінального провадження дослідити зміст інформації, що міститься в пам'яті таких пристроїв чи обробляється ними.

З ухваленням Закону України № 2137–IX від 15 березня 2022 року «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та «протидії кібератакам» така інформація дістала назву «комп'ютерні дані», а процедура її вилучення, фіксування й оперативного дослідження стала новим легально визначеним видом огляду – оглядом комп'ютерних даних»[363].

Що таке комп'ютерні дані?

Термін «комп'ютерні дані» визначений у ст. 1 Конвенції про кіберзлочинність як будь-яке подання фактів, інформації або концепцій у формі, придатній для обробки у комп'ютерній системі,

[363] Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту*. Вип. 4. 2023. С. 54. DOI https://doi.org/10.32999/ksu2307-8049/2023-4-9

включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою[364]. Як вбачається зі змісту Конвенції про кіберзлочинність, *комп'ютерна система* – це будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, одине чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних[365].

Розкриваючи сутність комп'ютерних даних, А. В. Коваленко зазначає, що

> ...за своїм визначенням це є інформацією, яка була зашифрована для обробки логічними процесорами комп'ютерної техніки і, відповідно, в оригінальному вигляді не може бути сприйнята органами чуттів людини. Тому *безпосередньому дослідженню уповноваженими особами підлягає візуальне та аудіовізуальне подання комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки*[366].

Судячи із зазначеного *цифрова інформація з відкритих джерел є одним із видів комп'ютерних даних.*

Що треба врахувати під час підготовки до пошуку, огляду та фіксації цифрових матеріалів з відкритих джерел?

Як видно зі змісту ст. 237 КПК України, СРД-огляд комп'ютерних даних проводиться з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення. Особливістю проведення СРД-огляду комп'ютерних даних є те, що він складається з таких етапів:

1) пошук цифрових матеріалів, які мають значення для кримінального провадження;

2) безпосередній огляд цифрових матеріалів, який включає:

– фіксацію оглянутої інформації та ходу СРД у протоколі огляду з відображенням послідовності усіх дій під час проведення СРД;

– збереження цифрових матеріалів з відкритих джерел, які будуть використовуватися як доказ у кримінальному провадженні;

– формування додатків до протоколу огляду.

---

[364] Конвенції про кіберзлочинність (дата підписання: 23.11.2001, дата набрання чинності в Україні: 01.07.2006) наведені поняття «комп'ютерна система» та «комп'ютерні дані» [https://zakon.rada.gov.ua/laws/show/994_575#Text]

[365] Там само.

[366] Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту*. Вип. 4. 2023. С. 56. DOI https://doi.org/10.32999/ksu2307-8049/2023-4-9

Кожний з цих етапів передбачає комплекс заходів, які треба вжити під час підготовки до СРД для їх здійснення. Окрім цього, у Ⓑ Протоколі Берклі йдеться, що слідчі, які ведуть розслідування з використанням даних у відкритому доступі, повинні *розпочинати розслідування в Інтернеті лише після вжиття певних підготовчих заходів, які включають*:

• Проведення *цифрової оцінки загроз та ризиків*:

– щоб визначити загальні та конкретні загрози, які можуть виникнути в результаті діяльності в Інтернеті, зокрема відвідування цільових вебсайтів, постійний моніторинг конкретних джерел або вилучення даних із платформ соціальних медіа, оцінку цифрових загроз та ризиків слід здійснювати, консультуючись (або із залученням) із спеціалістом з кібербезпеки. Загальну інформацію про загрози та ризики у розслідуваннях з використанням даних у відкритому доступі див. у Главі IV Ⓑ Протоколу Берклі (про безпеку) та в Додатку II Ⓑ Протоколу Берклі (щодо шаблону оцінювання цифрових загроз та ризиків).

• Проведення *оцінювання цифрового середовища*:

– слідчі повинні розуміти цифрове середовище досліджуваної ситуації (тип доступної та використовуваної технології, зокрема хто її використовує, який вплив вона матиме на типи доступних цифрових даних).

• Розробку *плану онлайн-розслідувань* (див. Додаток I Ⓑ Протоколу Берклі щодо шаблону онлайн-розслідування):

– план онлайн-розслідування має охоплювати:

1) загальну стратегію розслідування;

2) конкретні операції з розслідування в Інтернеті.

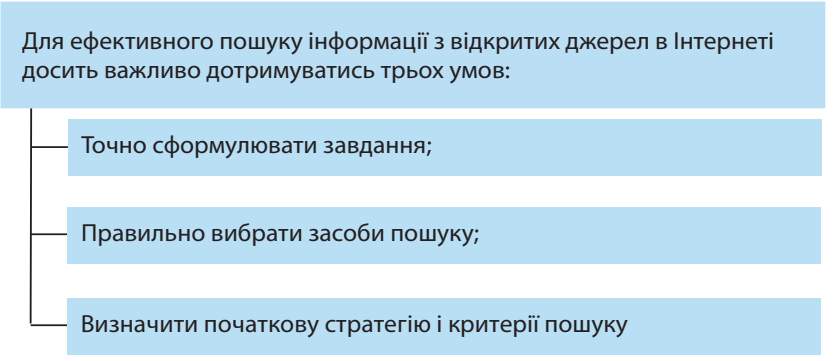
Якщо онлайн-розслідування є частиною більш широкого розслідування з використанням традиційних методів, таких як взяття показань свідків або збирання речових доказів, план онлайн-розслідування слід включити до основного плану розслідування.

• Встановлення політики щодо *збереження даних, видалення даних, доступу до даних та обміну ними*, перш ніж збирати та зберігати інформацію[367].

Від чого залежить ефективність пошуку цифрової інформації з відкритих джерел?

Комплекс підготовчих дій для пошуку цифрової інформації з відкритих джерел залежить від виду цифрової інформації, яку слідчий планує отримати в результаті пошуку та використати як доказ у кримінальному провадженні.

[367] Там само … . С. 70.



Під час підготовки до пошуку інформації з відкритих джерел та під час здійснення безпосереднього пошуку рекомендуємо дотримуватися такого структурованого підходу:

1. **Визначити завдання:** чітко окреслити, яка інформація потрібна і навіщо вона потрібна, що допоможе відфільтрувати нерелевантну інформацію.
2. **Визначити ключові слова та фрази:** обдумати та скласти список ключових слів і фраз, що відповідають темі пошуку. Це включає синоніми, пов'язані терміни та варіації, які можна використовувати для описування інформації, яку треба знайти.
3. **Уточнити параметри пошуку:** визначити параметри пошуку, включаючи часові межі, географічне розташування, мову та будь-які інші відповідні фільтри. Це допомагає звузити результати пошуку та зосередитися на найбільш релевантній інформації.
4. **Вибрати пошукові системи та інструменти:** вибрати відповідні пошукові системи та онлайн-бази даних відповідно до характеру пошуку. Серед популярних варіантів – Google, Bing, Yahoo, спеціалізовані бази даних і платформи соціальних мереж тощо.
5. **Оцінити достовірність і надійність:** оцінити достовірність і надійність джерел, які трапляються під час пошуку. Треба шукати авторитетні вебсайти, офіційні публікації, наукові статті й джерела зі своєрідним «послужним списком» точності та чесності.
6. **Перевірити на об'єктивність:** слід пам'ятати про можливі упередження в інформації, яку буде знайдено. Також потрібно враховувати погляди, викладені в різних джерелах, і навести перехресні посилання на інформацію з багатьох джерел, щоб забезпечити збалансоване уявлення.
7. **Здійснити перевірку на точність:** слід перевірити точність зібраної інформації, підтвердивши її кількома джерелами й перехресними

посиланнями. Якщо це можливо, треба знайти першоджерело, щоб забезпечити надійність.

8. **Відстежити джерела походження цифрових матеріалів:** необхідно відстежити джерела, використовувані під час пошуку, включаючи URL-адреси, дати публікацій, інформацію про автора та будь-яку іншу відповідну інформацію.

9. **Потрібно дотримуватися визначених в законодавстві вимог щодо збирання та використання конфіденційної інформації про особу і законів про авторські права** під час доступу та використання цифрової інформації з відкритих джерел. Слід уникати поширення особистої інформації без згоди особи.

10. **Треба бути обізнаним в алгоритмах пошуку**, новітніх інструментах пошуку та нових тенденціях у пошуку цифрової інформації.

Які вимоги до проведення огляду комп'ютерних даних передбачені в КПК України?

Відповідно до абз. 2 ч. 2 ст. 237 КПК України огляд комп'ютерних даних проводять слідчий прокурор, а також дізнавач, який згідно з ч. 1 ст. 40^1 КПК України під час здійснення дізнання наділяється повноваженнями слідчого[368], шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі).

Сутність СРД-огляду як способу виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення та зміст абз. 2 ч. 2 ст. 237 КПК України вказують на те, що

> «під час огляду комп'ютерних даних уповноважені особи мають особисто сприйняти зміст аудіовізуального виразу комп'ютерних даних і відобразити його у протоколі процесуальної дії та додатках до нього у формі, придатній для сприйняття такого змісту іншими людьми. Для безпосереднього сприйняття людиною комп'ютерні дані, що містять текст, зображення, звуки й інші аудіовізуальні форми інформації, можуть бути відтворені через пристрої виведення даних (екран, аудіопристрої, принтери тощо), а код, що містить алгоритми дій, може бути виконано (запущено програму)»[369].

[368] Кримінальний процесуальний кодекс України: затв. Законом України від 13 квіт. 2012 р. № 4651-VI. *Верховна Рада України*: [сайт]. URL: http://zakon3.rada.gov.ua/laws/show/4651-17

[369] Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту*. Вип. 4. 2023. С. 56. DOI https://doi.org/10.32999/ksu2307-8049/2023-4-9

Згідно з ч. 3 ст. 237 КПК України для участі в огляді можуть бути запрошені потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження. З метою отримання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів. Отже, КПК України не передбачає обов'язкової участі спеціаліста під час здійснення слідчим, прокурором огляду комп'ютерних даних. Утім, слід звернути увагу, що згідно з ч. 4 ст. 99 КПК України копії інформації, зокрема комп'ютерних даних, які містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, визнаються судом як оригінали документів за умови, якщо вони виготовлені слідчим, прокурором із залученням спеціаліста. Також ч. 2 ст. 71 КПК України передбачає, що під час досудового розслідування спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень тощо) сторонами кримінального провадження.

Окрім цього слід врахувати, що згідно з ч. 1 ст. 41 КПК України слідчий може доручити проведення огляду сайтів, інтернет-ресурсів, відео та інших відомостей, що розміщенні в мережі «Інтернет», працівнику оперативного підрозділу, який володіє знаннями у сфері інформаційних технологій.

Резюмуємо! У нормах КПК України передбачено:

– огляд комп'ютерних даних як один із способів виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення;

– слідчий, прокурор, працівник оперативного підрозділу за дорученням слідчого є уповноваженими суб'єктами з проведення огляду комп'ютерних даних;

– слідчий, прокурор можуть залучити спеціаліста з метою отримання допомоги з питань, що потребують спеціальних знань, для проведення огляду комп'ютерних даних та надання технічної допомоги під час проведення СРД;

– слідчий, прокурор виготовляють копії інформації, зокрема комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, з обов'язковим залученням спеціаліста (що є умовою визнання їх судом як оригінала документа);

– форму відображення інформації, яку містять комп'ютерні дані, яка має бути придатною для сприйняття їх змісту;

– можливість використання електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі як способи фіксації комп'ютерних даних.

Які організаційно-тактичні заходи слідчий має вжити під час підготовки до огляду цифрових матеріалів з відкритих джерел?

Заходи, які слідчий має вжити під час підготовки до огляду цифрових матеріалів, ми узагальнили в таблиці, для формування якої використано: положення (B) Протоколу Берклі, норми КПК України, якими передбачено підстави, порядок проведення СРД-огляду комп'ютерних даних, визначено уповноважених суб'єктів на проведення цієї СРД, а також інших учасників кримінального провадження, які можуть бути присутніми під час проведення цієї СРД, підстави та умови участі спеціаліста під час проведення цієї СРД тощо; особливості організації і тактики проведення огляду комп'ютерних даних, огляду вебресурсів тощо, які розкрито у працях А. В. Коваленка[370], а також порядок виявлення та дослідження цифрових (електронних) слідів, визначений у навчальному посібнику «Криміналістика: криміналістична техніка»[371].

Організаційно-тактичні заходи під час підготовки до огляду цифрових матеріалів з відкритих джерел

Під час підготовки до проведення огляду цифрової інформації з відкритих джерел слідчий повинен
Визначити мету проведення огляду цифрових матеріалів з відкритих джерел у кримінальних провадженнях щодо злочинів проти миру, безпеки людства та міжнародного правопорядку:

[370] Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. DOI: 10.21564/2414-990X.161.278117; Коваленко А. В. Огляд комп'ютерних даних: сутність і процесуальний порядок проведення. *Вісн. Харків. нац. ун-ту внутр. справ.* 2023. № 3 (102), ч. 2. С. 187–197. URL: https://doi.org/10.32631/v.2023.3.41; Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту.* Вип. 4. 2023. С. 54. URL: https://doi.org/10.32999/ksu2307-8049/2023-4-9; Коваленко А. В. Особливості проведення огляду веб-ресурсів як різновиду огляду комп'ютерних даних. *Актуальні питання судової експертології, криміналістики та кримінального процесу*: матеріали V Міжнар. наук.-практ. конф. (м. Київ, 21 груд. 2023 р.) / КНДІСЕ. Київ, 2023. С. 199–202.

[371] Криміналістика: криміналістична техніка: навч. посіб. / Р. Л. Степанюк та ін. Харків: ХНУВС, 2023. 388 с.

- провести пошук, виявлення та фіксацію слідів цієї категорії злочинів або перевірити вже отримані докази у конкретному кримінальному провадженні;
- провести пошук, виявлення та фіксацію даних про осіб, причетних до цього виду злочинів, визначити характер їх взаємин, а також електронних слідів підготовки, учинення і приховання злочину;
- провести пошук, виявлення та фіксацію інформації про контакти між учасниками події та іншої інформації, яка підтверджує злочинну діяльність;
- провести пошук, збирання та фіксацію інформації про підозрюваного, який переховується, тощо.

Ознайомитися з матеріалами кримінального провадження (зі змістом заяви про вчинення кримінального правопорушення, із протоколами допиту свідків, потерпілих, у разі наявності підозрюваного, та іншими матеріалами кримінального провадження, щоб з'ясувати:

- пошук яких цифрових матеріалів з відкритих джерел треба здійснити;
- на які особливості контенту (цифрової інформації) слід звернути увагу під час огляду;
- які дії треба здійснити з метою пошуку цифрових матеріалів;
- які відомості можуть містити дані, що підлягають перегляду;
- до якої категорії належить контент вебресурсу (цифрові матеріали) (текстовий вміст, зображення, аудіо-, відеоматеріали, супутникові знімки, карти, файли для завантаження тощо), який підлягає перегляду;
- кого зі спеціалістів (залежно від виду цифрових матеріалів) потрібно залучити для огляду;
- яким способом буде здійснюватися фіксація ходу огляду цифрових матеріалів з відкритих джерел;
- які носії інформації слід підготувати для копіювання оглянутих цифрових матеріалів.

Визначити, чи безпечно збирати цифровий елемент, чи можна і потрібно вжити заходів безпеки, та визначити, яких саме заходів безпеки слід вжити під час пошуку та огляду цифрових матеріалів.

Визначити час, дату та місце проведення огляду.

Цифрові матеріали з відкритих джерел мережі «Інтернет» оглядатимуться з використанням комп'ютера (службового) із доступом до мережі «Інтернет» та програмного забезпечення веббраузера.

Під час планування проведення СРД ❗ слідчий має врахувати, що згідно з ч. 4 ст. 223 КПК України проведення СРД у нічний час (з 22-ї години вечора до 6-ї години ранку) не допускається, за винятком невідкладних випадків:

➢ коли затримка в їх проведенні може спричинити втрату слідів кримінального правопорушення чи втечу підозрюваного;

➢ здійснення кримінального провадження в умовах воєнного стану у порядку, встановленому ст. 615 КПК України.

Вжити заходів щодо підготовки технічних засобів, необхідних для проведення огляду цифрових матеріалів з відкритих джерел мережі «Інтернет»:

➢ комп'ютер з автономним джерелом живлення з підключенням до мережі «Інтернет», на якому мають бути встановлені:

• веббраузер (наприклад, Google Chrome, Firefox, Opera та інші), за допомогою якого буде здійснюватися пошук потрібного вебсайту (вебсторінки), на яких розміщені цифрові матеріали з відкритих джерел, які підлягають огляду;

• вебверсії відповідного месенджера (Telegram, Viber, WhatsApp, Signal, WeChat тощо) чи відеохостингу «YouTube», з використанням яких буде здійснюватися огляд цифрових матеріалів;

• спеціальні програми-браузери, такі як Opera або Tor Browser, що мають вбудований функціонал для використання технології VPN, яку доречно використовувати у випадку отримання доступу до вебресурсів російської федерації чи окупованих територій. Tor Browser також надає можливість отримати доступ до вебресурсів, розміщених у «темних мережах» (англ. «Dark web»). Завдяки анонімності, з одного боку, в таких мережах є можливість вільно розповсюджувати та отримувати інформацію у країнах з жорсткою цензурою або диктаторськими політичними режимами, не побоюючись переслідувань;

➢ якщо огляд здійснюється з використанням ноутбука, треба підготувати комплекти запасних батарей або забезпечити неперервний доступ до звичайної електромережі змінного струму;

➢ диски з необхідними для огляду програмними засобами;

➢ принтер;

➢ технічні засоби, потрібні для документування процесу огляду (фото-, відеокамера тощо);

➢ носії інформації, на які безпосередньо копіюватимуться оглянуті матеріали, – жорсткі диски (вінчестери), змінні носії (CD-DVD-диски), USB-накопичувач (флешка) тощо;

➢ якщо під час огляду може виникнути необхідність скопіювати вебсайти чи вебпортали у повному обсязі, з огляду на те, що вони можуть мати досить великий обсяг інформації, треба заздалегідь узгодити особливості копіювання такої кількості інформації із спеціалістом.

Скопіювати увесь вебпортал або вебсайт наявними програмними засобами операційної системи Windows неможливо через відсутність у них функціоналу, призначеного для такого копіювання.

Для збереження цілого вебпорталу або вебсайту, зі збереженням коректних зв'язків між вебсторінками та різними посиланнями між ними, потрібно використовувати програмне забезпечення, яке спеціально призначене саме для цього, наприклад *розширення-додаток* WebScrapBook для браузера Google або Firefox, чи окреме *програмне забезпечення*, таке як Teleport Pro, Httrack Website Copier, Cyotek WebCopy, WebCopier, Website Ripper Copier, Offline Explorer, Web2Disk тощо, чи *онлайн-платформи типу:*

- saveweb2zip.com (адреса: https://saveweb2zip.com/);
- Website Copier Online (адреса: https://www.toolsbug.com/website-copier-online.php),
- Website Downloader Online (адреса: https://www6.waybackmachine downloader.com/website-downloader-online/) тощо.

➢ мережеве обладнання;
➢ блоки безперебійного живлення (UPS);
➢ резервне живлення (акумулятори та генератори, зарядні станції);
➢ програмне забезпечення (операційна система, візуальної фіксації (програма «захоплення» екрану), тощо.

Підготовку відповідних технічних засобів здійснює уповноважена особа, яка буде проводити огляд, або покладається на залученого спеціаліста.

Визначити комплекс дій, спрямованих на забезпечення виявлення максимальної кількості слідів кримінального правопорушення та інформації про злочин, щодо якого здійснюється досудове розслідування.

Передбачити всі можливі ризики, які можуть виникнути під час проведення цієї СРД, і вжити заходів щодо їх запобігання. Зокрема, слідчий має врахувати, що цифрові матеріали з відкритих джерел мають такі особливості:

➢ мають вільний доступ для користувача;
➢ зберігаються та поширюються за допомогою комп'ютерних мереж;
➢ їх може легко видалити, змінити чи підробити особа, яка їх розмістила;
➢ вебресурси містять цифрові матеріали таких основних категорій, як текстовий вміст, зображення, аудіо- чи відеоматеріали, карти, супутникові знімки, файли для завантаження тощо, які мають власні особливості, та ін.

Визначити коло учасників, які будуть присутні, й тих, які безпосередньо братимуть участь у проведенні огляду, та вжити необхідних заходів для забезпечення їх присутності під час проведення огляду.

- Згідно з абз. 2 ч. 2, ст. 237 КПК України, ч. 1 ст. 40-1 КПК України та ст. 41 КПК України огляд комп'ютерних даних може проводитися:

➢ слідчим, дізнавачем, прокурором за наявності у них необхідних знань і технічних навиків;

➢ слідчим, дізнавачем, прокурором із залученням спеціаліста, з метою одержання допомоги з питань, що потребують спеціальних знань (ч. 3 ст. 237 КПК України).

Керуючись ст. 71, 79 та ч. 3 ст. 237 КПК України, слідчому необхідно визначити, якого саме спеціаліста необхідно залучити до огляду та вжити заходів із забезпечення його участі в огляді;

➢ працівником оперативного підрозділу за дорученням слідчого, дізнавача, прокурора (ст. 41 КПК України).

• Під час прийняття рішення щодо доцільності проведення огляду працівником оперативного підрозділу слідчий згідно зі ст. 41 КПК України має підготувати доручення про проведення огляду сайтів, Інтернет-ресурсів, відео та інших відомостей, що розміщенні в мережі «Інтернет», які містять інформацію про вчинення кримінального правопорушення. Доручення слідчого, прокурора щодо проведення СРД є обов'язковими для виконання оперативним підрозділом.

У КПК України не передбачена обов'язкова участь спеціаліста під час огляду комп'ютерних даних. Утім, згідно з ч. 4 ст. 99 КПК України копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, визнаються судом як оригінал документа за умови, якщо вони виготовлені слідчим, прокурором із залученням спеціаліста.

Зважаючи на те, що копіювання інформації з відкритих джерел мережі «Інтернет» є одним з обов'язкових етапів їх збереження та вилучення, з метою забезпечення належного збереження такої інформації та виготовлення додатків до протоколу огляду, враховуючи вимоги ст. 99 КПК України, міжнародні стандарти порядку збирання та дослідження електронних доказів доцільно забезпечити участь спеціаліста під час огляду цифрових матеріалів з відкритих джерел у мережі «Інтернет».

• Відповідно до ч. 3 ст. 237 КПК України для участі в огляді може бути запрошений потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження.

• Ст. 223 КПК України не передбачає обов'язкової участі понятих під час проведення СРД огляду комп'ютерних даних. Згідно з абз. 1 ч. 7 ст. 223 КПК України поняті можуть бути запрошені, якщо слідчий прокурор вважатиме це за доцільне. У такому випадку треба вжити заходів щодо запрошення не менше двох понятих та забезпечити їх присутність під час проведення огляду.

Підбираючи понятих для участі у проведенні огляду слідчий, крім вимог, визначених в абз. 3 ч. 7 ст. 223 КПК України (понятими не можуть бути потерпілий, родичі підозрюваного, обвинуваченого і потерпілого, працівники правоохоронних органів, а також особи, зацікавлені в результатах кримінального провадження), повинен врахувати, що недоцільно запрошувати як понятих осіб з ознаками психічних розладів, з вадами зору, слуху тощо.

Визначити спосіб фіксації інформації, яку оглядають в мережі «Інтернет».

Огляд комп'ютерних даних проводять слідчий, прокурор шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі). У зв'язку з чим необхідно:

- визначити та підготувати технічні засоби фіксації огляду цифрових матеріалів з відкритих джерел мережі «Інтернет»;
- визначити працівника, який буде здійснювати фіксацію технічними засобами здійснення огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» та забезпечити його участь під час проведення СРД.

У разі залучення такого працівника слідчий має заздалегідь пояснити йому:

- що фіксація такої СРД здійснюється від початку проведення огляду до його закінчення;
- на відеокамеру має бути зафіксований весь процес пошуку, виявлення та огляду цифрових матеріалів з відкритих джерел у мережі «Інтернет», процес їх копіювання та формування додатків до протоколу огляду.

5.1.2. Технічне та техніко-криміналістичне забезпечення роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет»

Однією зі складових підготовки до пошуку, огляду та фіксації цифрової інформації з відкритих джерел, яка буде використовуватися як доказ у кримінальному провадженні, є технічне та техніко-криміналістичне забезпечення роботи з цифровими матеріалами.

Розмежування на технічне та техніко-криміналістичне забезпечення роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет» є досить умовним і виходить лише з того, що у криміналістиці є сформована система техніко-криміналістичних засобів, які використовує слідчий під час проведення СРД. А втім, враховуючи те, що техніко-криміналістичні засоби у вузькому значенні є лише матеріальним обладнанням, приладами, апаратурою та матеріалами, які використовують для збирання і дослідження речових доказів, описані нижче технічні засоби також можна до них віднести. У зв'язку із цим можна констатувати, що **технічне забезпечення роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет»** – це вид забезпечення роботи слідчого, її організації та ефективного використання технічних засобів (комп'ютера, мережевого обладнання, джерела безперебійного живлення (далі – UPS), програмного забезпечення візуальної фіксації алгоритму дій тощо) під час проведення слідчих (розшукових) заходів, метою яких є збирання та фіксація цифрових матеріалів (доказів) з ресурсів (вебсайти, онлайн-бази

даних, сторінки у соціальних мережах тощо), які є доступними та надають інформацію, не обмежену законодавством, авторськими правами або іншими обмеженнями.

Які технічні засоби потрібні для пошуку, огляду та фіксації цифрової інформації з відкритих джерел мережі «Інтернет»?

До таких технічних засобів належать:

1) комп'ютер;

2) з'ємне зовнішнє обладнання (зовнішні жорсткі диски, USB-флеш-накопичувачі, змінні носії (CD/DVD-диски));

3) мережеве обладнання;

4) блоки безперебійного живлення;

5) резервне живлення (акумулятори та генератори, зарядні станції);

6) програмне забезпечення (операційна система, система візуальної фіксації (програма «захоплення» екрана)).

Якою має бути мінімально орієнтовна конфігурація комп'ютера?

Пошук, огляд та фіксацію цифрових матеріалів з відкритих джерел у мережі «Інтернет» здійснюють на стаціонарному комп'ютері або ноутбуці з мінімально орієнтовною конфігурацією, яка може змінюватися у зв'язку з постійним розвитком комп'ютерних технологій. Використовувати нетбуки, планшети, смартфони тощо не рекомендується через низьку продуктивність або невеликий розмір екрана, сенсорну клавіатуру, які унеможливлять якісну фото- та відеофіксацію всього алгоритму дій.

На момент написання науково-практичного порадника пошук, огляд та фіксацію цифрової інформації з відкритих джерел слідчий, прокурор можуть здійснювати з *використанням комп'ютера або ноутбука, які мають таку орієнтовну конфігурацію*:

1) кількість ядер процесора – від 4;

2) частота одного ядра – від 3,8 ГГц;

3) оперативна пам'ять – від 16 Гб;

4) жорсткий диск – від 2 Тб;

5) дискретна відеокарта – з підтримкою відео 4К з об'ємом пам'яті від 8 Гб.

Також слід звернути увагу на кількість зовнішніх USB-портів на комп'ютері – від цього залежить можливість підключити до нього потрібну кількість зовнішніх пристроїв (жорсткі диски, змінні носії (CD-DVD-диски, USB-флеш-накопичувачі, інші зовнішні пристрої з накопичувачами та для роботи з оптичними носіями інформації). Рекомендовано мати на пристрої не менше трьох портів. Якщо їх кількість недостатня, можливе використання USB-хабів (розгалужувачів). Крім цього, має значення і швидкість передавання інформації через USB-порт. Так, рекомендовано використання персональних комп'ютерів з USB-портами 3.0, 3.1 та 3.2.

Які є мінімальні вимоги для підключення до мережі «Інтернет»?

Мережеве обладнання має забезпечувати стійкість з'єднання з Інтернетом на швидкості від 100 Мбіт/с.

Для усунення кіберзагроз треба застосувати базові принципи забезпечення інформаційної безпеки – це, зокрема, введення суворої парольної політики і відмова від надання адміністративних повноважень стороннім користувачам, зберігання критично важливої інформації у закритому доступі, регулярне оновлення програмного забезпечення на всіх рівнях.

Які блоки безперебійного живлення та портативні зарядні станції можна використовувати у разі зникнення електричного струму в електромережі або відхилення його показників (параметрів) від допустимих норм?

В умовах планових/позапланових відключень світла з метою забезпечення належної (безперервної) процедури огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» важливим є забезпечення постійного доступу технічних засобів, які використовуються під час їх пошуку, огляду та фіксації цих матеріалів до джерел електроживлення, що можна здійснити завдяки використанню блоків безперебійного (безперервного) живлення чи портативних зарядних станцій.

Наприклад, UPS (Uninterruptible Power Supply) – автоматичний пристрій, котрий дозволяє приєднаному до нього обладнанню деякий час працювати від вбудованих акумуляторів у разі зникнення електричного струму в електромережі або відхилення його показників (параметрів) від допустимих норм (насамперед рівнів напруги, на які налаштовано електронну схему приблизно 170–255 В).

Портативні зарядні станції – це прилади, що дозволяють запитувати ПК без підключення до мережі 220 В. Таке обладнання забезпечить стабільну роботу під час пошуку та аналізу доказової інформації з відкритих джерел у мережі «Інтернет», що важливо під час проведення СРД-огляду.

Яке програмне забезпечення потрібне для фіксації ходу СРД-огляду цифрових матеріалів з відкритих джерел?

Попри те, що програмне забезпечення становить окремий комплекс засобів, який відрізняється від технічних та техніко-криміналістичних, розгляд одного з них в цьому підрозділі необхідний у зв'язку з їх відношенням до фіксації послідовності дій під час збирання цифрових (електронних) матеріалів з відкритих джерел (доказів) у мережі «Інтернет» під час проведення СРД-огляду.

До такого програмного забезпечення належать програмні засоби «захоплення» екрана – з їх допомогою є можливість робити знімок вікна або всього екрана, обрати область прямокутної або довільної форми. Знімок

можна зберегти у вигляді зображення (PNG, GIF або JPEG-формату) або вебсторінки, також є можливість надіслати знімок електронною поштою.

Крім цього, для відеофіксації прямо з екрана комп'ютера можна скористатися десятками спеціальних програм, які є безкоштовними. Розглянемо ті, які використовуються на платформах Windows, macOS та Linux.

Програмне забезпечення, за допомогою якого можна здійснити відеофіксацію інформації з екрана монітора комп'ютера

Назва програми	Стислий зміст
Wave.video	Цей вебвідеореєстратор дозволяє легко записувати відео в режимі онлайн за допомогою будь-якого браузера з будь-якого місця. Жодні завантаження або установки непотрібні.
https://wave.video/ua/live-streaming/online-video-recorder	
OBS Studio (Open Broadcaster Software)	Безкоштовне програмне забезпечення, яке дозволяє записувати відео з десктопа.
https://obsproject.com/uk/download	
FastStone Capture	Потужний, легкий, але повнофункціональний інструмент захоплення екрана, який дозволяє легко знімати та коментувати будь-що на екрані, включаючи вікна, об'єкти, меню, повний екран, прямокутні/довільні області та навіть вікна/вебсторінки, що прокручуються. Він також дозволяє записувати дії на екрані, звук і вебкамеру у відеофайли MP4.
https://www.faststone.org/download.htm	
CamStudio	Безкоштовна комп'ютер на програма для запи сування того, що відбу вається на екрані комп'ю тера у файл AVI або SWF (флеш) разом зі звуком.
http://camstudio.org/	

Camtasia Studio	Програмне забезпечення для захоплення відео з екрана. Видавцем цього програмного забезпечення є компанія TechSmith. Користувач визначає область екрана чи вікна, яке має бути захопленим, а також встановлює пара метри запису перед його початком. Camtasia Studio також дозволяє користувачеві записувати звук з мікрофона або динаміків, а також розмістити на екрані відеоматеріали з вебкамери. Camtasia Studio має можливість записувати зображення з екрана у відеофайли різних форматів, є можливість редагувати відео, є вбудовані Macromedia Flash (SWF) і відеопрогравачі. Camtasia захоплює дії та звуки в будь-якій частині Windows-систем і зберігає у файл стандарту AVI. Зроблене за допомогоюпрограми відео можна експортувати у кілька підтримуваних програмою форматів.
https://www.techsmith.com/video-editor.htm	
UVScreen Camera 6	Проста і зручна програма, яку застосовують для записування ігор і ство-рення навчального контенту. Вона дає можливість записувати екран цілком чи лише обрану користувачем прямокутну ділянкуабо виділене вікно з інтерфейсом потрібного додатка. Є можливість вручну підганяти розміри захоплюваної області, а також записувати разом з відео ще й звук з мікро-фона, колонки або іншого пристрою. У вбудованому редакторі в уже готовий ролик можна додати звук, повністю замінити звукову доріжку або відредагувати аудіо. Під час захоплення екрана утиліта вміє підсвічувати клацання миші та показувати натиснуті комбінації клавіш.
https://winsoft.com.ua/ windows/multimedia/zapis-z-ekrana/uvscreencamera	

За допомогою яких техніко-криміналістичних засобів забезпечується фіксація цифрових матеріалів з відкритих джерел мережі «Інтернет»?

Якісну фіксацію цифрових матеріалів (доказів) з відкритих джерел мережі «Інтернет» можна забезпечити цифровими засобами фіксації фото- та відеозображень.

До фотофіксуючих засобів належать сучасні фотоапарати або цифрові камери. Під час проведення СРД рекомендуємо застосовувати

професійні цифрові камери, до яких належать цифрові дзеркальні фотоапарати (DSLR – Digital Single Lens Reflex Cameras).

Важливо! Використовувати MIRRORLESS-групу цифрових бездзеркальних фотоапаратів не рекомендується у зв'язку з низькою якістю зображень. До них належать усі камери, у тому числі й мобільних ґаджетів, у яких спрощений (порівняно з DSLR) принцип роботи.

Для належної відеофіксації ходу СРД-огляду цифрових матеріалів з відкритих джерел рекомендуємо використовувати *цифрові відеокамери.* Наведемо приклади сучасних цифрових відеокамер, які оптимально придатні для проведення фіксації роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет».

Найпопулярнішими на 2024 рік є:

• *Flash-відеокамери*, які використовують як носій флеш-пам'яті. Камера такого виду має дуже низьке енергоспоживання, вона невелика за розміром і вагою, в ній немає рухомих елементів. Відеокамера може мати як вбудовану флеш-пам'ять, так і спеціальний слот для карт пам'яті. Відео можна записувати у форматах MPEG-2 або AVCHD, але флеш-пам'ять завжди має обмежену ємність, тому треба або вчасно змінювати флеш-карту, або переписувати отримане відео на комп'ютер чи зовнішній диск.

• *HDD-відеокамери* з можливістю записувати відео на вбудований жорсткий диск (від англ. Hard Disk Drive). Принцип дії аналогічний DVD-відеокамерам, але як носій використовується жорсткий диск. На HDD записується відео у форматі MPEG-2 зі стандартною роздільною здатністю 720x576. AVCHD-HDD – різновид HDD-відеокамер з підтримкою формату запису відео високої чіткості в режимах 720p, 1080i та 1080p.

Перевагою такої відеокамери є велика ємність носія, який використовується в HDD-відеокамері. На жорсткий диск обсягом 30 Гбайт можна записати до 12,5 годин відео з чудовою якістю. Оскільки жорсткий диск є незнімним носієм, зростає надійність, адже під час зміни касети або DVD в механізм камери може потрапити пил.

• *HDV (High Definition Video)* – відеостандарт, який забезпечує запис відео високої роздільної здатності (720 рядків із прогресивною розгорткою або 1080 рядків з чергуванням рядків). Відеокамери стандарту HDV зазвичай підтримують також запис відео зі стандартною роздільною здатністю (720×576).

5.1.3. Основи безпеки роботи з цифровими матеріалами з відкритих джерел у мережі «Інтернет» (тактичні й технічні аспекти)

Дані, що містяться в Інтернеті у відкритому доступі (на вебсайтах), зазвичай оглядаються слідчими з використанням службового комп'ютера з доступом до Інтернету та програмного забезпечення веббраузера. Комп'ютерні дані, що містяться на публічних ресурсах у межах сторінок, груп, пабліків у месенджерах (Telegram, Viber, WhatsApp, Signal, WeChat тощо), можуть бути оглянуті з використанням вебверсії відповідного месенджера засобами програми веббраузера, а якщо немає вебверсії – з використанням програми-клієнта такого месенджера[372].

Будь-які дії з комп'ютерними даними мають здійснюватися уповноваженими особами суто за допомогою сертифікованого та справного службового обладнання, з використанням ліцензійного програмного забезпечення.

Використання несертифікованого, несправного обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з комп'ютерних даних, через апаратні та/або програмні збої й помилки[373].

Враховуючи специфіку категорії злочинів проти миру, безпеки людства та міжнародного правопорядку, перед початком роботи з цифровими матеріалами з відкритих джерел суб'єкту, уповноваженому на здійснення досудового розслідування, важливо забезпечити цифрову безпеку. Про необхідність дотримання слідчими мінімальних стандартів безпеки під час роботи з цифровою інформацією з відкритих джерел йдеться у Главі IV Ⓑ Протоколу Берклі. Міркування безпеки мають бути подвійними:

1) пов'язаними з Інфраструктурою, включаючи апаратне забезпечення, програмне забезпечення та мережі;

2) пов'язаними з поведінкою, включаючи поведінку слідчих та всіх тих, з ким вони спілкуються.

Оцінку безпеки слід проводити на трьох рівнях, включаючи рівень організації, конкретне розслідування/справу та конкретні заходи/завдання[374].

---

[372] Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту*. Вип. 4. 2023. С. 55. URL: https://doi.org/10.32999/ksu2307-8049/2023-4-9

[373] Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналістів. *Вісн. Нац. акад. правов. наук України*: зб. наук. пр. 2017. № 1 (88). С. 184.

[374] Протокол Берклі … .

У Протоколі Берклі йдеться, що під час розслідування з використанням даних у відкритому доступі слідчі мають дотримуватися мінімальних стандартів безпеки, а саме:

– зберігати свою анонімність в Інтернеті та стежити за тим, щоб їх діяльність в Інтернеті не була віднесена до них, наскільки це можливо;

– проводити діяльність в Інтернеті з розрахунком на те, що таку діяльність можуть контролювати та аналізувати треті сторони;

– знати, що надмірне використання єдиного онлайн-джерела інформації, такого як певний сайт, може збільшити ризик моніторингу та аналізу сторонніми особами, тому їм слід запровадити практику мінімізації цієї ймовірності, наприклад, урізноманітнювати цифрові джерела;

– уникати ідентифікованих або передбачуваних моделей поведінки, таких як повторювані шаблони пошуку на пристроях, які ідентифікуються, що може допомогти третій стороні визначити цілі розслідування;

– розмежовувати свою професійну роботу та особисту діяльність в Інтернеті. Особисті облікові записи в мережі та, наскільки це можливо, особисте обладнання не можна використовувати для професійних розслідувань, а професійне обладнання ніколи не має використовуватися для особистої діяльності в Інтернеті;

– використовувати технічні системи чи середовища, які піддаються мінімальному впливу можливого впровадження агресивного чи шкідливого програмного забезпечення або іншим руйнівним впливам, які можуть виникнути під час діяльності;

– фіксувати час початку та закінчення кожного розслідування, зберігати дані та документацію для кожного розслідування в окремих місцях.

Для убезпечення робочого комп'ютера і збереження досліджуваних даних від видалення антивірусними програмами науковці, практики вважають за доцільне здійснювати огляд даних із застосуванням «віртуальних машин[375] або комп'ютера, який використовується лише для кіберрозслідувань».

Окрім цього, особа, яка проводить огляд (або залучений спеціаліст), має вжити заходів для недопущення внесення змін до даних, що оглядаються під час їх дослідження[376].

---

[375] Криміналістика: криміналістична техніка: навч. посіб. / [Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін.]; МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2023. 124 с.

[376] Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту.* Вип. 4. 2023. С. 54. URL: https://doi.org/10.32999/ksu2307-8049/2023-4-9

Що таке віртуальні машини?

Віртуальні машини – це екземпляри однієї або кількох операційних систем на одному комп'ютері (який називають «хостом»), якими можна керувати одночасно. На хості встановлено програмне забезпечення віртуалізації.

Хост емулює абсолютно окреме апаратне забезпечення віртуального комп'ютера (пам'ять, мережа, периферійні пристрої тощо) у кожній окремій віртуальній машині (також називається гостьовою системою), яке сумісне з найпоширенішими операційними системами. Це забезпечує відокремлення «накопичувачів інформації» від звичайної робочої станції, де зберігаються електронні листи, робочі системи та документи. Наприклад, збирати дані можна у віртуальній машині, а їх дослідження та аналіз можна виконувати на робочій станції. Обмін файлами між хостом і віртуальною машиною або між віртуальними машинами може здійснюватися через зовнішні диски, мережу чи за допомогою механізмів, наданих програмним забезпеченням віртуалізації.

Віртуальну машину доцільно використовувати, якщо конфігурація комп'ютера дозволяє встановити програмне забезпечення віртуальних машин. Якщо це програмне забезпечення планується встановити на вживаний комп'ютер, попередньо його потрібно повністю переформатувати і переустановити все програмне забезпечення, що може призвести до видалення всіх даних з комп'ютера. Тому обов'язково треба створити резервну копію всіх важливих даних.

Під час використання віртуальної машини потрібно:

1. Створити окремий акаунт рівня адміністратора в операційній системі.

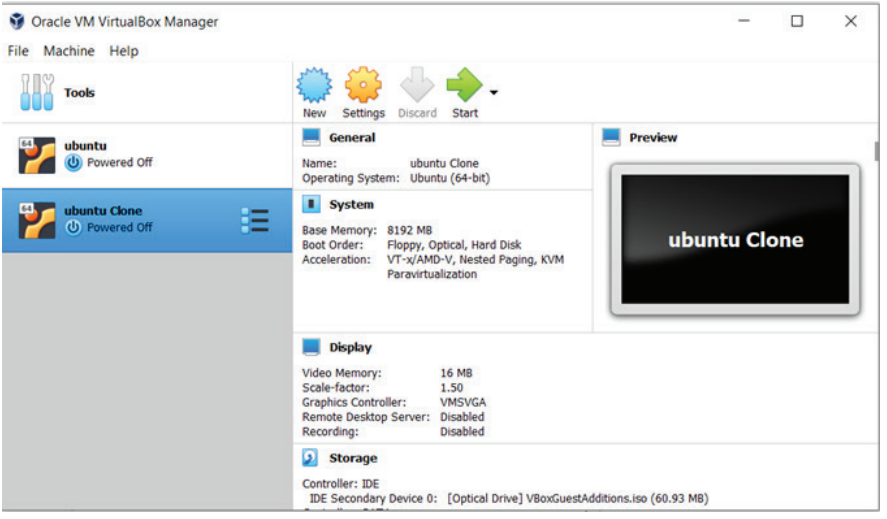
За допомогою натискання комбінації клавіш Win+R потрібно ввести lusrmgr.msc у вікно «Відкрити» і натиснути клавішу «Enter». Потім вибрати групу «Користувачі» і в пункті «Дія» вибрати підпункт «Новий користувач».

2. Застосовувати захист до хосту, включаючи програмне забезпечення для захисту від шкідливих програм і рішення віртуальної приватної мережі (VPN).

Для прикладу наведемо такі найпоширеніші віртуальні машини Oracle VM VirtualBox та WMWare Workstation:

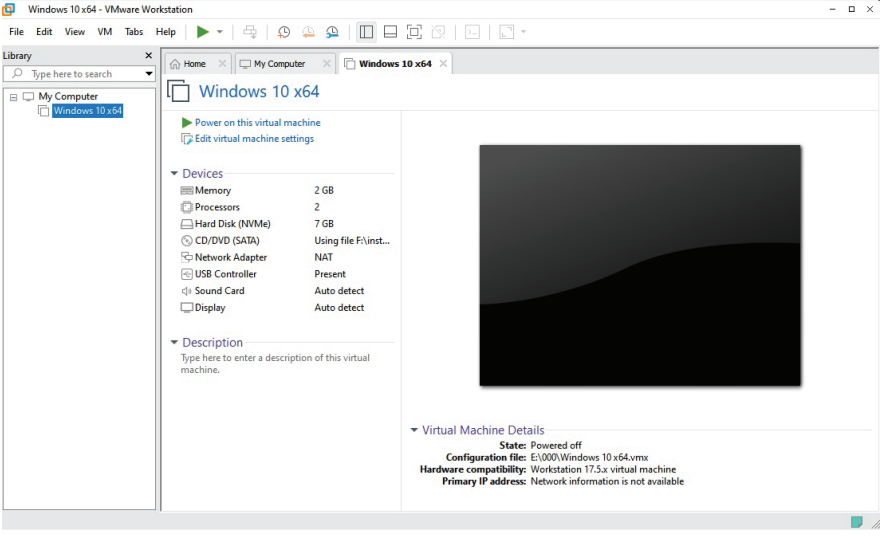
- Oracle VM VirtualBox: https://www.virtualbox.org





Приклад Oracle VM VirtualBox – Linux Ubuntu

- WMWare: https://www.vmware.com/products/workstation-player.html



Приклад WMWare Workstation – MS Windows 10

На віртуальні машини рекомендовано встановити операційну систему (наприклад, Windows 10/11) з антивірусним захистом та браузери з можливістю відкривати заблоковані сайти (наприклад, Opera з openvpn).

Які Інтернет-браузери рекомендується використовувати під час огляду цифрової інформації з відкритих джерел?

Для документування цифрових доказів в мережі «Інтернет» можна використовувати різні Інтернет-браузери. Важливо постійно оновлювати ці браузери, щоб усунути можливі вразливості.

Загалом **найбільш використовуваним браузером є Mozilla Firefox**, і цьому є декілька причин:

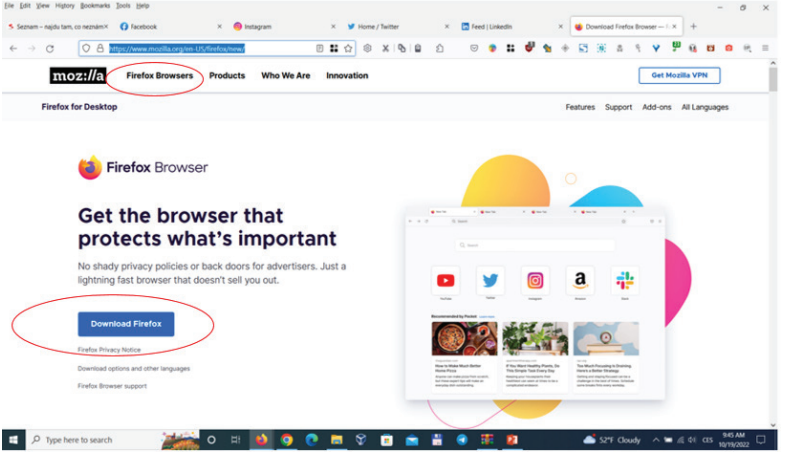
– включено до встановлення Virtualbox / Linux Ubuntu як браузера за замовчуванням;

– інсталяція Firefox є набагато більш конфіденційною та безпечною, ніж інші браузери.



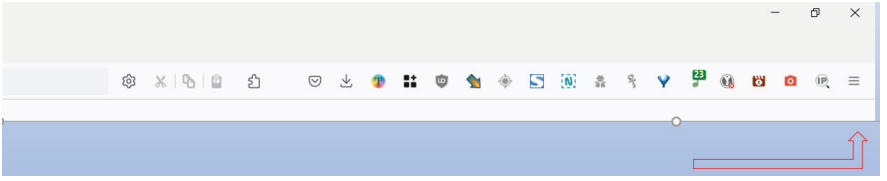
Браузер **Mozilla Firefox** є найбільш надійним і безпечним і підходить для кіберрозслідувань і документувань (фіксації) цифрових доказів у мережі «Інтернет».

Завантаження та налаштування Firefox можна здійснити перейшовши на сторінку Mozilla.org.



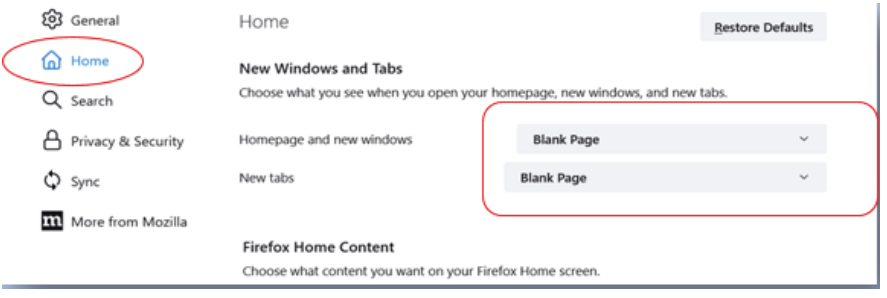
Водночас для найбільш ефективної та безпечної роботи браузера Mozilla Firefox рекомендується змінити такі налаштування:

• Натисніть на меню у верхньому правому куті та виберіть «Параметри» або «Налаштування».



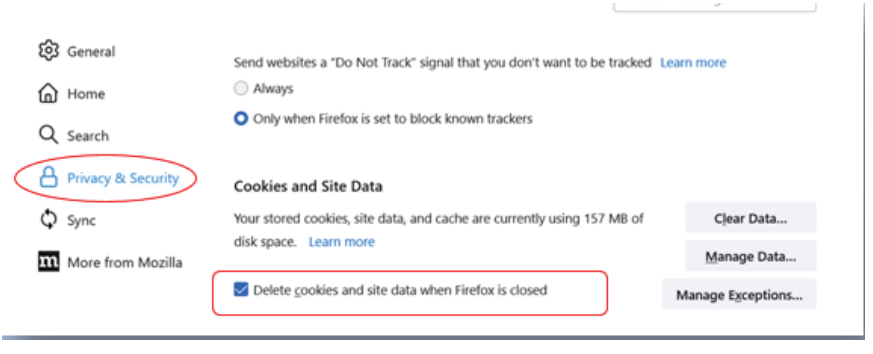
• У параметрах «Загальні» зніміть прапорці «Рекомендувати розширення під час перегляду» та «Рекомендувати функції під час перегляду». Це запобігає надсиланню певної інформації про використання Інтернету до Firefox.

• У параметрах «Домашня сторінка» змініть «Домашня сторінка та нові вікна» та «Нові вкладки» на «Порожня сторінка». Це не дозволяє Firefox завантажувати свої служби на нових сторінках і вкладках.

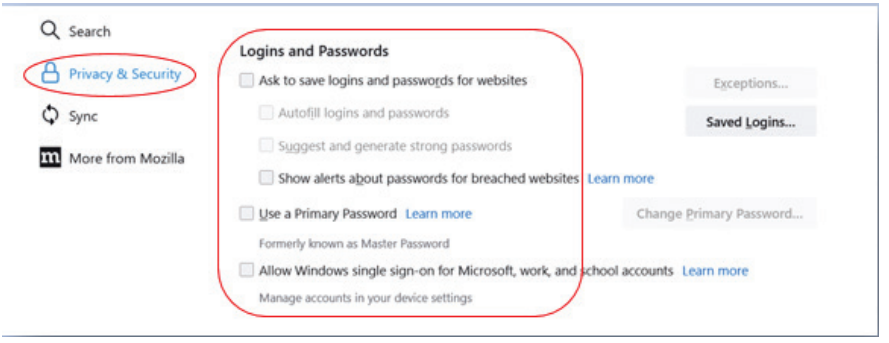


• У параметрах конфіденційності та безпеки виберіть опцію «Строгий» у розділі «Блокування вмісту».

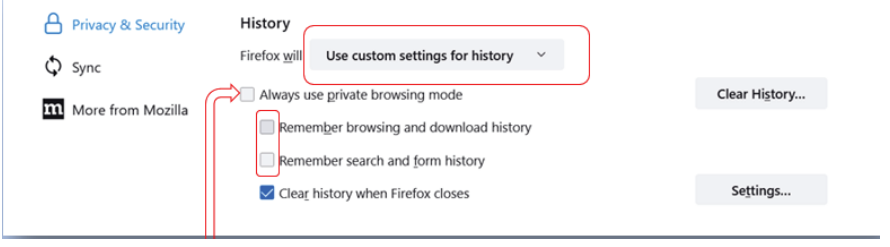
• Поставте прапорець «Видалити файли cookie та дані сайту, коли Firefox закрито».



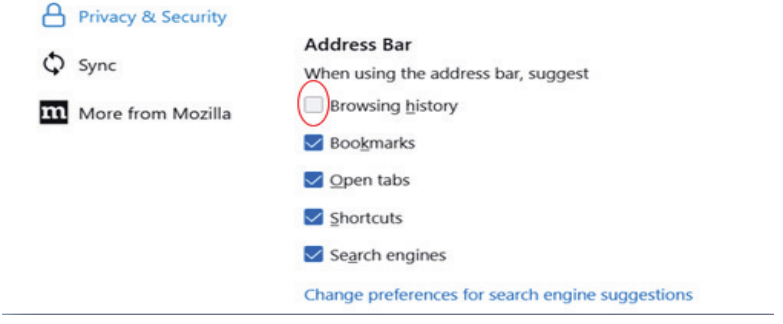
• Зніміть прапорець «Запитувати збереження логінів і паролів для вебсайтів».



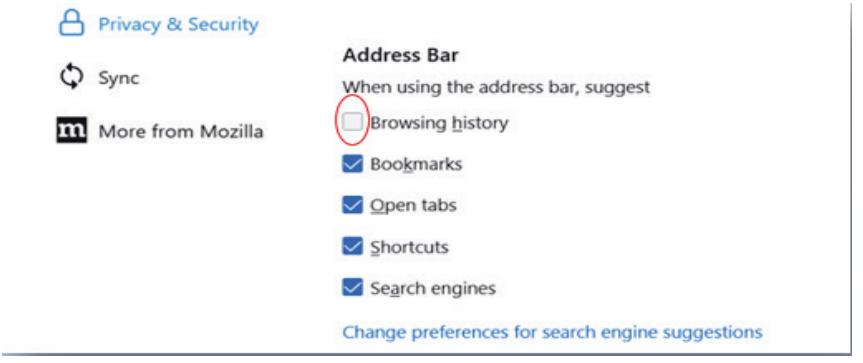
• Змініть параметр «Історія» на «Firefox використовуватиме спеціальні налаштування для історії».



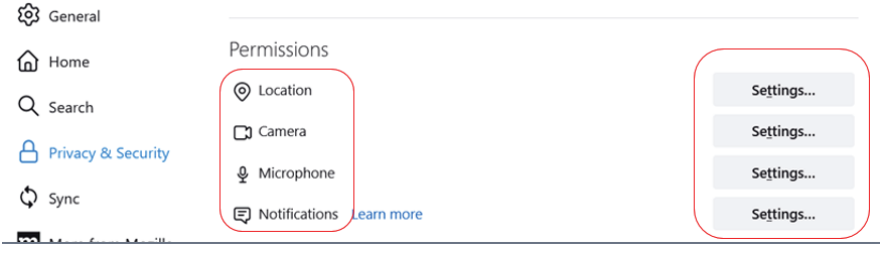
• Зніміть прапорці «Запам’ятовувати історію перегляду та завантажень» і «Запам’ятовувати історію пошуку та форм».



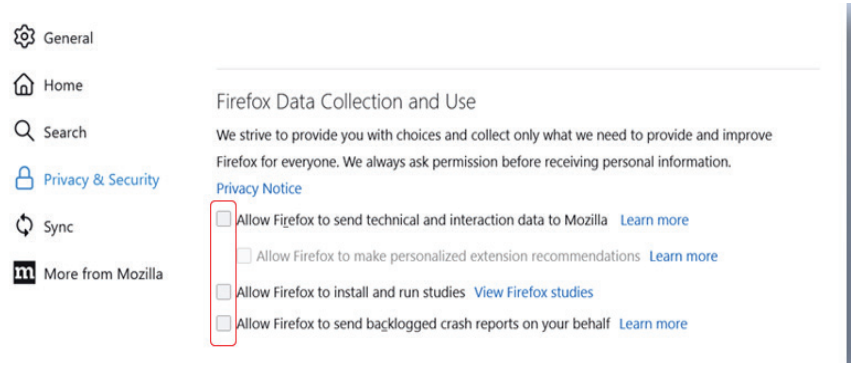
• Поставте прапорець «Очищати історію, коли Firefox закривається».
• Зніміть прапорець «Історія перегляду» в меню «Адресний рядок».



• У меню «Дозволи» клацніть «Налаштування» біля «Місцезнаходження», «Камера», «Мікрофон» і «Сповіщення». Поставте прапорець «Блокувати нові запити...» для кожної з цих опцій.



• Зніміть прапорці з усіх опцій у розділі «Збір і використання даних Firefox».



Для Firefox також доступно багато розширень, деякі з яких є корисними в кіберрозслідуваннях. Ви можете встановити розширення, коли Firefox відкрито, клацнувши меню у верхньому правому куті, а потім «Додатки». Відкриється сторінка з полем пошуку у верхньому правому куті. Введіть назву розширення та встановіть його звідти. Ось **кілька рекомендованих розширень**:

- **uBlock Origin** – блокує завантаження небажаних сценаріїв.
- **Bulk Media Downloader** – автоматично завантажує масові медіафайли.
- **VideoDownloadHelper** – завантажує медіа зі сторінки одним натисканням кнопки.
- **FireShot** – створює скріншоти часткових і цілих вебсторінок.
- **Nimbus** – забезпечує альтернативне захоплення екрана для великих вебсторінок.
- **Exif Viewer** – ідентифікує метадані, вбудовані у фотографію.
- **Перемикач агентів користувача** – емулює різні браузери та пристрої.
- **Параметри пошуку зображень** – проводить автоматичний зворотний пошук зображень.
- **Копіювати вибрані посилання** – швидко копіює всі гіперпосилання з вебсайту.



Іншим потужним браузером є Google Chrome (https://www.google.com/chrome/)

Для пошуку в Інтернеті можна використовувати адресний рядок (універсальне вікно пошуку). У деяких країнах стандартною пошуковою системою у Chrome є Пошук Google. В інших її потрібно буде вибрати. Ви можете будь-коли змінити стандартну пошукову систему.

Ви можете швидко знаходити потрібну інформацію в Інтернеті, закладках та історії вебперегляду. Функція Chrome може бути недоступна, якщо ваша стандартна пошукова система її не підтримує.

- Відкрийте Chrome на комп'ютері.
- Введіть пошуковий запит в адресному рядку вгорі сторінки.
- Виберіть результат або натисніть клавішу Enter.

Підказка. Під час введення запиту ви можете отримувати пропозиції на основі історії додатків і вебпошуку. Ви можете видаляти пропозиції з історії пошуку або ховати розділи пропозицій, що підбираються на основі ваших дій.

Налаштування головної та стартової сторінки: можна зробити будь-яку сторінку головною або стартовою в Google Chrome. Це дві різні сторінки, але їх можна зробити однаковими.

Стартова сторінка відкривається першою, коли ви запускаєте Chrome на пристрої. Головна сторінка відкривається, коли ви натискаєте значок Домашня сторінка. Якщо ваша стартова або головна сторінка чи пошукова система раптом змінилися, можливо, у вас установлено небажане програмне забезпечення.

Щоб керувати пошуковими системами й командами для пошуку на сайтах, можна додавати, змінювати й вилучати команди для пошуку на сайтах і налаштувати типову пошукову систему.

Для цього потрібно:

1. Відкрити Chrome на комп'ютері.
2. Угорі праворуч вибрати значок **«Налаштування»**.
3. Ліворуч вибрати **«Пошукова система»** → **«Керувати пошуковими системами та пошуком на сайтах»**.
4. Щоб змінити команди для пошуку на сайтах:

- **Додати.** Праворуч від опції «Пошук на сайтах» виберіть **«Додати»**. Заповніть текстові поля й виберіть **«Додати»**.
- **Змінити.** Праворуч від команди для пошуку на сайтах виберіть позначку ✎.
- **Установити за умовчанням.** Праворуч від команди для пошуку на сайтах виберіть значок ⋮ › «**Установити за умовчанням»**.
- **Вимкнути.** Праворуч від команди для пошуку на сайтах виберіть значок ⋮ › **«Вимкнути»**.
- **Видалити.** Праворуч від команди для пошуку на сайтах виберіть значок ⋮ › **«Видалити»**.

Підказки:

- Можна налаштувати команди для пошуку на конкретних сайтах.
- Команди для відкритих вкладок, закладок та історії вебперегляду увімкнено для пошуку на сайтах. Ви можете змінювати й вимикати ці команди, але їх не можна видалити.
- Якщо вимкнути команду для пошуку на сайтах, вона переміститься в розділ «Неактивні команди».
- У цьому розділі також можна переглянути інші пропоновані сайти. Щоб додати їх до команд для пошуку на сайтах, натисніть **«Активувати»**.
- Деякі сайти з'являються в розділі «Неактивні команди» лише після того, як ви виконали на них пошук.

Приклади інших інтернет-браузерів:

• Браузер Brave – https://brave.com/



• Microsoft Edge – https://www.microsoft.com/en-us/edge



• Opera – https://www.opera.com/



Іншим хорошим варіантом є використання анонімного браузера, такого як браузер Tor (https://www.torproject.org/download/). Це дозволяє замаскувати вашу IP-адресу та створити враження, що ви переглядаєте Інтернет з неправдивого місцезнаходження, залишаючись анонімним.

Дуже важливо мати обліковий запис електронної пошти, особливо створений для кіберрозслідувань.

Кожна соціальна мережа вимагає адреси електронної пошти як частину реєстрації облікового запису, і ви ніколи не повинні використовувати старий обліковий запис електронної пошти.

Надзвичайно важливо залишатися анонімним, коли ви досліджуєте соціальні мережі, і набагато важливіше, щоб ваша електронна пошта залишалася непоміченою, якщо ви хочете уникнути будь-якого стеження.

Є захищені служби електронної пошти, які використовують шифрування для шифрування ваших надсилань і вимагають від отримувача мати пароль, який розшифровує ваше повідомлення.



(https://protonmail.com/)

Якщо вам потрібна служба електронної пошти, яка оброблятиме зашифровані повідомлення, то ProtonMail може надати таку можливість.

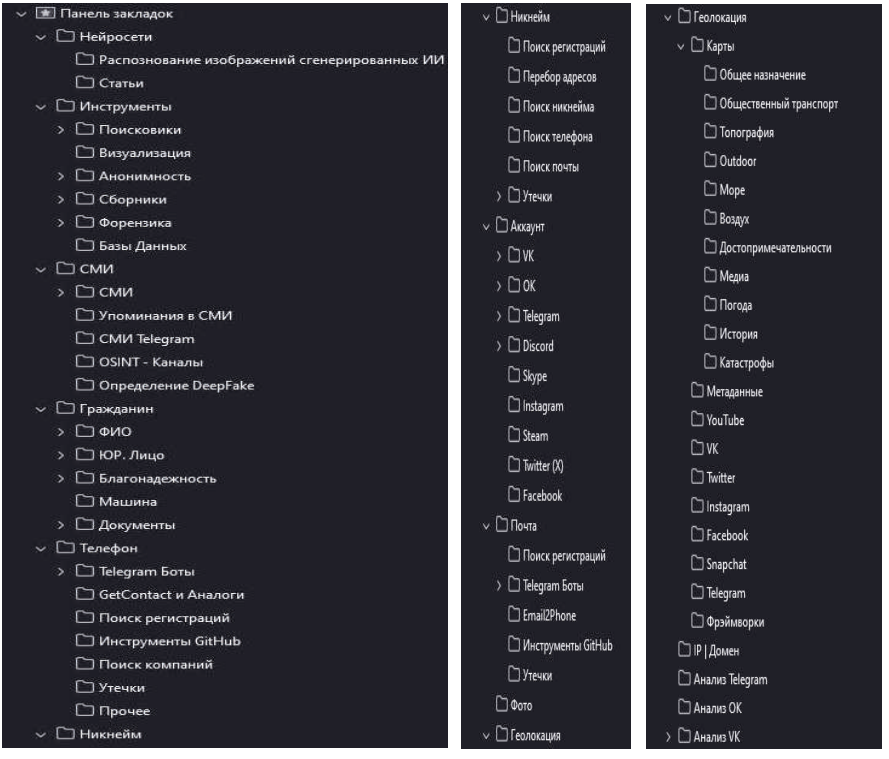
Також з Інтернету (https://t.me/venatorbrowser/81) можна завантажити багатофункціональний OSINT-браузер Venator (назва «Venator» перекладається з латини як «Мисливець»), створений на базі браузера

Librewolf (це такий собі форк Firefox з акцентом на приватність та безпеку) (https://habr.com/ru/companies/tomhunter/articles/809725/). Браузер орієнтований на використання у країнах СНД, що вигідно відрізняє його від таких аналогів, як Oryon, CSI та інших. Інтерфейс браузера містить додаткові панелі для швидкого переходу до пошукових систем, а також до спеціалізованих OSINT-ресурсів, розбитих за темами досліджень (телефон, пошта, нікнейм, сайт тощо).

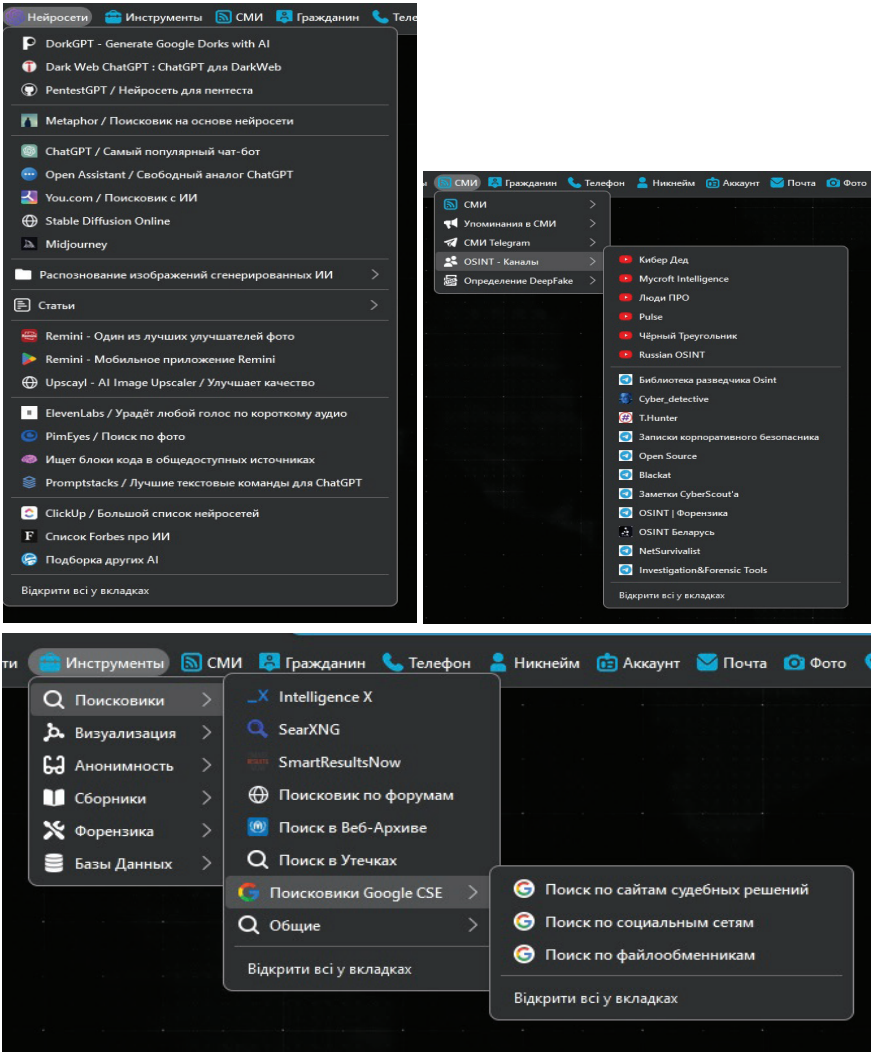
Розробники створили *дві додаткові спеціалізовані версії*:

1) Venator Red – спеціальна збірка браузера для дослідження Даркнету (https://t.me/venatorbrowser/77);

2) Venator Security – версія з підвищеним акцентом на безпеку (https://t.me/venatorbrowser/62).



Перелік закладок різних сервісів
у браузері Venator для пошуку інформації
у відкритих російських джерелах



Приклади детальних посилань на конкретні ресурси у закладках браузера Venator для пошуку інформації у відкритих російських джерелах

Перевірка підключення

Після того, як ви застосували попередні заходи безпеки до вашої системи, перевірте своє з'єднання на **www.ipleak.net**, щоб переглянути поточну IP-адресу, геолокацію та інформацію про систему.

5.2. Пошук, аналіз, виявлення, фіксація та збирання цифрових матеріалів з відкритих джерел у мережі «Інтернет» та їх використання

5.2.1. Особливості пошуку, аналізу та виявлення цифрових матеріалів з відкритих джерел у мережі «Інтернет»

Що таке OSINT і які є особливості пошуку, збирання цифрових матеріалів з відкритих джерел у мережі «Інтернет» з використанням методів та інструментів OSINT?

OSINT (Open source intelligence – розвідка відкритих баз даних) в цілому можна визначити як розвідку інформації, отриманої із загальнодоступних джерел, яка не потребує таємних методів збору[377]. В національній практиці правоохоронних органів використання OSINT надає можливість отримувати інформацію, яка може бути корисною слідчому для прийняття рішення щодо подальшого проведення розслідування.

В експертних колах прийнято поділяти OSINT на активний і пасивний. **Активний** OSINT передбачає цільове збирання даних та інформації для конкретних цілей і на практиці реалізується через пошук інформації та взаємодію з об'єктом дослідження. **Пасивний підхід не** передбачає активної взаємодії з об'єктом дослідження. Такий підхід передбачає лише збирання інформації з відкритих джерел, використовуючи загальнодоступні дані.

Водночас очікуваний результат проведення OSINT-розвідки має бути таким, що відповідає вимогам кримінального процесуального законодавства та потребам слідчого, адже саме слідчий повинний чітко визначати завдання, які мають виконувати оперативні працівники під час проведення відповідних заходів, у тому числі розвідки інформації з відкритих джерел.

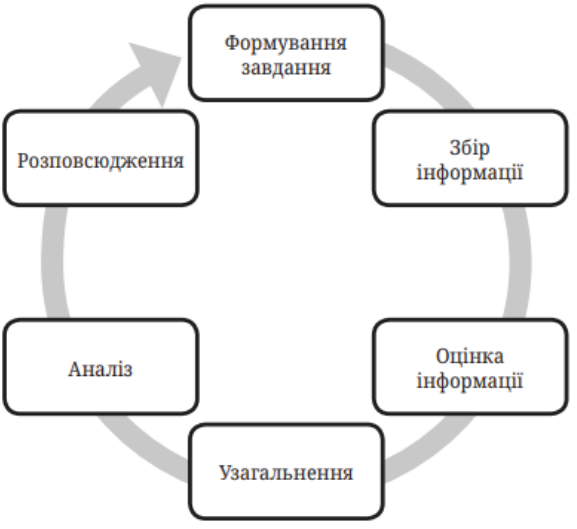
Враховуючи те, що результати роботи з відкритими джерелами, серед іншого, є допоміжною інформацією для слідчого для прийняття того чи іншого рішення в межах виконання службових обов'язків, очевидною є реалізація слідчим повноваження щодо надання запитів на пошук відповідної інформації з відкритих джерел або стосовно моніторингу відкритих джерел інформації.

Отже, важливим на початковому етапі роботи з відкритими джерелами інформації є чітке розуміння мети такої роботи або

[377] Sampson, Fraser. Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *The Police Journal*. 2016. 90. P. 3.

формування уявлення про передбачуваний результат проведення відповідного OSINT-дослідження.

У літературі досить поширеним є цикл проведення розвідки[378], зображений на рисунку.



Цикл проведення розвідки

Після формування завдання відбувається збирання даних, зокрема й із застосуванням інструментарію OSINT. Надалі відбуваються оцінювання узагальнення та аналіз інформації, що найчастіше проводять відповідні підрозділи Департаменту кримінального аналізу Національної поліції України.

Водночас для якісного виконання слідчим його функцій значимою є робота, пов'язана з аналізом отриманих результатів OSINT-дослідження відкритих джерел інформації.

Збирання даних для OSINT-розвідок може відбуватися із будь-яких джерел інформації, однак така інформація має бути перевірена на достовірність, а також оцінено надійність джерела інформації.

Розвідка з відкритих джерел по суті є збором та аналізом інформації з публічно доступних джерел, що можна використовувати для розслідування злочинів, пошуку інформації про людей та організації,

[378] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. - Одеса: Вид-во «Юридика», 2024. С. 10.

а також для відстеження тенденцій і подій. Враховуючи тенденції цифровізації суспільних процесів і загальну інформатизацію суспільства, актуальними є підходи, рекомендовані Протоколом Берклі щодо використання цифрової інформації у відкритому доступі[379].

Безпосередньо інструментарій OSINT включає низку інструментів і методів, які використовуються для збирання, аналізу та обробки відкритих джерел інформації.

Інструментарій OSINT постійно розвивається та вдосконалюється, на 2024 рік є декілька ресурсів, які дозволять ознайомитися з відповідними інструментами.

Найпопулярнішими ресурсами, які акумулюють інструментарій OSINT для роботи з цифровою інформацією, є такі.

• **Osintframework.com** (https://osintframework.com) – найбільший фреймворк інструментів OSINT, структурований за групами їх призначення.

• **Asint_collection** (https://start.me/p/b5Aow7/asint_collection) – один із банків інструментів OSINT.

• **Osint Essentials** (https://www.osintessentials.com) – містить популярні OSINT-інструменти.

Як проводити пошук та аналіз інформації за допомогою інформаційно-пошукових систем з відкритих джерел (Google, Yandex та інших)?

Пошукова система Google (https://www.google.com/search/about/) **є** найпопулярнішою пошуковою системою у світі, яка дозволяє користувачам знаходити інформацію в Інтернеті. Пошукова система Google є досить інформативною, зручною та інтуїтивно зрозумілою в користуванні. В основу роботи системи покладено роботу пошукових роботів Googlebot, які, отримуючи запит, введений користувачем у відповідне пошукове поле, починають автоматично відшуковувати сторінки, які відповідають запиту, в мережі «Інтернет».

Для *стандартного пошуку інформації* потрібно відкрити браузер Google, ввести відповідний запит у поле пошукової системи й натиснути клавішу пошуку, після відповіді пошукової системи обрати задовільний результат.

Для професійних потреб доцільно використовувати й інші можливості пошукової системи Google, окрім стандартного пошукового запиту, який не завжди є достатнім для досягнення бажаного результату.

[379] Регнер, Е., & Тапай, Д. (1990). Протокол Berkeley: специфікація протоколу мережевої безпеки. University of California, Berkeley. https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

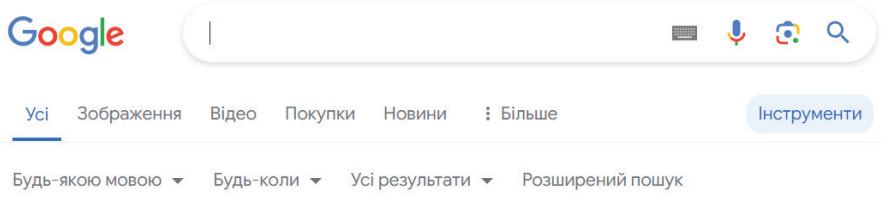
Панель пошукової системи Google надає можливість використовувати такі інструменти, як:

– вибір країни та мови;

– вибір періоду опублікування запитуваної інформації;

– вибір усіх результатів пошуку;

– дослівний пошук.



Панель пошукової системи Google

У випадках, коли *стандартний пошук* за ключовими словами є недостатнім для задоволення потреб з пошуку інформації, доцільно використовувати *оператори пошуку Google* (або *Google Dorks*) – це спеціальні символи або команди, які можна використовувати для уточнення і покращення результатів пошуку в Google.

Застосування операторів пошукової системи надає можливість структурувати пошукові запити. Будь-яка пошукова система використовує оператори пошуку, оскільки вони дають змогу уточнити й сортувати запитувану інформацію відповідно до пошукового запиту. Пошук інформації у такому випадку здійснюється за допомогою та з використанням певних символів і слів.

Логіка використання операторів пошуку відповідає такому принципу:

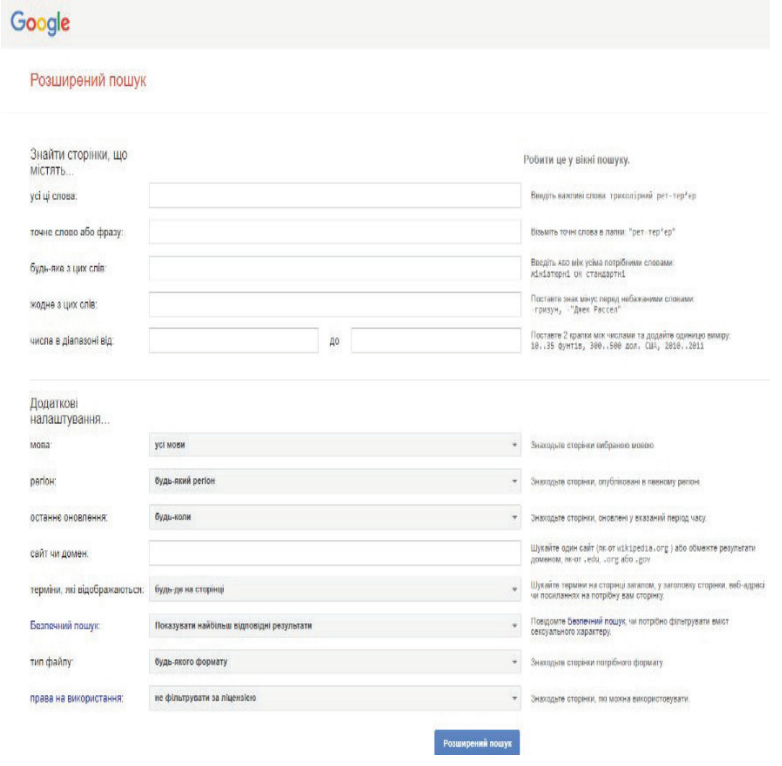
• У пошукове поле браузера вводимо пошуковий запит, який складається з оператора пошуку (або їх комбінації), джерела та ключових слів. Пошук за конкретним словом чи словосполученням дозволяє відшукати запитувану інформацію або конкретне словосполучення, в якому слова розміщені в певному порядку.

• Відтак, використання такого пошукового оператора, як, наприклад, лапки («_»), є корисним, оскільки вони виключають із результатів пошуку значну кількість непотрібних посилань. За таким механізмом доцільно виконувати пошук номерів телефонів або поштові скриньки з різним варіантом написання.

Оператори пошуку Google

site:	Показувати лише результати з певного вебсайту.
«»	Обмежує результати пошуку, які містять точну фразу в лапках.
or чи |	Оператор or покаже результати ключового слова 1 або ключового слова 2, чи обох.
()	Дозволяє групувати кілька запитів чи операторів.
–	Дозволяє унеможливити термін, поставивши перед ним знак мінус.
*	Оператор працює як знак підстановки, шукає ключові фрази, між якими є одне або кілька слів.
related:	Оператор дозволяє шукати схожі сайти на домен у пошуковому запиті.
inurl:	Оператор дозволяє знаходити сайти з певним словом в URL-адресі.
allinurl:	Оператор дозволяє знаходити вебсторінки з певним словом в URL-адресі.
intitle:	Оператор показує у пошуку сторінки, що містять вказане слово у заголовку (Title).
allintitle:	Оператор знаходить сторінки, що містять усі вказані слова в заголовку (Title).
intext:	Оператор показує лише результати у видачі Google, які включають потрібне слово у тексті на сторінці.
allintext:	Оператор показує сторінки, що містять усі вказані слова в title у будь-якій послідовності.
filetype:	Оператор показує лише файли певного типу (PDF, DOCX, TXT, CSV, PPT тощо).
cache:	Оператор дає змогу побачити актуальний кеш вебсторінки.
AROUND(X):	Оператор дозволяє шукати сторінки за словами, розміщеними через певну кількість фраз. У дужках слід вказати число.
site: inurl:	Комбінація операторів дозволяє знаходити сторінки вебсайту з потрібним вам анкором в URL, з якими можна зробити перелінкування.
site: allintitle:	Комбінація операторів дозволяє знаходити сторінки на сайті з потрібним ключовим словом у Title.
inurl: -site.com	Комбінація операторів дозволяє знаходити сайти конкурентів, які ведуть блоґ.
site: -inurl:	Комбінація операторів дозволяє знаходити на сайті незахищені сторінки без https.
site: filetype:	Комбінація операторів дозволяє знаходити різні типи документів чи файлів на одному конкретному сайті.
in title: « « or	Комбінація операторів дає змогу знаходити різні сайти, що дозволяють публікувати у себе партнерські матеріали та гостьові пости з посиланнями.

Якщо треба отримати інформацію з високим рівнем відповідності пошуковому запиту, окрім операторів пошуку Google, доцільно використовувати розширений пошук Google (https://www.google.com/advanced_search). Після переходу на сторінку розширеного пошуку система надає можливість реалізувати додаткові налаштування пошуку.



Сторінка розширеного пошуку Google

Загалом Google пропонує користувачам мережі «Інтернет» велику кількість сервісів і послуг, які можуть стати інструментом пошуку оперативної інформації з відкритих джерел із цієї мережі.

Сервіси Google:

• *Google Статистика пошуку* – дозволяє дізнатись найбільш популярні, а також ті, які швидше за все набирають популярність, запити в заданий відрізок часу.

• *Blogger* – сервіс для ведення блогів, що дозволяє тримати на своєму хостингу не лише програмне забезпечення, а і всю інформацію: записи, коментарі та персональні сторінки в СУБД на серверах Google.

• *Google Docs* – веборієнтований застосунок для роботи з документами, що допускає спільне використання документа. Нині замінений на Google Drive.

• *Google Drive* – хмарне сховище від Google з можливістю перегляду онлайн (у браузері) безлічі типів файлів (зокрема файлів фотошопу). Документи також можна редагувати і створювати в Google Docs. Пропонується 5 Гб вільного місця у безкоштовному тарифі.

• *Gmail* – безкоштовна електронна пошта з великим обсягом місця для зберігання повідомлень (понад 10,1 Гб), з доступом по POP3 і зручним вебінтерфейсом. Також є OpenID-провайдером для всіх служб Google.

• *Google Maps* – набір карт, побудованих на основі безплатного картографічного сервісу.

• *YouTube* – відеохостинг.

Сервіси спеціального пошуку Google:

• *Google Custom Search* – сервіс для створення власної системи пошуку на основі пошукової системи Google.

• *Google Book Search* – повнотекстовий пошук за книгами, оцифрованими компанією Google.

• *Google Images* – сервіс пошуку картинок у пошуковій системі Google.

• *Special Searches* – пошук на спеціалізованих сайтах (BSD, Linux, Mac OS X та Microsoft).

• *Google Patents Search* – пошук за патентами серед понад 7 мільйонів, доступних у базі даних.

• *Google Scholar* – сервіс для пошуку наукових джерел: статей, книг, дисертацій, опублікованих різними науковими організаціями та професійними спільнотами.

• *Google SSL* – безпечний пошук від Google. Зв'язок між користувачем і сервером здійснюється зашифрованим каналом, що виключає можливість перехоплення інформації користувача третіми особами.

• *Google Suggest* – частина пошуку Google, технологія автозаповнення рядка пошукового запиту на основі загальної статистики найпопулярніших запитів.

• *Google Video* – сервіс для пошуку, перегляду і збереження відео.

Інструменти Google:

• *Google Earth* – модель планети Земля, створена за допомогою супутникових знімків.

• *Google Web Accelerator* – програма, яка прискорює роботу браузера шляхом кешування та попереднього скачування інформації,

що, можливо, буде цікавити користувача. Програма використовує проксі-сервери, що належать Google.

• *Google Toolbar* – розширення для браузерів Internet Explorer і Mozilla Firefox, що являє собою панель пошукового сервісу Google і виконує ряд додаткових функцій.

Які альтернативні пошукові системи можна використовувати для пошуку цифрових матеріалів з відкритих джерел?

Пошукова система компанії Google є найбільш популярною серед користувачів мережі «Інтернет», окрім того, вона накопичує величезну кількість інформації про користувачів, які своєю роботою з мережею «Інтернет» залишають велику кількість цифрових слідів. Нині Google проіндексував більше HTML-сторінок у мережі, ніж будь-який інший браузер.

Водночас під час роботи доцільно використовувати й інші пошукові системи, які за логікою свого використання та методологією роботи з ними є схожими. Фахівцям можуть бути корисні такі пошукові системи (список не є вичерпним):

• *Microsoft Bing* (https://www.bing.com) – пошукова система від компанії Microsoft.

• *Yandex* (https://yandex.ru) – пошукова система, поширена на території Росії, Білорусі та Казахстану, в Україні заблокована (доступ можливий через VPN), є однією з кращих пошукових систем рунету.

• *Duckduckgo* (https://duckduckgo.com) – відома пошукова система без цензури.

• *Startpage* (https://www.startpage.com) – анонімна пошукова система, яка дозволяє знаходити ті ж результати, що і пошукова система Google, але без трекінгу.

• *Gibiru* (https://gibiru.com) – пошукова система, яка позиціонує себе як така, що не використовує файли cookie, завдяки чому працює швидше порівняно з іншими пошуковими системами.

• *Swisscows* (https://swisscows.com/uk) – анонімна пошукова система, яка не проводить трекінгу користувачів та не використовує унікальні ідентифікатори користувачів, що дає можливість користувачу зберігати певний ступінь анонімності в мережі.

Також доцільно використовувати українські пошукові системи, наприклад *Meta* (https://meta.ua/uk/) або *Search.com.ua* (https://search.com.ua).

Водночас звертаємо увагу і на *метапошукові системи*, які, не маючи пошукового індексування сторінок у мережі «Інтернет»,

формулюють видачу пошукового запиту за рахунок міксування та ранжування результатів пошукових запитів інших пошукових систем, таких як Google та Bing.

Популярними метапошуковимим системами є такі:
- *Carrot* (https://search.carrot2.org/#/search/web).
- *Excite* (https://www.excite.com).
- *Intelx* (https://intelx.io/tools).
- *Izito* (https://www.izito.com).
- *Webmii* (https://webmii.com).
- *Yippy* (https://yippy.com).

Які є методи та інструменти пошуку й аналізу відео- і фотозображень, а також розпізнавання обличчя?

Пошук оперативно значимої інформації за фото або відео не відрізняється від звичайного пошуку інформації в мережі «Інтернет» за допомогою будь-якої пошукової системи. Водночас умовою такого пошуку є робота з фото- та відеоконтентом, як наслідок користувач отримає результати свого запиту у формі фото- або відеофайлів.

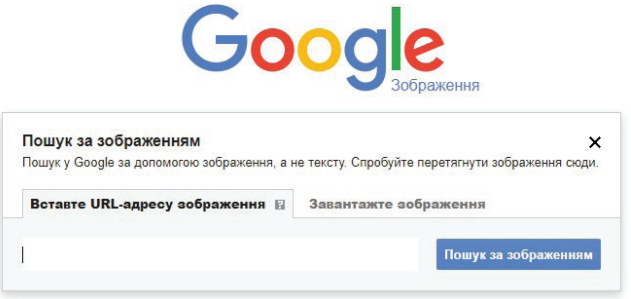
Робота із зображеннями та фото

Методологія роботи із зображеннями та фото зводиться до двох підходів їх опрацювання. У першому випадку в поле пошуку вводиться текст, який описує зображення (або фото) чи якимось чином його характеризує.



Вікно пошуку фото і зображень

У другому випадку пошук здійснюється за зображенням – пошук активується натисканням відповідної іконки в полі пошуку (на рисунку вище – крайня іконка зліва).



Вікно завантаження фото або посилання на нього

У результаті цього в полі пошукового запиту з'явиться можливість або розмістити фото, за яким потрібно зробити пошук, завантаживши його, якщо фото розміщене на комп'ютері, або посилання на фото, якщо воно розміщене в мережі «Інтернет».

Якщо ввести в поле пошукового запиту текстовий опис фото, у результатах пошуку можна отримати зображення, а натиснувши на зображення, можна збільшити його розмір у вікні браузера та отримати доступ до відображення посилання на ресурс (сайт), на якому воно розміщене.

З точки зору роботи із зображеннями як джерелами інформації доцільно наголосити на можливості зворотного пошуку за зображенням (фото), де воно є джерелом інформації. Під час зазначених маніпуляцій з таким зображенням (або фото), окрім очевидних речей, що зображені на фото, потрібно аналізувати метадані, аналогічні зображення, та можливі збіги з іншими фото за змістом (або частковим змістом).

Пошукові системи, які мають потрібний функціонал:

- *Microsoft Bing* (https://www.bing.com).
- *Google Зображення* (https://images.google.com).
- *Яндекс Картинки* (https://yandex.ru/images/).
- *Yahoo* (https://images.search.yahoo.com).

Є ще кілька спеціальних сервісів, які дозволяють працювати із зображеннями:

- *ImageSearch* (https://www.image-search.org).
- *PimEyes* (https://pimeyes.com/en).
- *ReverseImageSearch* (https://www.reverseimagesearch.com).
- *Reverse-image-search* (https://www.reverse-image-search.org).
- *TinEye* (https://tineye.com).

Під час аналізу зображень та фото доцільно звертати увагу на їх походження. Аналізоване зображення чи фото може бути частиною

іншого зображення або містити інші елементи (пейзажі, фото осіб тощо), що може бути предметом повторного та більш детального аналізу.

Зворотний пошук може виявитися малорезультативним через деякі фактори (непроіндексованість сторінок, низьку якість фото, невдалий ракурс тощо), у такому випадку доцільно використовувати метадані фото.

Працюючи з контекстним меню файлу, яке відкриваємо, натиснувши на праву кнопку миші через вкладу «Властивості», слід звернути увагу на формати запису допоміжних метаданих зображення – EXIF-відомості (тип, вид і параметри налаштування камери пристрою, на який було зроблено фото, дату, час, координати зйомки тощо). Утім, слід зважати на те, що такі дані можуть бути цілеспрямовано відредаговані. Крім того, зазначені дані автоматично втрачаються за умови редагування фото та/або його публікації в соціальних мережах чи під час передачі його через месенджери.

Для встановлення EXIF-даних корисними є ресурси *Exifdata* (https://exifdata.com) та *Onlineexifviewer* (https://onlineexifviewer.com).

Для визначення геолокації за зображенням (фото) у пригоді можуть бути такі інструменти:

- *Google Streetview* (https://www.google.com/streetview/).
- *Google Maps* (https://www.google.com/maps/).
- *Imagehunter* (https://imagehunter.apollomapping.com).
- *Mashedworld* (https://data.mashedworld.com/dualmaps/map.htm).
- *Geohints* (https://geohints.com).
- *Geonames* (https://www.geonames.org).
- *Openstreetmap* (https://www.openstreetmap.org/).
- *Osm finder netlify* (https://osm-finder.netlify.app).
- *Pic2map* (https://www.pic2map.com).

Інструментарій аналізу погодних умов, дати та часу фотозйомки:

- *Wolframalpha* (www.wolframalpha.com).
- *Andrewmarsh* (https://andrewmarsh.com).
- *Meteoblue* (https://www.meteoblue.com).
- *Mooncalc* (https://www.mooncalc.org).
- *Shadowmap* (https://shadowmap.org).
- *Toolpie* (https://www.toolpie.com).

Робота з відео

Загальні принципи та методи роботи з відео аналогічні пропонованим підходам до роботи із зображеннями та фото.

У роботі з відео доцільно використовувати можливості пошукових систем та шукати відео за ключовими словами, іменами, назвами тощо, а також використовувати сортування за різними критеріями.

Цінними у практичній роботі з відео є такі сервіси: *Google Video* (https://www.google.com/videohp), *Яндекс Відео* (https://yandex.ru/video/) та *Yahoo video search* (https://video.search.yahoo.com/).

Також доцільно здійснювати пошук за ключовими словами у різних соціальних мережах (у тому числі з використанням пошукових операторів), під час перегляду прямих ефірів (стрімів) та аналізу відеохостингів.

Для аналізу відео (зокрема за кадрами) доцільно використовувати *Scene Edit Detection* (https://huggingface.co/spaces/fffiloni/scene-edit-detection) та *Youtube DataViewer* (https://citizenevidence.amnestyusa.org).

Разом з тим, під час аналізу відео важливо враховувати деталі, які можуть свідчити про недостовірність відео (склеювання кадрів, невідповідність аудіо, відзеркалення, розмитість кадрів та зміна їх розмірів).

У розпізнаванні обличчя з метою успішної роботи доцільно використовувати актуальні інструменти, адже в сучасних умовах інструментарій є мінливим.

У практичній діяльності можуть бути використані такі інструменти:

• *Search4faces* (https://search4faces.com/search.html) – ресурс для пошуку людей в мережі «Інтернет» за фото (працює на основі нейромереж, що забезпечує швидкість результату). Результатом є активне посилання на зображення в мережі або посилання на профіль знайденої людини в соціальній мережі.

• *Facecheck* (https://facecheck.id) – ресурс для пошуку людей в мережі «Інтернет» за фото.

• *Neuroidentigraf* (https://identigraf.center) – система розпізнавання обличчя, створена на основі нейромережі.

Які є особливості пошуку та аналізу за фрагментарними даними фізичних осіб з використанням соціальних мереж (Facebook, Instagram тощо)?

Для роботи з соціальними мережами *доцільно створити «робочий» профіль*, який би імітував реальну особу, з історією публікацій (постів), інтересами та хобі. Такий профіль має бути активним і не викликати підозри про його фіктивність. Такий профіль має містити друзів, фото, підписки й відомості про особу.

Для оформлення відповідного профілю корисними є такі ресурси:

• *Fakeinfo* (https://fakeinfo.net).

• *Fake Details Generator* (https://fakedetail.com).

- *Fake Name Generator* (https://www.fakenamegenerator.com).
- *GMX FreeMail* (https://www.gmx.com/consentpage).
- *Meragor.com* (https://meragor.com/avatar).
- *Random Face Generator* (https://thispersondoesnotexist.com).
- *Temp-mail.org* (https://temp-mail.org).
- *Thispersondoesnotexist.com* (https://this-person-does-not-exist.com/en).
- *Thisresumedoesnotexist.com* (https://thisresumedoesnotexist.com).
- *CardGeneration* (https://cardgenerator.org).
- *CardGuru* (https://cardguru.io).
- *CG II* (https://cardgenerator.io).
- *VCCGenerator* (https://www.vccgenerator.org/#google_vignette).

Також будуть корисними сервіси, які пропонують придбати готові акаунти в соціальних мережах:

- *Accsmarket.com* (https://accsmarket.com/ru).
- *Install-shop.org* (https://install-shop.org).
- *Olimp-shop.net* (https://olimp-shop.net).
- *Smsactivate.org* (https://sms-activate.org/ru) та інші.

Соціальні мережі можуть містити масив інформації про особу, її коло контактів та інтереси. Шукаючи інформацію про людину в соціальних мережах, доцільно аналізувати всю її вхідну та вихідну активність, що включає згадування про неї в постах третіх осіб. Певну інформацію можна отримати з геоміток у профілі особи, а порівнявши їх із часом доби та за певний проміжок часу, можна встановити райони місця роботи та дому й місця частого відвідування.

З метою перегляду загальнодоступної інформації про будь-якого користувача соціальної мережі «Facebook» доцільно використовувати такий інструмент, як *StalkFace* (https://stalkface.com/en/), який дозволяє переглядати всю загальнодоступну інформацію сторінки соціальної мережі хронологічно та за різними критеріями пошуку запитуваної до перегляду інформації. Оскільки відомості, наведені самим користувачем соціальної мережі, містяться у відкритому доступі, з ними можна вільно працювати.

Для пошуку людей в соціальній мережі «ВКонтакте» доцільно використовувати сервіс *VKwatch* (https://vk.watch), який містить архів інформації відповідної соціальної мережі.

Оптимальним для роботи із соціальною мережею «Instagram» є інструмент *Osintgram* (https://github.com/Datalux/Osintgram), який надає можливість проводи комплексний аналіз облікового запису Instagram будь-якого користувача за його ніком.

Які особливості пошуку та аналізу цифрових матеріалів з відкритих джерел у DarkNet та DarkWeb?

Ключовою умовою в роботі у DarkNet та DarkWeb є збереження анонімності.

Одним із найбезпечніших варіантів роботи є використання віртуальної машини, яка за своєю суттю є операційною системою на комп'ютері (хості), що функціонує повністю незалежно від основної операційної системи та є імітацією повністю відокремленого програмного забезпечення віртуального комп'ютера (по суті, віртуальна машина – це комп'ютер зі своєю операційною системою на робочому столі вашого комп'ютера).

Найпоширенішими віртуальними машинами є такі:

- *Docker* (https://www.docker.com/).
- *Hyper-V* (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/).
- *Linux KVM* (https://www.linux-kvm.org/page/Main_Page).
- *Oracle VM* VirtualBox (https://www.virtualbox.org/).
- *WMWare* (https://www.vmware.com/products/workstation-player.html).

Слід враховувати, що віртуальна машина може працювати з будь-якою операційною системою, однак **склалась практика поширеного використання віртуальних машин на операційній системі Linux, найвідомішими є такі:**

- *Caine* (https://www.caine-live.net/).
- *Debian* (https://www.debian.org/).
- *Deft* (https://distrowatch.com/table.php?distribution=deft).
- *Kali* (https://www.kali.org/) – є найпопулярнішою.
- *OpenSUSE* (https://www.opensuse.org/).
- *Paladin* (https://sumuri.com/software/paladin/).
- *Puppy* (http://puppylinux.com/).
- *Tsurugi* (https://tsurugi-linux.org/).
- *Ubuntu* (https://ubuntu.com/).

Окрім наведеного вище, для забезпечення безпеки потрібно використовувати VPN. Найпопулярнішим браузером (пошуковою системою) для роботи в DarkNet та DarkWeb є браузер Tor (https://www.torproject.org/ru/download/). Tor-браузер шифрує ваш трафік і пересилає його через декілька вузлів мережі, а потім доставляє трафік на потрібні сайти. Шлях вашого трафіка можна описати таким чином: вхідний вузол → кілька проміжних вузлів → вихідний вузол → цільовий сайт або додаток. Tor-браузер використовує мережу Tor для забезпечення конфіденційності та анонімності. Використання мережі Tor має дві основні переваги: ваш інтернет-провайдер та будь-хто, хто

може спостерігати за вашими з'єднаннями, не зможуть відстежувати вашу активність в Інтернеті, включаючи назви та адреси відвідуваних сайтів.

Як здійснювати пошук інформації в Інтернет-архівах?

В Інтернеті щотижня архівується понад мільярд сторінок. Веб-архіви використовують для різних цілей: за їх допомогою можна знайти вже неіснуючий сайт або статтю, вебсторінку, дизайн якої змінився, витягти/завантажити дані для аналізу.

Оскільки Інтернет надає доступ до найсвіжішої інформації, сайти регулярно оновлюються, постійно розвиваються та зазнають змін. Безумовно, це одна із сильних сторін Інтернету. Але це означає ще й те, що важливу інформацію також можна втратити. Вебархіви призначені саме для того, щоб зберігати контент як «докази» в ділових чи історичних цілях.

Як і в традиційних архівах, вебархіви збирають і обробляють архівісти, у цьому випадку «вебархівісти».

Оскільки Інтернет містить величезну кількість сайтів та контенту, вебархівісти зазвичай використовують автоматизовані методи збору даних. Власне, процес включає «збір» сайтів за допомогою спеціально розробленого програмного забезпечення – краулера.

Інтернет-архіви виконують ту саму функцію, що й бібліотеки, дозволяючи нам зазирнути у минуле та побачити, як усе змінилося з часом. Вебархіви зберігають інформацію, опубліковану в Інтернеті або оцифровану з друкованих видань. Більшість цієї інформації унікальна та історично цінна.

Wayback Machine (**Web.archive.org**) – це одна з найкращих архівних бібліотек, якою щодня користуються мільйони людей. Багато компаній покладаються на цей вебархів в оцінюванні конкурентів та побудові стратегії розвитку. Він дозволяє побачити історію проіндексованого сайту та те, як він був створений.

Хоча Wayback Machine є найстарішим і найбільшим загальнодоступним вебархівом, це не єдина загальнодоступна веббібліотека, яка містить дані про сайти та вебсторінки. Наведемо приклади лише деяких із них.

Архів **archive.md** доступний за адресами http://archive.today/ та http://archive.ph/.

Сервіс **Web-arhive.ru** зберігає копії сторінок сайтів. Він повністю безкоштовний[380].

[380] Веб-архіви інтернету: список існуючих ресурсів. URL: https://highload.today/uk/web-archive/

5.2.2. Процесуальні, тактичні та технічні основи збирання цифрових матеріалів з відкритих джерел у мережі «Інтернет»

Одним з основних етапів процесу розслідування з використання матеріалів з відкритих джерел є збір таких матеріалів, який відповідно до ст. 223 КПК України здійснюється шляхом проведення СРД[381], у цьому випадку через огляд цифрових матеріалів з відкритих джерел.

У Протоколі Берклі «*збір*» визначено як «акт заволодіння інформацією в Інтернеті за допомогою знімка екрана, конвертації у PDF, експертного завантаження чи іншої форми захоплення». Після того, як цифровий контент буде ідентифіковано та визнано придатним для розслідування та prima facie відповідним і надійним для своєї мети, слідчий повинен визначити належний метод збору. Методи збору можуть змінюватися залежно від того, чи має онлайн-контент потенційну доказову силу, чи його будуть використовувати для прийняття рішень, чи він буде сприяти лише внутрішньому продукту роботи. У випадках, *коли мова йде просто про робочий продукт*, може бути достатньо *скріншоту або перетворення в PDF*, тоді як вміст, який *має потенційну доказову силу*, може вимагати більш *ретельного й обґрунтованого методу збору* (наприклад, шляхом призначення значення хешу)[382].

Збирання онлайн-контенту може здійснюватися вручну за стандартною операційною процедурою або бути автоматизованим за допомогою різноманітних інструментів.

Вказівки щодо того, як і які цифрові матеріали збирати з відкритих джерел, наведено в п. 155 Розділу VI Протоколу Берклі[383]. Наразі вони слугують мінімальними стандартами для надання доказів у суді[384]. *Керуючись цими вказівками під час збирання цифрових матеріалів з відкритих джерел, слідчі повинні*:

1. **Записати вебадресу зібраного контенту**.

Така вебадреса відома як єдиний локатор ресурсів (URL) або ідентифікатор (URI).

2. **Захопити вихідний код HTML вебсторінки**, якщо це можливо.

Вихідний код HTML містить набагато більше інформації, ніж видима частина вебсайту. Вихідний код HTML сприятиме автентифікації зібраного матеріалу.

---

[381] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI URL: https: // zakon.rada.gov.ua/laws/show/4651-17#n5091 (дата звернення: 23.10.2023)

[382] Протокол Берклі … . С. 86.

[383] Протокол Берклі … . С. 87.

[384] Там само.

3. **Захопити всю сторінку, яка оглядається.**

Зробити знімок екрана цільової вебсторінки із зазначенням дати та часу. Причина цього процесу полягає в найкращому уявленні того, що було побачено під час збору.

4. **Зібрати вбудовані мультимедійні файли.**

Наприклад, якщо завантажують вебсторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з переглядуваної вебсторінки.

5. **Зібрати вбудовані метадані.**

Якщо вони є та застосовні. Метадані можуть змінюватися залежно від джерел, але загальні метадані включають ідентифікатор користувача завантажувача; ідентифікатор публікації, зображення чи відео; дату та час завантаження; геотег; хештег; коментарі та анотацію.

6. **Зібрати контекстуальні дані.**

Контекстний контент також слід збирати, якщо він має значення для розуміння цифрового елемента. Такі дані можуть включати коментарі до відео, зображення чи публікації; передбачати завантаження інформації та/або інформацію про завантажувача/користувача, таку як ім'я користувача, справжнє ім'я чи біографію. Необхідність збору навколишньої інформації слід визначити, виходячи зі специфіки випадку та цифрового матеріалу.

7. Записати всі відповідні дані (**дані збору**), які стосуються збору.

Це ім'я збирача, IP-адреса машини, яка використовується для збирання інформації, віртуальна особистість (за наявності) та мітка часу. Слідчі мають переконатися, що системний годинник точний, бажано шляхом його синхронізації із сервером мережевого протоколу часу. Причиною цього кроку є забезпечення того, щоб метадані, пов'язані з часом, були точно представлені у зібраних файлах. Якщо для доступу до зібраної інформації використовується віртуальна особистість, це слід зазначити.

8. **Додати хеш-значення.**

Хеш-значення – це унікальна форма цифрової ідентифікації, яка за допомогою криптографії підтверджує, що зібраний контент є унікальним і не змінювався з моменту збору. На момент збору слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вручну додати – або інструмент збирання – автоматично додати – значення хешу. Є безліч різних типів хешів, і стандарти з часом змінилися. Слідчі повинні оцінити, який хеш використовувати, виходячи з прийнятого на поточний момент стандарту.

Фактори, які визначені у Протоколі Берклі і які слідчий має врахувати під час прийняття рішення щодо доцільності збирання цифрових матеріалів з відкритих джерел мережі «Інтернет»

Релевантність	Чи є цифровий елемент придатним для конкретного розслідування?
Достовірність	Чи є інформація щодо цифрового контенту достовірною? Це може включати перевірку метаданих і спробу виявити першоджерела матеріалу пов'язаної інформації та джерела (*більш детально див. Главу VI E Протоколу Берклі щодо перевірки*)[385].
Видалення	Чи є ймовірність видалення цифрового елемента з Інтернету чи загального доступу? Якщо так, слід зібрати найнадійнішу відому версію.
Безпека	Чи безпечно збирати цифровий елемент, чи можна і потрібно вжити додаткових заходів безпеки?
Подальші обов'язки	Слідчі, які ведуть розслідування з використанням даних у відкритому доступі, повинні визначити, які заходи треба буде вжити, наприклад, щодо збереження цифрових матеріалів.

5.2.2.1. Збереження цифрових матеріалів з відкритих джерел у мережі «Інтернет»

У Протоколі Берклі «збереження цифрових матеріалів» передбачено як один з основних етапів процесу розслідування[386]. Постійність та доступність інформації в Інтернеті часто є нестабільними через те, що платформи соціальних медіа можуть видаляти контент зі своїх платформ відповідно до умов використання, або користувачі можуть вибирати видалення чи редагування власного завантаженого контенту. Крім того, інформацію в Інтернеті можна легко деконтекстуалізувати, втратити, стерти або пошкодити[387].

[385] Протокол Берклі … . С. 85–87.
[386] Протокол Берклі … . С. 80.
[387] Протокол Берклі … . С. 88.

Які властивості цифрового елемента потрібно захищати і зберігати з плином часу?

На думку архівістів, властивості цифрового елемента, які потрібно охороняти та зберігати з плином часу, включають його *автентичність*, *доступність*, *ідентичність*, *стійкість*, *можливість відображення та зрозумілість*, як коротко описано нижче[388].

Автентичність – це здатність продемонструвати, що цифровий елемент залишається незмінним з моменту його збирання. Цифровий елемент має залишатися незмінним під час перебування в архіві, а будь-які зміни, які були внесені до нього, мають бути задокументовані.

Доступність – це наявність цифрового елемента у простому значенні, що постійно існує та може бути відновленим, а також у юридичному сенсі забезпечення відповідних прав інтелектуальної власності на доступ та використання цього елемента.

Ідентичність належить до здатності цифрового елемента бути предметом посилання. Цифровий елемент має бути ідентифікований та відрізнятись від інших цифрових елементів.

Стійкість належить до цілісності та життєздатності цифрового елемента в технічному розумінні. Бітові послідовності цифрового елемента мають бути неушкодженими, оброблятися та вилучатися.

Можливість відображення означає здатність людини або машин використовувати цифровий елемент або взаємодіяти з ним за допомогою відповідного обладнання і програмного забезпечення.

Зрозумілість – це здатність передбачуваних користувачів інтерпретувати й розуміти цифровий елемент.

[388] Протокол Берклі … . С. 89.

Інші важливі питання, які можуть виникнути під час процесу збереження[389]	
Ланцюг забезпечення збереження	Це хронологічна документація послідовності дій зберігачів інформації чи доказів, а також документація контролю, дати та часу, передавання, аналізу та розпорядження такими доказами.
Доказова копія	Це цифровий елемент, який зібрав слідчий у його первісному вигляді і який не слід змінювати. Цифрові елементи слід зберігати в оригінальному вигляді. Це означає збереження чистого оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний.
Робочі копії	Копію або копії цифрового елемента для аналізу слід створити та зберігати окремо, щоб слідчі могли працювати із копією, а не з оригіналом. Це дозволяє мінімально обробляти оригінал і зменшувати ризик його компрометації або зміни. Будь-які зміни до елемента, включаючи виготовлення копій, мають бути задокументовані. Якщо це можливо, слід використовувати окремі системи зберігання: для доказових копій та для робочих копій.
Зберігання	Зберігання допомагає забезпечити довготривалість цифрових елементів та можливість їх пошуку й відновлення. Зберігання слід розглядати як активний процес, що включає поточні, керовані завдання та відповідальність. Варіанти зберігання цифрового контенту включають локальний жорсткий диск або локальний знімний носій інформації; або мережевий диск, який є частиною локальної мережі чи віддаленого сервера, чи системи зберігання даних у хмарі. Міркування, пов'язані з вибором сховища, включають ємність сховища (простір); доступ та контроль; резервні копії; відповідний закон; інформаційну безпеку і захист даних. Вибір сховища також має враховувати швидкість, доступність, вартість, стійкість, характеристики систем зберігання та пошуку.

Важливо! У резюме до Глави III Протоколу Берклі йдеться, що «збереження цифрового матеріалу таким чином, щоб зберегти його автентичність та документувати ланцюг забезпечення збереження, збільшить ймовірність того, що він може бути прийнятий як доказ у суді»[390].

[389] Протокол Берклі … . С. 90–91.
[390] Протокол Берклі … . С. 37.

З метою правильного збору та збереження отриманих даних і недопущення видалення інформації з мережі «Інтернет», посилаючись на Протокол Берклі[391] та наявну на сьогодні практику Верховного Суду[392], слід дотримуватися такої послідовності дій:

1. Має бути здійснене повне збереження вебсторінки за допомогою будь-якого браузера (Google Chrome, Firefox, Opera та ін.).

2. Утворюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.

3. За допомогою Інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та ін.), здійснюється архівація потрібної сторінки.

4. Уся послідовність дій під час проведення слідчої дії огляду інформації, розміщеної в Інтернеті, підлягає чіткому відображенню у протоколі огляду з графічним копіюванням вебсторінок та збереженням цифрової інформації на диску.

Цифрова копія такого документа, що буде прирівнюватися до оригіналу, має зберігатися у тому вигляді, в якому вона створювалася. Це означає збереження оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний[393].

Як зберегти вебсторінки за допомогою браузерів (Microsoft Edge, Google Chrome, Firefox, Opera)?

На час написання цього Порадника на переважній більшості комп'ютерів та ноутбуків використовується операційна система Microsoft Windows 10, в якій встановлено стандартний браузер Microsoft Edge.

У *Microsoft Edge* зробити повну копію вебсторінки можна за допомогою натискання комбінації клавіш CTRL+S або можна вибрати пункт меню «три крапки у правому верхньому куті» → «More tools» («Інші інструменти») → «Save page as» («Зберегти сторінку як»).

У *Google Chrome* зробити повну копію вебсторінки можна за допомогою натискання комбінації клавіш CTRL+S або можна вибрати пункт меню «три крапки у правому верхньому куті» → «Save and share» («Зберегти й поділитися») → «Save page as…» («Зберегти сторінку як…»).

У *Mozilla Firefox* зробити повну копію вебсторінки можна за допомогою натискання комбінації клавіш CTRL+S або можна вибрати пункт «Menu» («Меню») → «Save page as…» («Зберегти як…»).

---

[391] Протокол Берклі … .

[392] Слідчі (розшукові) дії та негласні слідчі (розшукові) дії: практика Верховного Суду. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf

[393] Там само.

В *Opera* зробити повну копію вебсторінки можна за допомогою натискання комбінації клавіш CTRL+S або можна вибрати пункт «Menu» («Меню») → «Page» («Сторінка») → «Save as…» («Зберегти як…»).

Як здійснити архівацію потрібної сторінки за допомогою Інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та інших)?

Wayback Machine[394]

Перейдіть на *https://web.archive.org/,* вкажіть URL-адресу сайту чи сторінки, яку потрібно архівувати, та натисніть «BROWSE HISTORY».

Вебархів автоматично підвантажує секцію «Calendar», де можна подивитися старі версії потрібного сайту.

Після обробки запиту ви відразу ж видно загальну інформацію про вебсторінку: кількість згенерованих архівів і шкалу часу, починаючи з першої копії й дотепер.

Виберіть рік на шкалі часу. Нижче ви побачите календар, де кольоровими маркерами позначено дати, коли вебкраулери Інтернет-архіву сканували сторінку.

Вибравши дату, наведіть курсор на неї й натисніть на час збереження. Ви побачите бажану версію вебсторінки.

Бувають ситуації, коли в Інтернет-архіві немає старих версій ресурсу: правовласник зажадав видалити свій контент або сайт закритий через порушення закону про захист інтелектуальної власності. Додатково на сайті можуть бути налаштування, які обмежують роботу вебархівів. Таким чином, боти його не сканують.

Іноді потрібний ресурс доступний, але в копії немає картинок або частини контенту. Це відбувається, якщо сайт був заархівований Wayback Machine не в повному обсязі. У такому випадку спробуйте відкрити версію сайту за інший день.

Додаткову інформацію про сайт можна знайти в секціях «Summary» і «Site Map».

У секції «Summary» зібрана статистика за типом файлів, наприклад HTML, CSS, PNG на вашому сайті.

Функціонал секції «Site Map» групує всі архіви потрібного ресурсу за роками, а потім будує візуальну карту сайту – радіальну діаграму. Центральне коло – це «корінь» сайту, його головна сторінка. Наступні кільця – інші сторінки. Наводячи курсор на кільця та осередки зверніть

[394] Hostiq блог. Що таке вебархів і як його використовувати. URL: https://hostiq.ua/blog/ukr/web-archive/

увагу, що URL-адреси вгорі змінюються. Ви можете вибрати сторінку, щоб перейти до архіву певної URL-адреси.

Щоб виявити й відобразити зміни у вмісті архівів, використовуйте секцію «Changes». Виберіть дві дати і натисніть кнопку «Compare». На новій сторінці з'являться дві версії сайту. Віддалений контент забарвлений в жовтий колір. Синій вказує на додавання вмісту.

Як зберегти поточну версію сайту у вебархіві (альтернативний варіант)?

Щоб створити копію однієї URL-адреси, знайдіть опцію «Save page now» на головній сторінці Wayback Machine, введіть посилання і натисніть «Save page» – у вебархів сайтів додасться поточна версія заданої URL-адреси.

Повторюйте цю дію перед важливими змінами на сайті та після них. У разі поломки або втрати даних ви завжди зможете відновити сайт через вебархів.

Ви можете вручну скопіювати текст і код сторінок, а також зберегти картинки.

Щоб скопіювати код сторінки, перейдіть на неї в Wayback Machine, клікніть правою кнопкою миші та виберіть «View page source». Скопіюйте код і вставте його в текстовий редактор, де ви можете зберегти його як HTML-файл.

Як здійснити архівацію вебсторінки за допомогою ресурсу «Archive.today»?

Для архівації вебсторінки за допомогою ресурсу «archive.today» виконайте такі кроки.

Відкрийте сайт: перейдіть на вебсторінку archive.today (https://archive.ph/).

Вставте URL: у полі на головній сторінці введіть URL-адресу сторінки, яку ви хочете заархівувати.

Розпочніть архівацію: натисніть кнопку «Save» або відповідну кнопку, щоб почати процес архівації.

Дочекайтеся завершення: зачекайте, поки ресурс заархівує сторінку – на це може піти деякий час, що залежить від розміру сторінки та завантаженості сервера.

Отримайте архівне посилання: після завершення архівації з'явиться посилання на збережену копію сторінки. Це посилання можна зберегти та використовувати для доступу до заархівованої версії сторінки.

Таким чином, за допомогою «archive.today» ви можете зберегти потрібну вебсторінку для майбутнього використання.

Як відбувається графічне копіювання вебсторінок та збереження цифрової інформації на диск?

Для графічного копіювання вебсторінок та збереження цифрової інформації за допомогою браузера рекомендуємо дотримуватися такого алгоритму дій:

1. Завантаження вебсторінки.

Відкрийте веббраузер.

Введіть URL-адресу вебсторінки, яку хочете скопіювати, в адресний рядок.

Натисніть Enter або кнопку «Перейти».

Зачекайте, поки вебсторінка повністю завантажиться.

2. Графічне копіювання вебсторінки.

Метод 1. Знімок екрана.

Натисніть кнопку «Print Screen» на вашій клавіатурі.

Відкрийте програму для редагування зображень, наприклад Paint або Photoshop.

Натисніть Ctrl+V, щоб вставити знімок екрана.

Обріжте знімок екрана, щоб видалити небажані частини.

Збережіть зображення у форматі PNG, JPEG або іншому форматі зображення.

Метод 2. Інструменти для створення вебсторінок.

Встановіть інструмент для створення вебсторінок, наприклад Webpage Screenshot Capture Tool або Fireshot.

Відкрийте інструмент для створення вебсторінок.

Введіть URL-адресу вебсторінки, яку хочете скопіювати.

Натисніть кнопку «Створити скріншот».

Інструмент для створення вебсторінок створить копію вебсторінки у форматі HTML, CSS та JavaScript.

Збережіть файли HTML, CSS та JavaScript на свій диск.

3. Збереження цифрової інформації.

Виберіть текст, зображення, відео або аудіо, які хочете зберегти.

Натисніть правою кнопкою миші на виділений текст.

У контекстному меню виберіть «Зберегти як».

Виберіть папку, де хочете зберегти файл.

Введіть ім’я файлу.

Виберіть формат файлу (наприклад, DOCX, PDF, MP3, MP4 або JPG).

Натисніть «Зберегти».

Які є інші способи графічного копіювання вебсторінок та збереження цифрової інформації?

1. *Розширення браузера.*

Є багато розширень браузера, які дозволяють вам робити знімки екрана вебсторінок та зберігати цифрову інформацію.

Деякі з популярних розширень:

• **Awesome Screenshot** (https://www.awesomescreenshot.com/) – це розширення дозволяє робити знімки екрана всієї вебсторінки або лише частини її. Ви можете редагувати знімки екрана перед їх збереженням.

• **FireShot** (addons.mozilla.org) – розширення схоже на Awesome Screenshot, але воно також пропонує додаткові функції, такі як можливість створювати анотовані знімки екрана та записувати відео з екрана.

• **Web Page Saver** (https://play.google.com/store/apps/details?id=com.webpagesaver.dmitriy.appwps&hl=uk) – розширення дозволяє зберігати вебсторінки у форматі HTML, CSS та JavaScript. Також можна використовувати це розширення для експорту цифрової інформації з вебсторінок у форматах PDF, TXT та CSV.

2. *Вебсайти та онлайн-сервіси.*

Є багато вебсайтів та онлайн-сервісів, які дозволяють робити знімки екрана вебсторінок та зберігати цифрову інформацію.

Деякі з популярних вебсайтів та онлайн-сервісів:

• **Lightshot** (https://app.prntscr.com/uk/download.html) – безкоштовний вебсайт, який дозволяє вам робити знімки екрана вебсторінок та редагувати їх перед їх збереженням.

• **Snagit** (https://www.techsmith.com/) – платний вебсайт, який пропонує більш розширені функції, такі як можливість створювати анотовані знімки екрана та записувати відео з екрана.

• **Clipbucket** (https://github.com/MacWarrior/clipbucket-v5) – безкоштовний онлайн-сервіс, який дозволяє вам зберігати вебсторінки у форматі HTML, CSS та JavaScript. Ви також можете використовувати цей сервіс для експорту цифрової інформації з вебсторінок у форматах PDF, TXT та CSV.

3. *Використання **вбудованих інструментів браузера***.

• **Браузер Google Chrome / Microsoft Edge.** Відкрийте вебсторінку, яку хочете зберегти. Натисніть клавіші Ctrl + Shift + I (або Cmd + Option + I на Mac), щоб відкрити панель розробника. Потім натисніть Ctrl + Shift + P (або Cmd + Shift + P на Mac) і введіть «screenshot», оберіть «Capture full size screenshot».

• **Браузер Mozilla Firefox.** Відкрийте вебсторінку, яку хочете зберегти. Натисніть клавіші Ctrl + Shift + S (або Cmd + Shift + S на Mac), щоб зняти скріншот всього екрана чи обраної частини.

4. *Збереження вебсторінок у у форматі **PDF***.

• **Браузер Google Chrome.** Відкрийте вебсторінку, яку хочете зберегти. Натисніть Ctrl + P (або Cmd + P на Mac), щоб відкрити діалогове вікно друку. У полі «Destination» виберіть «Save as PDF» і натисніть «Save».

• **Браузер Mozilla Firefox.** Відкрийте вебсторінку, натисніть Ctrl + P (або Cmd + P на Mac), виберіть «Microsoft Print to PDF» або інший PDF-принтер і натисніть «Print».

5. *Збереження вебсторінок у форматі **HTML***.

• **Браузер Google Chrome / Mozilla Firefox.** Відкрийте вебсторінку, яку хочете зберегти. Натисніть Ctrl + S (або Cmd + S на Mac), виберіть місце на диску для збереження, оберіть формат «Webpage, Complete» для збереження всієї сторінки або «Webpage, HTML Only» для збереження лише HTML-коду.

5.2.2.2. Порядок огляду та фіксації цифрових матеріалів з відкритих джерел

Враховуючи норми КПК України щодо проведення СРД-огляду комп'ютерних даних, Ⓑ Протокол Берклі, відому на 2024 рік практику Верховного суду[395], слідчу практику щодо порядку збирання та використання як доказів у кримінальному провадженні цифрових матеріалів з відкритих джерел мережі «Інтернет» та наукові напрацювання із процесуальних, тактичних і технічних основ огляду, збирання та фіксації інформації, яка міститься в оглянутих цифрових матеріалах з відкритих джерел мережі «Інтернет» А. В. Коваленка, Р. Л. Степанюка[396] та ін., *пропонуємо слідчим дотримуватися таких рекомендацій*:

1. Такий вид огляду може здійснювати слідчий (за потреби із залученням спеціаліста) у службовому кабінеті з використанням службового комп'ютера, на якому встановлено ліцензійне програмне забезпечення та організовано доступ до мережі «Інтернет» із застосування технічних засобів фіксації (якщо в цьому є необхідність).

---

[395] Слідчі (розшукові) дії та негласні слідчі (розшукові) дії: практика Верховного Суду. URL:https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf

[396] Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. С. 207. Вип. 161. С. 202–214. DOI: 10.21564/2414- 990X.161.278117; Криміналістика: криміналістична техніка: навч. посіб. / Р. Л. Степанюк та ін. Харків: ХНУВС, 2023. С. 115.

2. Перед початком огляду:

– за потреби вжити заходів безпеки роботи з цифровими матеріалами;

– у браузері мають бути відключені усі додатки та надбудови, що можуть змінити вигляд вебсторінки, яка оглядається;

– слід підключити й налаштувати всі технічні засоби, які будуть використовуватися під час огляду.

3. Через пошуковий сервіс / додаток (наприклад, «Google», «Telegram Desktop» та ін.), увівши у пошукову стрічку запит, здійснити пошук потрібної інформації.

4. Перед початком огляду вебсторінка має бути масштабована у браузері на повний розмір (100 %).

5. Огляду та опису підлягають лише ті цифрові матеріали, які мають значення для кримінального провадження.

6. Огляд знайденої вебсторінки слідчий здійснює через безпосереднє сприйняття розміщеної на ній інформації (візуального та аудіовізуального вигляду комп'ютерних даних після їх інтерпретації засобами комп'ютерної техніки).

7. Має бути здійснене повне збереження оглянутої вебсторінки за допомогою будь-якого браузера (Google Chrome, Firefox, Opera та ін.).

8. У результаті збереження вебсторінки утворюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.

9. Архівація потрібної сторінки здійснюється за допомогою Інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та ін.).

10. Треба зробити скрін кожної оглянутої сторінки, який розмістити у протоколі огляду після її опису.

11. Окрім основних комп'ютерних даних, криміналістично значущу інформацію можуть містити й метадані (від давньогр. μετά – після, за межами й англ. data – дані) – додаткова інформація, що характеризує основні дані (файл «контейнер» даних, каталог індексації даних) і зберігається разом з основними даними чи окремо від них. Перелік і зміст метаданих залежать від формату основних даних, операційної системи, типу файлу та програмного забезпечення, з яким файл асоційовано тощо[397].

В операційних системах Microsoft Windows метадані файлу можна відобразити на екрані за кліком по ньому правою кнопкою

[397] Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. С. 207. Вип. 161. С. 202–214. DOI: 10.21564/2414- 990X.161.278117

миші та вибором опції «Властивості». Основними метаданими можна вважати розмір файлу (міра кількості даних, базовою одиницею є байт), назву, розширення назви (наприклад: *.doc, *.exe), назву асоційованого програмного забезпечення, каталог розміщення, час створення, час останнього редагування, час останнього відкриття, кількість редакцій, найменування користувача, який створив чи останнім редагував файл тощо[398].

Перелічені основні метадані підлягають обов'язковому дослідженню і фіксуванню під час проведення огляду комп'ютерних даних. В окремих випадках дослідженню та фіксуванню також підлягають більш специфічні метадані, що притаманні деяким різновидам комп'ютерних файлів. Так, доказове значення можуть мати метадані, характерні для текстових файлів, зображень, аудіо- та відеофайлів, виконуваних файлів тощо[399; 400].

12. За допомогою програмних засобів, які використовуються для вивчення різних метаданих і є у відкритому доступі в мережі «Інтернет» (*див. таблицю, наведену нижче*), провести аналіз потрібних файлів.

Для вивчення більшої кількості різних метаданих використовують програмні засоби, які є у відкритому доступі в мережі «Інтернет».

Програмні засоби мережі «Інтернет»,

які використовують для вивчення метаданих

Назва програми	Стислий зміст
FotoForensics	Дозволяє переглядати метадані з фотозображень. Також дозволяє дізнатися дуже багато про фотографію, а найголовніше з його допомогою можна визначити, які ділянки на фотографії були змінені – наприклад домальовані або поверх них були додані інші фрагменти. Головна перевага сервісу – він працює як мікроскоп, допомагаючи побачити ті зміни на знімках, які не помітить людське око.
https://fotoforensics.com	

[398] Криміналістика: криміналістична техніка: навч. посіб. / Р. Л. Степанюк та ін. Харків: ХНУВС, 2023. С. 115.

[399] Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. Проблеми законності. 2023. Вип. 161. С. 202–214. DOI: 10.21564/2414-990X.161.278117

[400] Криміналістика: криміналістична техніка: навч. посіб. / Р. Л. Степанюк та ін. Харків ХНУВС, 2023. 388 с.

Назва програми	Стислий зміст
Forensically	Також дозволяє переглядати метадані з фотозображень.
https://29a.ch/photo-rensics/#forensic-magnifier	
ImageForensic	Автоматизований криміналістичний аналіз зображень, який дозволяє переглядати метадані з фотозображень.
https://www.imageforensic.org/#home	
Metadata2Go	Автоматизований аналіз файлів будь-якого фор мату – документ, фото або відео, – який дозволяє переглядати їх метадані.
https://www.metadata2go.com	
InVID-WeVerify	Розширення для браузерів Chrome та Firefox для перевірки зображень та відео. За допомогою цього розширення можна отримувати контекстну інформацію про відео з Facebook та YouTube, провести зворотний пошук зображень у пошукових системах Google, Baidu чи Яндекс, переглянути метадані, здійснити пошук за ключовими кадрами, дізнатися, хто перший завантажив відео чи зображення до мережі «Інтернет», щоб встановити його авторство.
https://www.invid-project.eu	

13. Зазначити у протоколі, за яким посиланням розміщено «Звіт аналізу метаданих».

14. Перейти за цим посиланням та зробити знімок екрана, на якому відображено звіт аналізу, й розмістити його за змістом в описову частину протоколу.

15. За допомогою програми «RapidCRC Unicode 0.3.37.0» провести хешування отриманого файлу з метою отримання хеш-коду (алгоритм sha256).

16. Зробити знімок екрана й розмістити його за змістом в описову частину протоколу/оформити додатком до протоколу.

17. Скопіювати цифрові матеріали на носій інформації, про що зазначити у протоколі огляду (*доцільно зробити декілька копій збереженої вебсторінки для того, щоб втрата чи пошкодження однієї з них не призвели до втрати матеріалу взагалі*).

18. Цифровий носій інформації, на який було скопійовано оглянуту інформацію, має бути належним чином упакований, засвідчений підписом слідчого та інших учасників слідчої (розшукової) дії та використовуватися як додаток до відповідного протоколу.

19. У разі використання технічного засобу фіксації СРД після закінчення її проведення слід відтворити запис за участю всіх учасників слідчої (розшукової) дії, про що слід зазначити у протоколі огляду.

20. Здійснити фіксування СРД-огляду цифрових матеріалів.

5.2.2.3 Відображення послідовності дій, фіксування інформації, яка міститься в оглянутих цифрових матеріалах з відкритих джерел мережі «Інтернет»

Якою має бути послідовність фіксування результатів проведеної СРД огляду цифрових матеріалів у протоколі огляду?

Фіксування результатів огляду цифрових матеріалів з відкритих джерел здійснюється у протоколі огляду відповідно до вимог ст. 104–107 КПК України, який складає слідчий або прокурор під час його проведення або безпосередньо після закінчення. Фіксуванню у протоколі огляду підлягає*:

1) інформація, передбачена нормами КПК України, якими врегульовано порядок проведення цієї СРД;

2) послідовність дій під час огляду з описом оглянутої інформації з відкритих джерел, а саме:

– дії, пов'язані з пошуком потрібної інформації з відкритих джерел мережі «Інтернет» та її виявлення;

– оглянуті цифрові матеріали (детальний опис інформації, яка розміщена на вебсторінці й має значення для кримінального провадження);

– порядок збереження вебсторінки;

– програмне забезпечення, з використанням якого здійснювався аналіз метаданих;

– за яким посиланням розміщено «Звіт аналізу метаданих»;

– за змістом розмістити знімок екрана, на якому відображено звіт аналізу метаданих;

*Особливості фіксування результатів проведення огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» сформовані з врахуванням Протоколу Берклі, існуючої на сьогодні слідчої практики та судової практики.

– назву програми, за допомогою якої було проведено хешування отриманого файлу з метою отримання хеш-коду;

– результати хешування – зробити знімок екрана й розмістити його за змістом в описову частину протоколу / оформити додатком до протоколу.

У вступній частині протоколу огляду цифрових матеріалів з відкритих джерел мережі «Інтернет» з урахуванням вимог п. 1 ч. 3 ст. 104 КПК України слід зазначити:

1. Місце, час проведення огляду.

2. Відомості про особу, яка проводить процесуальну дію (прізвище, ім'я, по батькові, посада).

3. Відомості про всіх осіб, які присутні під час проведення процесуальної дії (прізвища, імена, по батькові; дати народження; місця проживання).

4. Інформацію про те, що особи, які беруть участь у процесуальній дії, заздалегідь поінформовані про застосування технічних засобів фіксації, характеристики технічних засобів фіксації та носіїв інформації, які застосовуються під час проведення процесуальної дії, умови та порядок їх використання.

5. Відомості про залучення/незалучення спеціаліста.

6. У випадку залучення спеціаліста у протоколі треба зазначити інформацію:

а) про особу спеціаліста (прізвище, ім'я, по батькові, посада); його освіту (серія, номер диплома; спеціальність; кваліфікація); його місце проживання. У протоколі також зазначають:

– що спеціалісту роз'яснено його права та обов'язки, передбачені ст. 71 КПК України, а також що він поінформований про відповідальність, встановлену законом (ст. 72 КПК України, ст. 384 КК України (*Введення в оману суду або іншого уповноваженого органу*), 185-8 КУпАП (*Ухилення від виконання законних вимог прокурора*));

– що спеціаліста попереджено про обов'язок не розголошувати відомості досудового розслідування без письмового дозволу слідчого, прокурора, а також про кримінальну відповідальність, передбачену ст. 387 КК України (*Розголошення даних оперативно-розшукової діяльності, досудового розслідування*).

У протоколі також треба зазначити:

– в який час доби та в умовах якого освітлення (природне/штучне) проводиться огляд;

– технічні характеристики комп'ютера (серійний номер службового комп'ютера, назву та версію операційної системи, якою керується

цей комп'ютер, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі «Інтернет»);

Послідовність дій з перегляду технічних характеристик комп'ютера для Windows 11, Windows 10, Windows 7

Технічні характеристики комп'ютера можна подивитися так:

1. Для ***Windows 11***:

– натиснути кнопку **«Пуск»** → **«Налаштування»** → **«Система»** → відкрити налаштування **«Про програму»**;

– версію та випуск системи Windows зазначено в розділі **«Характеристики Windows»**.

2. Для ***Windows 10***:

– натиснути кнопку **«Пуск»** → **«Параметри»** → **«Система»** → Відкрити настройки **«Про програму»**;

– версію та випуск системи Windows зазначено в розділі **«Характеристики Windows»**.

3. Для ***Windows 7***:

– натиснути кнопку **«Пуск»**, ввести у полі пошуку слово **«комп'ютер»**, потім клацніть правою кнопкою миші пункт **«Комп'ютер»** і вибрати елемент **«Властивості»**;

– у розділі **Випуск Windows** відобразяться версія та випуск Windows.

– інформацію про флеш-диск, інші носії інформації, на які здійснюватиметься копіювання інформації, що оглядається, принтер (*серійний номер, назву та модель принтера*), колонки, інші технічні засоби, які використовувалися під час огляду;

– інтернет-ресурс, який використовується для архівації файлів (*наприклад, «archive.today», «Wayback Machine» та ін.*);

– через який браузер здійснюється огляд цифрової інформації з відкритих джерел мережі «Інтернет» (*Google Chrome, Firefox, Opera та ін.*);

– мету використання комп'ютера під час проведення огляду;

– комбінацію клавіш, за допомогою яких виготовлятимуться знімки екрана (*наприклад, залежно від браузера, який використовується, це можуть бути клавіші CTRL+S або окремі клавіші в системі Windows – PrtScr чи Print Screen*).

В описовій частині протоколу огляду цифрової інформації з відкритих джерел мережі «Інтернет» з урахуванням вимог п. 2 ч. 3 ст. 104 КПК України треба зазначити:

1) відомості про послідовність дій слідчого під час проведення огляду;

2) отримані в результаті процесуальної дії відомості, важливі для кримінального провадження.

В описовій частині протоколу треба відобразити:

1) назву пошукового сервісу / додатка, через який здійснювався пошук потрібної інформації (фото-, відеозаписів, публікацій, повідомлень тощо; наприклад, Google, Telegram Desktop), та введений у пошуковий рядок запиту;

2) результат здійсненого пошуку (назву знайденої сторінки), який є об'єктом огляду:

– у разі дослідження контенту, який створений користувачами у соціальних мережах, таких як «Facebook», «Instagram», «Telegram» та ін. чи відеохостингу «YouTube», треба зазначити назву соціальної мережі та посилання на відповідний ресурс у форматі «https://_____»;

– у разі дослідження фото, відео, інших публікацій, розміщених на вебсайті, треба вказати назву вебсайту та посилання на відповідний ресурс у форматі «https://_____»;

– категорію/жанр публікації, якщо вони зазначені на вебсторінці;

– назву публікації, відео тощо;

– системний час, який відображається в операційній системі, що встановлена на комп'ютері, з якого проводиться пошук інформації;

3) дату і час розміщення матеріалу (за наявності);

4) розміщення матеріалу, який оглядається, на сторінці сайту/додатка;

5) короткий текстовий опис публікації, фото, відео тощо, які оглядаються;

6) відомості про зображення, фото, аудіо- чи відеофайли, які прикріплені до публікації (у разі їх наявності) та їх короткий опис, із зазначенням посилання на кожний із таких файлів у мережі «Інтернет»;

7) у разі наявності відомості про автора публікації (прізвище, ім'я та по батькові/псевдонім);

8) відомості про метадані фото/відео, які оглядаються;

9) посилання на папку з архівом збереженої сторінки.

У разі наявності на вебсторінці опублікованих коментарів до публікацій, фото, відео, що оглядаються, у формі повідомлень рекомендуємо слідчим дослідити їх зміст та час розміщення з метою виявлення додаткової інформації, що стосується кримінального провадження.

Після закінчення огляду публікації, фото, відео тощо необхідно здійснити повне збереження вебсторінки, її архівацію та завантажити збережену вебсторінку на підготовлений завчасно носій інформації.

До протоколу огляду додаються оформлені належним чином додатки (носії збереженої інформації за їх наявності тощо).

У протоколі також зазначається про застосування/незастосування під час огляду фото-/відеозйомки, інших засобів фіксації.

Протокол зачитується всім учасникам та присутнім особам під час огляду, про що зазначається також у протоколі, а також про надходження/ненадходження від них зауважень щодо порядку проведення та фіксації цієї СРД.

Для прикладу наведемо порядок огляду фото-, відеоматеріалів, що містяться у відкритому доступі у мережі «Інтернет» на відеохостингу «YouTube», у застосунку «Telegram Desktop» та у пошуковому сервісі «Google»*:

1) за допомогою додатка Telegram Desktop здійснити пошук відеозапису та повідомлень у Телеграм-каналі (зазначити назву), який розміщений за посиланням https://_____;

2) здійснити опис знайденого повідомлення, зазначивши дату та час її опублікування;

3) якщо до повідомлення додано фото чи відео, про це треба зазначити у протоколі огляду, а також описати їх зміст;

4) застосовуючи клавішу PrtScr, зробити знімок екрана та вставити його в описову частину протоколу;

5) завантажити відео на комп'ютер і зазначити у протоколі огляду його назву, тип файлу та розмір;

6) натиснути правою кнопкою миші на файл з відео, розміщений у Телеграм-каналі, у результаті з'являється спливаюче вікно з посиланням «Copy Post Link»;

7) після натискання на рядок «Copy Post Link» система копіює посилання зазначеного фотофайлу (https://t.me/c...), яке використовується для архівування вебсторінки;

8) для збереження сторінки з посиланням на відеофайл потрібно здійснити її архівацію за допомогою Інтернет-ресурсу https://archive.ph,

*Порядок огляду фото-, відеоматеріалів, що містяться у відкритому доступі у мережі «Інтернет» на відеохостингу «YouTube», у застосунку «Telegram Desktop» та у пошуковому сервісі «Google» сформований на підставі існуючої на сьогодні слідчої практики та судової практики.

де у графі «Архівувати сторінку, яка зараз онлайн» ввести Інтернет-адресу https://t.me/c..., після чого буде запущено процес архівації після натискання кнопки «Зберегти»;

9) після завершення архівації при натисканні вкладки «Поділитися» на сторінці з'явиться інформація, яка містить посилання (коротке і повне) на адреси збереженої сторінки та інші відомості;

10) у протоколі треба зазначити, що «Збережена сторінка в архіві доступна за такими посиланнями: http://archive.today/...(коротке) та http://archive.today/0000.00.00...(повне);

11) слід зробити знімок екрана й розмістити його за змістом в описову частину протоколу / оформити додатком до протоколу;

12) за допомогою Інтернет-браузера «Google Chrome» (версія ___) відкрити вебсайт за адресою https://www.metadata2go.com/, куди завантажити указаний відеозапис та провести його аналіз з метою отримання всіх наявних у файлі метаданих;

13) зазначити у протоколі, за яким посиланням розміщено відеозапис: «Звіт аналізу було розміщено за посиланням https://www.metadata2go.com/result/...»;

14) перейти за цим посиланням та зробити знімок екрана, на якому відображено звіт аналізу, й розмістити його за змістом в описову частину протоколу;

15) за допомогою програми «RapidCRC Unicode 0.3.37.0» провести хешування отриманого файлу з метою отримання хеш-коду (алгоритм sha256). Зазначити у протоколі результати вказаної операції: наприклад, e26880eed41fdc32a7e552932a9fb96d09497e7c3/20866949281a7b3d8bdl 8d;

16) зробити знімок екрана й розмістити його за змістом в описову частину протоколу / оформити додатком до протоколу;

17) скопіювати відео на носій інформації (оптичний диск, флеш-диск чи ін.), про що зазначити у протоколі огляду. Для копіювання інформації рекомендуємо використовувати диски з режимом одноразового запису, такі як диски CD-R або DVD-R;

18) застосовуючи технічні засоби фіксації, потрібно: використовувати карти пам'яті, диски CD-R або DVD-R, вибір яких зумовлений використанням режиму одноразового запису на неперезаписувальному оптичному носії;

19) якщо під час огляду використовувалась відеофіксація СРД, у кінці СРД слід відтворити запис за участю всіх учасників слідчої (розшукової) дії[401];

[401] Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: монографія / [І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина]; за заг. ред. В. А. Колесника. Київ: 7БЦ, 2024. 484 с.

20) за допомогою спеціаліста виключити з програмно-технічного забезпечення засобів фіксації можливість для редагування цифрових даних, отриманих у процесі СРД[402];

21) цифровий носій інформації має бути належним чином упакований, засвідчений підписом слідчого та інших учасників слідчої (розшукової) дії й використовуватися як додаток до відповідного протоколу[403].

Як формуються додатки до протоколу огляду, їх процесуальне відображення?

Робота з відкритими джерелами інформації включає збирання, аналіз та інтерпретацію даних із загальнодоступних джерел, таких як вебсторінки, соціальні мережі, новинні сайти тощо.

У контексті вимог чинного КПК України додатки до протоколу огляду є важливим інструментом для фіксації та документування знайденої інформації.

Додатки до протоколу огляду можуть містити різні матеріали, отримані під час огляду, такі як:

– скріншоти вебсторінок, відеозаписи, аудіозаписи та інші електронні копії інформації;

– витяги з друкованих видань, фотокопії документів та інші матеріали, які неможливо долучити до протоколу в оригіналі;

– пояснення спеціалістів, які брали участь в огляді;

– стенограми, аудіо-, відеозапис процесуальної дії;

– носії скопійованої цифрової інформації з відкритих джерел;

– записи, здійснені за допомогою звуко- та відеозаписувальних технічних засобів під час проведення слідчим огляду, та інші матеріали, які пояснюють зміст протоколу тощо.

Керуючись п. 4 ч. 2 ст. 105 КПК України, до протоколу огляду доречно долучати повні копії досліджених даних на носіях.

Додатки мають важливе значення для забезпечення повноти й об'єктивності протоколу огляду. Вони допомагають слідчому, прокурору, суду та іншим учасникам кримінального провадження краще зрозуміти суть оглянутої інформації та зробити правильні висновки.

Додатки долучаються до протоколу огляду. На кожному додатку має бути зазначений його зміст. Додатки мають бути:

[402] Там само.
[403] Там само.

– належним чином виготовлені й упаковані з метою надійного збереження;

– пронумеровані;

– засвідчені підписами слідчого, прокурора, спеціаліста, інших осіб, які брали участь у виготовленні та/або вилученні таких додатків.

Які є додаткові вимоги до оформлення додатків?

Додаткові вимоги до оформлення додатків, отриманих у результаті проведення огляду цифрових матеріалів з відкритих джерел:

– докладний опис джерела інформації, включаючи URL-адресу, дату і час доступу;

– автентичність збереженої інформації, щоб уникнути звинувачень у фальсифікації даних;

– включення усіх необхідних метаданих, що підтверджують автентичність зібраної інформації;

– верифікація інформації з інших незалежних джерел для підтвердження її достовірності;

– використання логічної структури для подання інформації, включаючи розділи та підрозділи;

– забезпечення чітких пояснень і приміток, де це потрібно.

Разом з тим підкреслюємо, що додатки до протоколу огляду цифрових матеріалів з відкритих джерел мають бути розміщені в їх логічній послідовності, відповідно до дій особи, яка проводила огляд.

Загальні правила про оформлення протоколів огляду, які містяться у ст. 106 КПК України, застосовуються й до додатків до них, що треба враховувати під час їх оформлення.

Як використовуються додатки до протоколу огляду відкритих джерел у кримінальному провадженні?

Додатки до протоколу огляду відкритих джерел інформації, як і протокол, можуть бути використані у судовому розгляді як джерела доказів. Суд досліджує їх разом з іншими доказами у справі та дає їм оцінку відповідно до ст. 94 КПК України.

Якщо сторона у справі заперечує достовірність інформації, яка міститься у додатках, вона може подати клопотання про проведення додаткової перевірки. Суд може задовольнити таке клопотання й призначити експертизу.

5.3. Аналіз, перевірка та оцінка інформації, отриманої з відкритих джерел, під час розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку

За вимогами КПК України цифрові дані з відкритих джерел як доказ у кримінальному провадженні повинні оцінюватися з точки зору належності, допустимості (детально про критерії належності та допустимості йшлося у першому розділі) та достовірності й лише у сукупності та взаємозв'язку з іншими доказами і використовуватися як непрямі докази у сукупності та взаємозв'язку з іншими даними, які прямо викривають обвинуваченого у вчиненні інкримінованого йому злочину[404].

Саме таким чином, відповідно до критеріїв, установлених ст. 85, 86, 94 КПК України Велика Палата Верховного Суду дала свою оцінку тому, як суд першої інстанції оцінював «засоби доказування з точки зору належності, допустимості, достовірності» у вироку, і констатувала належність такої оцінки судом першої інстанції й відсутність допущених порушень вимог КПК, «які б відповідно до статті 438 КПК були підставами для втручання у вирок судом касаційної інстанції»[405]. Мова йде про ситуацію, коли у «…вироку, суд послався на задокументовані у відповідному протоколі результати огляду сторінок ОСОБА_25 та ОСОБА_26 у соціальних мережах, що містили фотографії цих засуджених у військовій формі зі зброєю та символікою незаконних збройних формувань (т. 2, а. к. п. 3-37), як на докази обвинувачення ОСОБА_25 та ОСОБА_26…»[406].

У Протоколі Берклі зазначено, що **допустимість** міжнародними кримінальними трибуналами, як правило (бо їхні установчі документи можуть це правило деталізувати) визначається за трифакторним критерієм, а саме:

– *релевантність* (річ (інформація) визнається такою, якщо вона допоможе зробити факт більш-менш ймовірним);

– *доказова сила* (чи допомагає річ (інформація) довести або спростувати той факт, про який ідеться у справі);

– *доказова сила, зважена проти будь-якого шкідливого впливу на справедливість судового розгляду*[407]. *Вага* належить до *сили,* приписаної

[404] Постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22). П. 123–125. URL: https://reyestr.court.gov.ua/Review/117555176

[405] Постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22). П. 125. URL: https://reyestr.court.gov.ua/Review/117555176

[406] Постанова Великої Палати Верховного Суду від 28.02.2024 у справі № 415/2182/20 (провадження № 13-15кс22). П. 125. URL: https://reyestr.court.gov.ua/Review/117555176

[407] Протокол Берклі. … . С. 47–48, п. 56.

предмету (інформації) та до *ступеня,* на який у кінцевому підсумку будуть покладатися під час прийняття юридичного чи фактичного висновку. Допустимість та вагу оцінюють окремо[408].

Для аналізу та оцінювання цифрових доказів можна використовувати такі методи:

• *Ручний аналіз.* Цей метод полягає в тому, що цифрові докази аналізує людина. Ручний аналіз може бути використаний для аналізу текстових файлів, зображень, відеозаписів та інших типів цифрових доказів.

• *Автоматизований аналіз*. Цей метод полягає в тому, що цифрові докази аналізують за допомогою спеціального програмного забезпечення. Автоматизований аналіз може бути використаний для аналізу великих обсягів даних, таких як журнали, кеші, файли cookie тощо.

• *Судова експертиза.* Цей метод полягає в тому, що цифрові докази досліджують судові експерти. Судова експертиза може бути використана для аналізу складних цифрових доказів, таких як дані з комп'ютерних систем.

Щоб визначити, чи є інформація, що міститься в цифрових матеріалах з відкритих джерел, у мережі «Інтернет», цифровим доказом, слід врахувати такі фактори:

• Чи була інформація створена, отримана, збережена або передана за допомогою комп'ютерної системи або мережі?

• Чи має інформація значення для справи?

• Чи є інформація достовірною?

• Чи є інформація допустимим доказом?

Якщо на всі ці питання можна відповісти ствердно, то інформацію, що міститься в цифрових матеріалах з відкритих джерел у мережі «Інтернет», можна вважати цифровим доказом.

Аналіз та оцінка цифрових доказів є важливою частиною кримінального розслідування. Вони можуть допомогти слідчому, прокурору та суду встановити фактичні обставини справи та/або визначити вину чи невинуватість підозрюваного.

У перебігу оцінювання отриманих з відкритих джерел цифрових даних важливо задатися питанням, а чи не є такі відомості дезінформацією. Сучасні технології дозволяють створювати deepfake (Deep Learning та Fakes, що у буквальному перекладі означає «глибинне навчання» й «підробка, дезінформація»[409]) неймовірної якості та «глибини».

---

[408] Протокол Берклі … . С. 48, п. 57.

[409] Що таке діпфейк і як його розпізнати. URL: https://ua.hive-mind.community/blog/383,shho-take-dipfeik-i-yak-iogo-rozpiznati (дата звернення: 23.05.2024).

Діпфейк – це, по суті, термін, який описує аудіо- та відеоматеріали, створені за допомогою штучного інтелекту, точніше, машинного навчання: заміна обличчя (коли обличчя однієї людини замінюється обличчям іншої); синхронізація губ (коли рот людини, яка говорить, можна налаштувати на доріжку, що відрізняється від оригіналу); клонування голосу (коли голос «копіюється», щоб змусити цей голос говорити)[410].

Така дезінформація продукується з різною метою, зокрема й задля психологічного впливу, загострення діалогу, шахрайства, фінансових афер тощо. Головне те, що через поширення фейків є ймовірність порушення приватності, що у кінцевому результаті негативно впливатиме на особисте життя і професійну сферу тих, про кого поширили такі фейки[411].

У разі поверхневої оцінки отриманих з відкритих джерел цифрових даних є висока ймовірність залучення у процес доказування таких недостовірних даних. Один із перших випадків кіберзлочину із використанням діпфейків трапився у 2021 році[412]. У національних судових розглядах вже теж маємо ситуації з таким станом справ, коли прокурору доводилося відмовлятися від підтримання обвинувачення, а, відповідно, суду – закривати кримінальне провадження[413].

Отож, як виявити діпфейк?

1. Якщо це відео, варто звернути увагу, чи кліпають очі та як саме. Раніше у підроблених відео очі не кліпали, але в останніх діпфейк-технологіях цю опцію уже почали використовувати, однак кліпання може бути нерегулярним.

2. Переглядаючи відео, слід зосередитися на якості зображення – низька якість має насторожити.

3. Потрібно провести масштабування відео і подивитися на рухи рота й губ, порівняти їх із власною поведінкою. Придивитися, як має виглядати рот під час озвучування певних звуків[414].

---

[410] Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (дата звернення: 23.05.2024).

[411] Віталій Матвєєв. ПРОБЛЕМИ ТА ВИКЛИКИ, ПОВ'ЯЗАНІ ЗІ ЗБОРОМ ЕЛЕКТРОННИХ ДОКАЗІВ. 27 лип. 2023. URL: HTTPS://JUSTTALK.COM.UA/POST/PROBLEMI-TA-VIKLIKI-POVYAZANI-ZI-ZBOROM-ELEKTRONNIH-DOKAZIV

[412] Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (дата звернення: 23.05.2024).

[413] Кейс: Суд закрив кримінальне провадження у відношенні трансжінки, яка обвинувачилась у розповсюдженні порнографічних зображень. 17.05.2023. URL: https://www.projector.org.ua/projects_ua/public_hrc_ua/cases_hrc_ua/case_marii-vinichenko_sud/

[414] Віталій Матвєєв. ПРОБЛЕМИ ТА ВИКЛИКИ, ПОВ'ЯЗАНІ ЗІ ЗБОРОМ ЕЛЕКТРОННИХ ДОКАЗІВ. 27 липня, 2023. URL: HTTPS://JUSTTALK.COM.UA/POST/PROBLEMI-TA-VIKLIKI-POVYAZANI-ZI-ZBOROM-ELEKTRONNIH-DOKAZIV

4. Знайти іншу версію досліджуваного відео та порівняти їх. Якщо відео опубліковане якимось фейсбук-акаунтом, створеним два дні тому, про яке немає згадки в жодних медіа, а оригінал цього відео був створений ще 5 років тому і воно сильно відрізняється – то одразу зрозуміло, що навряд чи це правдиве відео[415].

5. Оглянувши детально відео можна виявити таке:

1) обличчя не завжди пропорційно «накладається» на тіло, краї «маски» не всюди рівні;

2) біля очей та брів можуть пролягати дивні тіні;

3) неприродний відтінок кольору шкіри;

4) окуляри чи інші великі аксесуари можуть мати відблиски, котрі не гармоніюють із загальною картинкою;

5) незвичний/неприродній вигляд волосся (розмитість, неправильна лінія росту);

6) невідповідні міміка та рухи (зокрема рух очей!)[416].

Також потрібно звернути увагу на дивні «стрибки» у відео: зміна голосового тону, неякісний звук, розмиті плями, незвичні форми кінцівок, форми вух, носа, зубів, колір і тон ділянок шкіри, нерівності в ділянках шиї, дивне освітлення, інші надзвичайні невідповідності.

Для роботи з діпфейками у пригоді можуть стати такі інструменти:

• *watchframebyframe.com* – інструмент для перевірки відео. Можна розглянути відео пофреймово і показати відмінність між двома фреймами, у випадку, якщо там були внесені зміни[417];

• *digger-project.com* – проєкт від німецької агенції, яка займається виявленням діпфейків. Тут тренуються навички побачити те, що потрібно. Система вас буде тренувати, доки не навчить дивитися саме туди, куди потрібно. Найважливіше на цьому ресурсі – він дозволяє тренувати слух задля виявлення фейкового та справжнього голосу[418];

• *detectfakes.media.mit.edu* – інструмент, створений Массачусетським інститутом технологій, спрямований на тренування навички розпізнавання діпфейків. Цей ресурс тренує журналістську інтуїцію.

---

[415] Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (дата звернення: 23.05.2024).

[416] Там само. … (дата звернення: 23.05.2024).

[417] Що таке діпфейк і як його розпізнати. URL: https://ua.hive-mind.community/blog/383,shho-take-dipfeik-i-yak-iogo-rozpiznati (дата звернення: 23.05.2024).

[418] Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (дата звернення: 23.05.2024).

Треба прислухатися до тону голосу людей, до пауз між фразами, придивитися до міміки[419].

• *http://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter* – один із небагатьох робочих автоматичних інструментів, які дозволяють виявляти діпфейки[420].

У 2020 році компанія Microsoft оголосила про вихід у світ технології Microsoft Video Authenticator, яка аналізує зображення та відео і визначає їх справжність[421].

Призначення певного різновиду експертизи також сприятиме встановленню наявності діпфейків.

У підсумку органам розслідування та прокурору «важливо мати можливість продемонструвати, що немає підстав сумніватися в автентичності матеріалів із відкритих джерел, наприклад через те, що вони були сфабриковані або якимось чином змінені з метою створення очевидно обвинувачувальних доказів»[422].

І насамкінець, оцінка достовірності отриманих з відкритих джерел цифрових даних є надважливим завданням через ймовірні маніпуляції та внесення змін, від чого страждає їхня надійність. На ці процеси прямий вплив матиме й використання «…невідповідних інструментів (програм з неправильною специфікацією, з помилками в коді тощо) для доступу та збереження…»[423]. Перевірка достовірності здійснюється специфічними способами, як от «перевірка контрольної суми (хеш-суми)»[424]. Для більш розлогого осягнення цієї проблематики радимо скористатися науковим виданням із попереднього посилання.

---

[419] Там само. … . (дата звернення: 23.05.2024).

[420] Там само. … . (дата звернення: 23.05.2024).

[421] Там само. … . (дата звернення: 23.05.2024).

[422] Що таке діпфейк і як його розпізнати. URL: https://ua.hive-mind.community/blog/383,shho-take-dipfeik-i-yak-iogo-rozpiznati (дата звернення: 23.05.2024).

[423] Макбрайд Д. Застосовні міжнародно-правові рамки та стандарти щодо доказів із відкритих та електронних джерел: Європейська конвенція з прав людини. Council of Europe : веб-сайт. URL: https://rm.coe.int/coe-ukraine-open-uk/1680a6e571

[424] OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса : Видавництво «Юридика», 2024. С.114–115.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аврамова О. Є. Віртуальна (цифрова) особистість: суб'єктивний та об'єктивний аспект. *Зб. наук. пр. НДІ ПЗІР НАПрН України. Вип. : Інноваційний процес: виклики воєнного часу, проблеми, перспективи євроінтеграції* : за матеріалами Кругл. столу (м. Харків, 02 груд. 2022 р.) / за ред. С. В. Глібка, І. В. Подрез-Ряполової. Харків, 2022. С. 52–56.
2. Авторське право. Довідковий центр. *Facebook* : [сайт]. URL: https://www.facebook.com/help/instagram/126382350847838
3. Актуальні питання використання методів і засобів osint у роботі підрозділів захисту національної державності : зб. матеріалів кругл. столу (м. Київ, 31 берез. 2023 р.) : у 2 ч. Київ : НА СБУ, 2023. Ч. 1. 75 с. URL: https://academy.ssu.gov.ua/uploads/p_57_61186644.pdf
4. Актуальні рекомендації відносно веб-браузерів та інших заходів операційної безпеки розміщенні на платформі Ресурсного центра комп'ютерної безпеки Національного інституту стандартів і технологій США. *NIST Computer Security Resource Center* : [сайт]. URL: https://csrc.nist.gov
5. Атаманов О. М. Повідомлення про підозру особі, місцезнаходження якої не встановлено або яка перебуває за межами України : дис. … д-ра філос. : 081 – Право. Київ, 2021. 309 с.
6. Бабін Б. В. Категорія геноциду та поточна правова система України. *Війна в Україні: зроблені висновки та незасвоєні уроки* : зб. тез Міжнар. наук.-практ. конф. (22–23 лют. 2024 р.) / [упор. У. О. Цмоць] ; ЛьвДУВС. Львів, 2024. С. 66–70. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html
7. База даних. URL: https://uk.wikipedia.org/wiki/База_даних
8. База даних записів із даними росіян (проєкт від OSINT FLOW). *Osint Flow* : [сайт]. URL: https://search.osintflow.com/search
9. База російських військових, які чинили злочини в Україні. Пошук російських злочинців. *Книга катів українського народу* : [сайт]. URL: https://russian-torturers.com/
10. Бази даних доказів воєнних злочинів рф (проєкт міжнародної розвідувальної спільноти Inform Napalm). *Inform Napalm* : [сайт]. URL: https://informnapalm.org/ua/bazy-danyh/
11. Басиста І. В. Викрадення українських дітей, як різновид геноцидної політики росії. *Військові кримінальні правопорушення та особливості їх розслідування* : матеріали кругл. столу, проведеного в межах Днів науки на ф-ті правн. наук Нац. Ун-ту «Києво-Могилянська академія» (26 січ. 2024 р.) / НаУКМА. Київ, 2024. С. 6–22.
12. Басиста І. В. Зняття інформації з електронних інформаційних систем. *Велика українська юридична енциклопедія* : у 20 т. Харків, 2020. Т. 19. Кримінальний процес, судоустрій, прокуратура та адвокатура / [редкол. В. Т. Нор (голова) та ін.] ; Нац. акад. прав. наук України ; Ін-т держави і права ім. В. М. Корецького НАН України ; Нац. юрид. ун-т ім. Ярослава Мудрого. С. 348–350.

13. Басиста І. В. Насильницька передача українських дітей – акт геноциду чи воєнний злочин? *Українська воєнна та повоєнна кримінальна юстиція* : матеріали IX (XXII) Львівськ. форуму кримінальн. юстиції (м. Львів, 26–27 жовт. 2023 р.) / [упор. І. Б. Газдайка-Василишин] ; ЛьвДУВС. Львів, 2023. С. 18–64. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html

14. Басиста І. В. Притягнення до кримінальної відповідальності за геноцид за чинним КК України: окремі проблеми. *Процесуальне та криміналістичне забезпечення досудового розслідування* : тези доп. учасників наук.-практ. семінару (01 груд. 2023 р.) / [упор. А. Я. Хитра] ; ЛьвДУВС. Львів, 2023. С. 10–17. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html

15. Басиста І. В., Удовенко Ж. В., Кулинич М.-М. А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Наук. Вісн. Ужгород. нац. ун-ту.* Серія : Право. 2024. Вип. 80. Ч. 3. С. 19–38. URL: https://visnyk-jurisuzhnu.com/wp-content/uploads/2024/03/81_part-3.pdf

16. Берклійський протокол про розслідування цифрових відкритих джерел: практичний посібник з ефективного використання цифрових відкритих джерел та інформації під час розслідування порушень міжнародного кримінального права, прав людини та гуманітарного права. *ООН* : [сайт]. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

17. Бінарний перекладач – конвертер тексту у двійковий код. *Character Calculator* : [сайт]. URL: https://charactercalculator.com/uk/binary-translator/

18. Вибір заради справедливості : посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини : у 2 т. / [пер. О. Бондаренко] ; заг. ред. Р. Мартиновський, Л. Мороз ; видання здійснене за підтримки Програми «Права людини і правосуддя» Міжнародного фонду «Відродження». Київ : Відродження, 2018. Т. 2. 276 с. URL: https://www.irf.ua/wp-content/uploads/2020/06/tom_ii_web.pdf

19. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. [2-ге вид., допов.]. Київ : Нац. акад. внутр. справ, 2020. 104 с.

20. Вирок Київського районного суду м. Харкова від 14 серп. 2023 р. у справі № 953/2635/23. Провадження № 1-кп/953/807/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/112892204

21. Вирок Київського районного суду м. Харкова від 15 верес. 2022 р. у справі № 953/4064/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/106252541

22. Вирок колегії суддів Київського районного суду м. Харкова від 02 берез. 2023 р. у справі № 953/1240/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/109609026

23. Вирок Хмельницького міськрайонного суду Хмельницької області у справі № 686/3769/23. Провадження № 1-кп/686/745/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/113906215

24. Владимир Соловьев. *Telegram* : [сайт]. URL: https://t.me/s/SolovievLive

25. Воєнні злочинці рф. *ГУР МО України* : [сайт]. URL: https://gur.gov.ua/content/war-criminals-rf.html

26. Герои спецоперации Z. *Telegram* : [сайт]. URL: https://t.me/s/heroesofZ

27. Геронтьєва О. Проблеми з безпекою через зброю в країні не бачу, загрози громадянам немає – керівник Головного слідчого управління Нацполіції. 31 січ. 2024 р. *ІА «Інтерфакс-Україна»* : [сайт]. URL: https://interfax.com.ua/news/interview/963982.html

28. Глаз Бога. *Telegram* : веб-сайт. URL: https://telegram.im/@eyegodsbot?lang=ru

29. Гловюк І. В. Вироки за ст. 438 КК України: порушення законів та звичаїв війни (з 24 лют. 2022 р.). *Вищ. шк. адвокатури* : [сайт]. URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/porusennia-zakoniv-ta-zvicayiv-viini-st-438-kk-mezi-ta-pidstavi-kriminalizaciyi

30. Гловюк І. В. Порушення законів та звичаїв війни: про особливості кваліфікації злочину. *Вищ. шк. адвокатури* : [сайт]. URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/porusennia-zakoniv-ta-zvicayiv-viini-pro-osoblivosti-kvalifikaciyi-zlocinu-rozpovila-advokat-irina-gloviuk

31. Гловюк І., Стоянов М. Особливості доказування у спеціальному досудовому розслідуванні: окремі питання. *Право України.* 2017. № 12. С. 19–26.

32. Горох – українські словники : Онлайн-бібліотека : [сайт]. URL: https://goroh.pp.ua/%D0%A2%D0%BB%D1%83%D0%BC%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F/%D0%BD%D0%B5%D0%B7%D0%BC%D1%96%D0%BD%D0%BD%D0%B8%D0%B9

33. ГУР МО України. *Telegram* : [сайт]. URL: https://t.me/s/DIUkraine

34. Гутник А. В. Забезпечення права на захист персональних даних підозрюваного у кримінальному провадженні: проблеми та шляхи їх розв'язання. *Бізнес і права людини в Україні: проблеми та рішення під час війни й повоєнного відновлення* : зб. матеріалів III Всеукр. конкурсу наук. робіт / за заг. ред. В. А. Устименка ; [ред.-упоряд. А. Є. Санченко]. Київ, 2024. С. 174–182.

35. Гутник А. В. Повідомлення про підозру у вчиненні ідеологічного та культурно-освітнього колабораціонізму: аналіз дотримання вимог ст. 277 КПК. *Military offences and war crimes: background, theory and practice*: collective monograph / ed. by V. M. Stratonov. Riga, Latvia : Baltija Publishing, 2023. С. 250–273.

36. Гутник А. В. Порушення Закону України «Про захист персональних даних» на веб-сайті Офісу Генерального прокурора.

Наукова весна. 2023 : матеріали XIII Міжнар. наук.-техн. конф. студ., аспірантів та мол. вчених (м. Дніпро, 1–3 берез. 2023 р.). Дніпро, 2023. С. 351–352.

37. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : кол. моногр. Львів : ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4725

38. Гутник А., Коць Є. Проблемні аспекти вручення процесуальних документів особі, яка перебуває на тимчасово окупованій території або на території держави-агресора. *Наук. вісн. Дніпропетров. держ. ун-ту внутр. справ.* 2023. № 2. С. 271–279. DOI: 10.31733/2078-3566-2023-2-271-279

39. Деґе Ш. Чи може штучний інтелект конкурувати з митцями? 6 лют. 2023 р. *Deutsche Welle* : [сайт]. URL: https://www.dw.com/uk/ci-mozestucnij-intelekt-konkuruvati-z-mitcami/a-64602090

40. Державний реєстр санкцій : [сайт]. URL: https://drs.nsdc.gov.ua/

41. Добросовісне використання на YouTube. *Youtube довідка* : [сайт]. URL: https://support.google.com/youtube/answer/9783148?hl=uk

42. Додаткові параметри пошуку. URL: https://support.microsoft.com/uk-ua/topic/додаткові-параметри-пошукуb92e25f1-0085-4271-bdf9-14aaea720930

43. Дроздов О. Кримінальне провадження за відсутності підозрюваного, обвинуваченого (in absentia) : підручник. Гл. 8. *Особливі порядки кримінального провадження* / [О. В. Капліна, О. І. Марочкін, М. І. Демура та ін.] ; за ред. О. В. Капліної ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2024. С. 172–206.

44. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). [Чинний 2016-10-10]. Київ : УкрНДНЦ, 2018. 31 с. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=67144

45. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні : монографія / [І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина] ; за заг. ред. В. А. Колесника. Київ : 7БЦ, 2024. 484 с.

46. Європейська конвенція про захист прав людини і основоположних свобод : підписана 04 листоп. 1950 р. *Верховна Рада України* : [сайт]. URL: http://zakon4.rada.gov.ua/laws/show/995_004

47. Жидков В. Л., Жила О. Б. Застосування спеціальної процедури притягнення до кримінальної відповідальності (in absentia) за колабораційну діяльність / USAID ; Українська Гельсінська спілка з прав людини. Київ : Укр. Гельсінська спілка з прав людини, 2023. 17 с. URL: https://www.helsinki.org.ua/wp-content/uploads/2023/06/Zastosuvannia-spetsialnoi-protsedury-prytiahnennia-do-kryminalnoi-vidpovidalnosti-in-absentia-za-kolaboratsiynu-diialnist.pdf

48. Задоя К. Перше кримінальне провадження в США щодо воєнних злочинів, вчинених в Україні. 01 лют. 2024 р. *Глобальна ініціатива T4P (Трибунал для Путіна)* : [сайт]. URL: https://t4pua.org/2281

49. Збір інформації з відкритих джерел як майбутній засіб доказів у найважчих міжнародних злочинах. 07 груд. 2023 р. *Antiraid* : [сайт]. URL: https://antiraid.com.ua/news/zbir-informatsii-z-vidkrytykh-dzherel-iak-majbutnij-zasib-dokaziv-u-najvazhchykh-mizhnarodnykh-zlochynakh/

50. Інтернет архів = Internet Archive : [сайт]. URL: https://archive.org/about/

51. Калька І. З. Реалізація прав підозрюваного, обвинуваченого в спеціальному кримінальному провадженні (in absentia) : дис. … д-ра філос. : 081 – Право. Київ, 2023. 265 с.

52. Капалкіна І. Провадження in absentia. Недоліки, сприйняття суспільством та очікування потерпілих. 08 черв. 2023 р. *JustTalk* : [сайт]. URL: https://justtalk.com.ua/post/provadzhennya-in-absentia-nedoliki-sprijnyattya-suspilstvom-ta-ochikuvannya-poterpilih

53. Кваліфікація та розслідування порушення законів і звичаїв війни : наук.-практ. посіб. / [А. А. Вознюк, І. В. Жук, О. В. Таран, С. С. Чернявський та ін.] ; за заг. ред. М. С. Цуцкіридзе, В. В. Чернея, А. А. Вознюка. Київ : Норма права, 2023. 320 с.

54. Кейс: Суд закрив кримінальне провадження у відношенні трансжінки, яка обвинувачилась у розповсюдженні порнографічних зображень. 17 трав. 2023. *Громадська організація Прожектор* : [сайт]. URL: https://www.projector.org.ua/projects_ua/public_hrc_ua/cases_hrc_ua/case_marii-vinichenko_sud/

55. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посіб. [електрон. вид.] / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. О. Денькович, д-ра права, проф. Г. Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

56. Кішка, що прославилася в інтернеті завдяки своєму знаменитому похмурому вигляду, отримала 710 тисяч доларів США у справі про захист авторських прав у федеральному суді штату Каліфорнія. 25 січ. 2018 р. *BBC Україна* : [сайт]. URL: https://www.bbc.com/ukrainian/other-news-42815049

57. Кобилянський О. Л., Кофанов А. В. Фотографічна фіксація перебігу та результатів слідчих (розшукових) дій : метод. рек. Київ : УкрДГРІ, 2012. 64 с. (Сер. «Запобігання, протидія, розслідування злочинів»).

58. Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності.* 2023. Вип. 161. С. 202–214. DOI: 10.21564/2414- 990X.161.278117.

59. Коваленко А. В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки* : зб. тез Міжнар. наук.-

практ. конф. (22–23 лют. 2024 р.) / [упор. У. О. Цмоць] ; ЛьвДУВС. Львів, 2024. С. 413–417. URL: https://www.lvduvs.edu.ua/uk/library/materialy-naukovykh-konferentsii.html

60. Коваленко А. В. Огляд комп'ютерних даних: сутність і процесуальний порядок проведення. *Вісн. Харків. нац. ун-ту внутр. справ.* 2023. № 3 (102). Ч. 2. С. 187–197. URL: https://doi.org/10.32631/v.2023.3.41

61. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналістів. *Вісн. Нац. акад. правов. наук України* : зб. наук. пр. 2017. № 1 (88). С. 182–191.

62. Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Наук. вісн. Херсон. держ. ун-ту.* Вип. 4. 2023. С. 54. URL: https://doi.org/10.32999/ksu2307-8049/2023-4-9

63. Коваленко А. В. Особливості проведення огляду веб-ресурсів як різновиду огляду комп'ютерних даних. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали V Міжнар. наук.-практ. конф. (м. Київ, 21 груд. 2023 р.) / КНДІСЕ. Київ, 2023. С. 199–202.

64. Комп'ютерна допомога. Методи збереження веб сторінки в опері. URL: http://pro-computer.pp.ua/8766-metodi-zberezhennya-veb-stornki-v-oper-kompyuterna-dopomoga.html

65. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

66. Коперсак Д. В. Спеціальне досудове розслідування кримінальних правопорушень : дис. … д-ра філос. : 081 – Право. Одеса, 2021. 247 с.

67. Корякін Р. О., Яковенко М. О. Актуальні проблеми спеціального досудового розслідування кримінальних правопорушень. *Вісн. Луганськ. держ. ун-ту внутр. справ ім. Е. О. Дідоренка.* 2016. № 2. С. 111–118.

68. Коць Є. П. Проблемні аспекти залучення та участі захисника під час спеціального досудового розслідування (in absentia). *Аналітично-порівняльне правознавство.* 2023. № 2. С. 342–346. DOI: https://doi.org/10.24144/2788-6018.2023.02.59

69. Краєвська Т. Українські правоохоронці представили в Гаазі результати розслідування воєнних злочинів. 11 берез. 2024 р. *ІА «УНН»* : [сайт]. URL: https://unn.ua/news/ukrainski-pravookhorontsi-predstavyly-v-haazi-rezultaty-rozsliduvannia-voiennykh-zlochyniv

70. Криміналістика : криміналістична техніка : навч. посіб. / [Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін.] ; МВС України ; Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. 388 с.

71. Кримінальний кодекс України : затв. Законом України від 05 квіт. 2001 р. № 4651-VI ; ред. від 01 січ. 2024 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2341-14?f

72. Кримінальний процес України. Академічний курс. У 3 т. Т. 1. Загальна частина / [В. Т. Нор, Н. Р. Бобечко, М. В. Багрій та ін.] ; за ред.

акад. НАПрН України, д-ра юрид. наук, проф. В. Т. Нора та д-ра юрид. наук, проф. Н. Р. Бобечка. Львів : ЛНУ ім. Івана Франка, 2021. 912 с.

73. Кримінальний процесуальний кодекс України : затв. Законом України № 4651-VI від 13 квіт. 2012 р. *Верховна Рада України* : [сайт]. URL: http://zakon3.rada.gov.ua/laws/show/4651-17

74. Кримчук С. Г. Окремі аспекти здійснення повідомлення про підозру у спеціальному досудовому розслідуванні. *Юрид. бюлетень.* 2019. Вип. 11. Ч. 2. С. 270–276. URL: http://www.lawbulletin.oduvs.od.ua/archive/2019/11/part_2/37.pdf

75. МакБрайд Д. Застосовні міжнародно-правові рамки та стандарти щодо доказів із відкритих та електронних джерел: Європейська конвенція з прав людини. *Council of Europe* : [сайт]. URL: https://rm.coe.int/coe-ukraine-open-uk/1680a6e571

76. Мамченко Н. Цитування чи плагіат: Верховний Суд розглянув справу авторки автореферату дисертації, який без її дозволу розмістив університет. *Судово-юрид. газета.* 2024. 11 берез. URL: https://sud.ua/uk/news/publication/295198-tsitirovanie-ili-plagiat-verkhovnyy-sud-rassmotrel-delo-avtora-avtoreferata-dissertatsii-kotoryy-bez-ee-razresheniya-razmestil-universitet?fbclid=IwAR29XWWUrQFRC7Flx6IfwVaTrUQue_t1PjeJJyHQf8WBZD06ipIJCAc0X7E

77. Маргарита Симоньян. *Telegram* : [сайт]. URL: https://t.me/s/margaritasimonyan

78. Мария Львова-Белова. *Telegram* : [сайт]. URL: https://t.me/s/malvovabelova

79. Матвєєв В. Проблеми та виклики, пов'язані зі збором електронних доказів. 27 лип., 2023. *Justtalk* : [сайт]. URL: https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zborom-elektronnih-dokaziv

80. Міністерство внутрішніх справ України : [сайт]. URL: https://mvs.gov.ua/

81. Навчально-методичні рекомендації щодо пошуку оперативно значущої інформації в мережі Інтернет / К. Ю. Ісмайлов, В. С. Жогов, Л. В. Лефтеров. Одеса : ОДУВС, 2019. 28 с.

82. Огляд судової практики Касаційного кримінального суду щодо здійснення спеціальної процедури кримінального провадження (досудового розслідування та судового розгляду) за відсутності обвинуваченого (in absentia). Рішення, внесені до ЄДРСР з 2018 року по серпень 2022 року / [упоряд. : заст. голови Касаційного кримінального суду у складі Верховного Суду, канд. юрид. наук В. В. Щепоткіна] ; Правове управління (III) департаменту аналітичної та правової роботи апарату Верховного Суду. Київ, 2022. 23 с. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1344119/

83. Онлайн-курс «Інтернет і цифрові права людини. Створений за підтримки Американської асоціації юристів, Ініціативи з верховенства права (ABA ROLI в Україні) в рамках програми «Сприяння Інтернет свободі в Україні». *Платформа дистанційного навчання системи безоплатної*

правничої допомоги : [сайт]. URL: https://academy.legalaid.gov.ua/course/view.php?id=166

84. Опендатабот : [сайт]. URL: https://opendatabot.ua/

85. ОПРИЧНИКИ : [сайт]. URL: https://www.oprichniki.org/

86. Особи, які переховуються від органів влади. Сервіси. *Міністерство внутрішніх справ України* : [сайт]. URL: https://wanted.mvs.gov.ua/searchperson/

87. Офіс Генерального прокурора : [сайт]. URL: https://www.gp.gov.ua/

88. Офіс Президента : [сайт]. URL: https://www.president.gov.ua/

89. Пам'ятка для випускників закладів вищої освіти МВС України з документування злочинів, пов'язаних із збройною агресією рф проти України : практ. посіб. / [кол. авт.-уклад. : В. М. Василенко, А. І. Кисько, О. М. Музичук, В. В. Романюк та ін. ; упоряд. : С. Є. Абламський] ; за заг. ред. В. В. Сокуренка ; МВС України ; Харків. нац. ун-т внутр. справ. [2-ге вид., допов. і переробл.]. Харків : ХНУВС, 2024. 56 с.

90. ПВК Вагнер. *Telegram* : [сайт]. URL: https://t.me/s/wagnernew

91. Пентестер: професія етичного хакера. 21 лют. 2022. *10guards* : [сайт]. URL: https://10guards.com/ua/articles/pentester-the-profession-of-ethical-hacker/

92. Петрів О., Спесивцева О. Автори проти штучного інтелекту: на чийому боці суд? 15 груд. 2023 р. *ЦЕДЕМ* : [сайт]. URL: https://cedem.org.ua/news/avtory-proty-shi-na-chyjomu-botsi-cud/

93. Платформа прав людини : [сайт]. URL: https://ppl.org.ua/

94. Повідомлення про підозру Кусік Маргариті Вікторівні, пам'ятка про процесуальні права та обов'язки підозрюваного та повістки про виклик підозрюваної Кусік М. В. на 25.10.2023, 26.10.2023, 27.10.2023. *Офіс Генерального прокурора* : [сайт]. URL: https://www.gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-kusik-mv-pamyatka-pro-procesualni-prava-ta-obovyazki-pidozryuvanoyi-kusik-mv-ta-povistki-pro-viklik-na-25102023-26102023-27102023

95. Повідомлення про підозру Мусієнку Д. М. та повістки про виклик на 01.11.2023, 02.11.2023, 03.11.2023. *Офіс Генерального прокурора* : [сайт]. URL: https://www.gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-musijenku-dm-ta-povistki-pro-viklik-na-01112023-02112023-03112023

96. Повідомлення про підозру та повістки про виклик Хитун Л. В. на 01.11.2023, 02.11.2023, 03.11.2023. *Офіс Генерального прокурора* : [сайт]. URL: https://www.gp.gov.ua/ua/posts/povidomlennya-pro-pidozru-xitun-lv

97. Полторак В. П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спец. 126 «Інформаційні системи та технології» / КПІ ім. Ігоря Сікорського. Електрон. текстові дані (1 файл: 1,73 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

98. Поняття, структура та різновиди веб-сайтів. Автоматизоване розроблення веб-сайтів. *Ніжин. держ. ун-т ім. Миколи Гоголя* : [сайт]. URL: http://www.ndu.edu.ua/liceum/web.pdf

99. Постанова Великої Палати Верховного Суду від 28 лют. 2024 р. у справі № 415/2182/20. Провадження № 13-15кс22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/117373993

100. Постанова Верховного Суду від 01 квіт. 2021 р. у справі № 759/2992/17. Провадження № 51-3360км20. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/95946565

101. Постанова Верховного Суду від 04 листоп. 2021 р. у справі № 326/1385/18. Провадження № 51-2018км21. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/101100299

102. Постанова Верховного Суду від 10 верес. 2020 р. у справі № 751/6069/19. Провадження № 51-1704км20. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/91722819

103. Постанова Верховного Суду від 13 черв. 2019 р. у справі № 607/9498/16-к. Провадження № 51-2422км18. *Єдиний державний реєстр судових рішень* : [сайт]. URL: http://reyestr.court.gov.ua/Review/82492181

104. Постанова Верховного Суду від 15 січ. 2020 р. у справі № 161/5306/16-к. Провадження № 51-3498км19. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/87053591

105. Постанова Верховного Суду від 19 лип. 2022 р. у справі № 727/13085/18. Провадження № 51-10250км18. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/105359481

106. Постанова Верховного Суду від 22 жовт. 2020 р. у справі № 677/2040/16-к. Провадження № 51-5738км19. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/92458395

107. Постанова Верховного суду від 26 січ. 2021 р. у справі № 236/4268/18. Провадження № 51-3124км20. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/94905297

108. Постанова Верховного Суду від 31 жовт. 2019 р. у справі № 404/700/17. Провадження № 51-4451км19. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/85390646

109. Постанова Другої судової палати Касаційного цивільного суду Верховного Суду від 17 січ. 2024 р. у справі № 308/7570/18-ц. Провадження № 61-7051св23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/117473137

110. Постанова Касаційного кримінального суду у складі Верховного Суду від 07 груд. 2022 р. у справі № 385/619/16. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/107834205

111. Постанова колегії суддів Другої судової палати Касаційного кримінального суду Верховного Суду від 30 квіт. 2020 р. у справі

№ 640/19897/16-к. Провадження № 51-6241км19. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/89034985

112. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 берез. 2021 р. у справі № 554/5090/16-к. Провадження № 51-1878кмо20. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/96074938

113. Постанова Третьої судової палати Касаційного кримінального суду Верховного Суду від 28 лют. 2024 р. у справі № 753/14148/21. Провадження № 51-6134 км 23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/117442733

114. Потерь.НЕТ : [сайт]. URL: https://poternet.site/ua

115. Пошукова система. URL: https://uk.wikipedia.org/wiki/Пошукова_система

116. Правила й вказівки. *YouTube* : [сайт]. URL: https://www.youtube.com/intl/uk_ALL/creators/how-things-work/policies-guidelines/

117. Правова охорона авторських і суміжних прав, прав інтелектуальної власності в Україні. *ЮК «УНІЛАВ»* : [сайт]. URL: https://unilaw.com.ua/pravova-ohorona-avtorskyh-i-sumizhnyh-prav/

118. Пріхно А. «Немає жодного сенсу в сотнях вироків без належних доказів», – суддя про воєнні злочини РФ. 14 листоп. 2022 р. *Судова влада України* : [сайт]. URL: https://court.gov.ua/press/publications/1345639/

119. Про авторське право і суміжні права : Закон України від 01 груд. 2022 р. № 2811-20 ; редакція від 15 квіт. 2023 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

120. Про електронні документи та електронний документообіг : Закон України № 851-IV від 22 трав. 2003 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

121. Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав : постанова Пленуму Верховного Суду України № 5 від 04 черв. 2010. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/v0005700-10#Text

122. Про затвердження Інструкції про порядок здійснення міжнародного співробітництва з питань взаємної правової допомоги, видачі правопорушників (екстрадиції), передачі (прийняття) засуджених осіб, виконання вироків та інших питань міжнародного судового співробітництва у кримінальному провадженні під час судового провадження : наказ Міністерства юстиції України № 2599/5 від 19 серп. 2019 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0956-19#Text

123. Про затвердження Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження та на офіційному веб-сайті Офісу Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового

розслідування : наказ Офісу Генерального прокурора № 141 від 30 трав. 2023 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/v0141905-23#Text

124. Про затвердження роз'яснення щодо втручання органів БПД до правової позиції адвоката при розгляді клопотання про обрання запобіжного заходу : рішення Ради адвокатів України № 70 від 08 серп. 2022 р. *Національна асоціація адвокатів України* : [сайт]. URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2022-08-02-r-shennya-rau-70_62fcfd46cb86e.pdf

125. Про затвердження роз'яснення щодо участі адвокатів у кримінальних провадженнях за відсутності підозрюваного, обвинуваченого : рішення Ради адвокатів України № 183 від 27 груд. 2022 р. *Національна асоціація адвокатів України* : [сайт]. URL: https://unba.org.ua/assets/uploads/legislation/rishennya/2022-12-27-r-shennya-rau-183_63d129b90a174.pdf

126. Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел : лист-орієнтування Офісу Генерального прокурора № 18/1-386 вих–515окв–21 від 28 серп. 2021 р.

127. Про утворення Координаційного штабу з питань поводження з військовополоненими : постанова Кабінету Міністрів України № 257. Абз. 3. П. 9 від 11 берез. 2022 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/257-2022-%D0%BF#Text

128. Проєкт «Кто воюет в Украине» : [сайт]. URL: https://war-proekt.media/base/voiska/

129. Просування відповідальності за міжнародні злочини в Африці : рек. зустрічі 24 експертів у жовт. 2013 р. для обговорення / Всеафриканський союз адвокатів ; Міжнародне кримінальне правосуддя в Африці. *Аналітична записка.* 2013. № 5. 17 лип. С. 1–2.

130. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних : практ. посіб. щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнар. кримін. права, з прав людини та гуманітарного права / [неофіц. пер. з англ. О. В. Зюзь]. Нью-Йорк і Женева : Центр з прав людини Каліфорн. ун-ту ; Берклі : Юрид. шк. ; ООН Упр. Верхов. комісара з прав людини, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

131. Рамзан Кадиров. *Telegram* : [сайт]. URL: https://t.me/s/RKadyrov_95/4699

132. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філос. : 081 – Право. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

133. Реєстр російських військових злочинців : спільний проєкт Антикорупційного штабу та «Слідство.Інфо» : [сайт]. URL: https://rwc.shtab.net/troopers

134. Реєстр російських окупантів, які воювали на Миколаївщині : проєкт центру журналістських розслідувань. *Nikcenter* : [сайт]. URL: https://invaders.nikcenter.org/

135. Реєстри «Вороги України» : проєкт від OSINT-спільноти MOLFAR. *Molfar* : [сайт]. URL: https://molfar.com/enemies

136. Резолюція № (75) 11 Комітету Міністрів Ради Європи «Про критерії, які регламентують розгляд, що проводиться за відсутності обвинуваченого» : прийнята 19 січ. 1973 р. *Council of Europe* : [сайт]. URL: https://rm.coe.int/09000016804f7581

137. Римський Статут Міжнародного Кримінального суду : прийнятий від 17 лип. 1998 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text

138. Рік розслідування воєнних злочинів. Інтерв'ю з Юрієм Бєлоусовим, начальником Департаменту війни ОГП. 02 берез. 2023 р. *Justtalk* : [сайт]. URL: https://justtalk.com.ua/post/rik-rozsliduvannya-voennih-zlochiniv-intervyu-z-yuriem-belousovim-nachalnikom-departamentu-vijni-ogp-tekstova-versiya

139. Розслідування воєнних злочинів в Україні: правозахисники анонімно опитали правоохоронців і зібрали дані. 21 верес. 2023 р. *Радіо Свобода* : [сайт]. URL: https://www.radiosvoboda.org/a/doslidzhennia-rozsliduvannia-voiennyh-zlochyniv-v-ukraini/32602285.html

140. Савчук Т. Dark Web: прихована сторона інтернету, яка поширена в Україні. 07 жовт. 2017 р. *Радіо Свобода* : [сайт]. URL: https://www.radiosvoboda.org/a/28778448.html

141. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

142. СБУ. *Telegram* : [сайт]. URL: https://t.me/SBUkr

143. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с.

144. Слідство. Інфо : [сайт]. URL: https://www.slidstvo.info/

145. Слідчі (розшукові) дії та негласні слідчі (розшукові) дії: практика Верховного Суду. URL : https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_Slidchi_dii.pdf

146. СОЛДАТСКАЯ ПРАВДА КРП(б). *Telegram* : [сайт]. URL: https://t.me/Soldiers_truth

147. Соціальна мережа. URL: http://igroup.com.ua/seo-articles/sotsialna-merezha/

148. Справа «Айлей та інші проти Росії» (Ayley and Others v. Russia) (Заяви № 25714/16, № 56328/18) : рішення Європейського суду з прав людини від 03 квіт. 2019 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-192578

149. Справа «Акденіз проти Туреччини» (Akdeniz v. Turkey) (Заява № 20877/10) : рішення Європейського суду з прав людини від 11 берез. 2014 р. URL: https://hudoc.echr.coe.int/eng?i=001-142383

150. Справа «Ахмет Їлдірім проти Туреччини» (Ahmet Yıldırım v. Turkey) (Заява № 3111/10) : рішення Європейського суду з прав людини від 18 груд. 2012 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng-press?i=003-4202780-4985142

151. Справа «Белькасем проти Бельгії» (Belkacem v Belgium) (Заява № 34367/14) : рішення Європейського суду з прав людини від 27 черв. 2017 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-175941

152. Справа «Булгаков проти Росії» (Bulgakov v. Russia) (Заява № 20159/15) : рішення Європейського суду з прав людини від 23 черв. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-203181

153. Справа «Ведува проти Румунії» (Văduva v. Romania) (Заява № 27781/06) : рішення Європейського суду з прав людини від 25 лют. 2014 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-141172&filename=001-141172.pdf

154. Справа «Вікімедія проти Туреччини» (Wikimedia Foundation, Inc. v. Turkey) (Заява № 25479/19) : рішення Європейського суду з прав людини від 01 берез. 2022 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-216677

155. Справа «Вільямсон проти Німеччини» (Williamson against Germany) (Заява № 64496/17) : рішення Європейського суду з прав людини від 31 січ. 2019 р. *Практика Європейського суду з прав людини. Український аспект* : [сайт]. URL: https://www.echr.com.ua/translation/sprava-vilyamson-proti-nimechchini-pres-reliz/

156. Справа «Владімір Харітонов проти Росії» (Vladimir Kharitonov v. Russia) (Заява № 10795/14) : рішення Європейського суду з прав людини від 23 черв. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-203177

157. Справа «Горватіч проти Хорватії» (Horvatić v. Croatia) (Заява № 36044/09) : рішення Європейського суду з прав людини від 17 жовт. 2013 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-126915

158. Справа «Егіль Ейнарссон проти Ісландії» (Egill Einarsson v. Iceland) (Заява № 24703/15) : рішення Європейського суду з прав людини від 07 листоп. 2017 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-178362

159. Справа «Енгельс проти Росії» (Engels v. Russia) (Заява № 61919/16) : рішення Європейського суду з прав людини від 23 черв. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-203180

160. Справа «Калда проти Естонії» (Kalda v. Estonia) (Заява № 17429/10) : рішення Європейського суду з прав людини від 19 груд. 2016 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-160270

161. Справа «Колоцца проти Італії» (Colozza v. Italy) (Заява № 9024/80) : рішення Європейського суду з прав людини від 12 лют. 1985 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-57462&filename=CASE%20OF%20COLOZZA%20v.%20ITALY.docx&logEvent=False

162. Справа «Кудер та Ашет Філіпачі Асосьє проти Франції» (Couderc and Hachette Filipacchi Associés v. France) (Заява № 40454/07) : рішення Європейського суду з прав людини від 10 листоп. 2015 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-158861

163. Справа «Ліліенталь проти Ісландії» (Lilliendahl vs Iceland) (Заява № 29297/18) : рішення Європейського суду з прав людини від 12 трав. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/fre?i=001-203199

164. Справа «Лопес Рібальда та інші проти Іспанії» (López Ribalda and Others v. Spain) (Заява № 1874/13) : рішення Європейського суду з прав людини від 17 жовт. 2019 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/fre?i=001-197098

165. Справа «Монір Лотфі проти Кіпру» (Monir Lotfy v. Cyprus) (Заява № 37139/13) : рішення Європейського суду з прав людини від 29 черв. 2021 р. E*uropean Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-210680

166. Справа «Нікс проти Німеччини» (Nix v. Germany) (Заява № 35285/16) : рішення Європейського суду з прав людини від 13 берез. 2018 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-182241

167. Справа «ООО Флавус та інші проти Росії» (ООО Flavus and Others v. Russia) (Заява № 12468/15) : рішення Європейського суду з прав людини від 23 черв. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-203178

168. Справа «Пасторс проти Німеччини» (Pastörs v. Germany) (Заява № 55225/14) : рішення Європейського суду з прав людини від 03 жовт. 2019 р. *Практика Європейського суду з прав людини. Український аспект* : [сайт]. URL: https://www.echr.com.ua/translation/sprava-pastors-proti-nimechchini/

169. Справа «Перінчек проти Швейцарії» (Perinçek v. Switzerland) (Заява № 27510/08) : рішення Європейського суду з прав людини від 15 жовт. 2015 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-158235

170. Справа «Прокурор проти Ахмада Аль-Факі Аль-Махді (Prosecutor v. Ahmad Al Faqi Al Mahdi) (Заява ICC-01/12-01/15) : рішення Міжнародного кримінального суду від 27 верес. 2016 р. *International Criminal*

Court : [сайт]. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2016_07244.PDF

171. Справа «Прокурор проти Махмуда Мустафи Бусайф аль-Верфаллі» (Prosecutor v. Mahmoud al-Werfalli) (Заява ICC-01/11-01/17) : рішення Міжнародного кримінального суду від 4 лип. 2018 р. *International Criminal Court* : [сайт]. URL: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2018_03552.PDF

172. Справа «Прокурор проти Младича» (Prosecutor v. Mladic) (Заява IT-09-92-T) : рішення Міжнародного кримінального суду від 22 листоп. 2017 р. *International Criminal Tribunal for the former Yugoslavia* : [сайт]. URL: https://www.icty.org/x/cases/mladic/tjug/en/171122-3of5_1.pdf

173. Справа «Прокурор проти Толіміра» (Prosecutor v. Tolimir) (Заява IT-05-88/2-T) : рішення Міжнародного кримінального суду від 12 груд. 2012 р. *International Criminal Tribunal for the former Yugoslavia* : [сайт]. URL: https://www.icty.org/x/cases/tolimir/tjug/en/121212.pdf

174. Справа «Рамазан Демір проти Туреччини» (Ramazan Demir v. Turkey) (Заява № 68550/17) : рішення Європейського суду з прав людини від 09 лют. 2021 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-207804

175. Справа «Родіна проти Латвії» (Rodina v. Latvia) (Заяви № 48534/10 та 19532/15) : рішення Європейського суду з прав людини від 14 трав. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-202437

176. Справа «С. Г. проти Сполученого Королівства» (S. H. v. United Kingdom). (Заява № 19956/06) : рішення Європейського суду з прав людини від 15 черв. 2010 р. *Refworld* : [сайт]. URL: https://www.refworld.org/jurisprudence/caselaw/echr/2010/en/73048

177. Справа «Сакіт Західов проти Азербайджану» (Sakit Zahidov v. Azerbaijan) (Заява № 51164/07) : рішення Європейського суду з прав людини від 12 листоп. 2015 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-158490

178. Справа «Санадер проти Хорватії» (Sanader v. Croatia) (Заява № 66408/12) : рішення Європейського суду з прав людини від 12 лют. 2015 р. Information Note on the Court's case-law 182. February 2015. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/fre?i=002-10371

179. Справа «Санчез проти Франції» (Sanchez v. France) (Заява № 45581/15) : рішення Європейського суду з прав людини від 02 верес. 2021 р. *Council of Europe* : [сайт]. URL: https://rm.coe.int/affaire-sanchez-c-france-uk-/1680a4df76

180. Справа «Седлецька проти України» (Sedletska v. Ukraine) (Заява № 42634/18) : рішення Європейського суду з прав людини від 1 квіт. 2021 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-208882

181. Справа «Сейдовіч проти Італії» (Sejdovic v. Italy). (Заява № 56581/00) : рішення Європейського суду з прав людини від 01 берез. 2006 р. *Інформаційний бюлетень з практики суду.* Березень, 2006. № 84. URL: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-179185&filename=CASE%20OF%20SEJDOVIC%20v.%20ITALY%20-%20%5BUkrainian%20Translation%5D%20legal%20summary%20by%20the%20CoE%20Project%20%22Continued%20support%20to%20the%20criminal%20justice%20reform%20in%20Ukraine%22.pdf&logEvent=False

182. Справа «Смажич проти Боснії та Герцеговини» (Smajic v. Bosnia and Herzegovina) (Заява № 48657/16) : рішення Європейського суду з прав людини від 16 груд. 2018 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-180956

183. Справа «Стомахін проти Росії» (Stomakhin v. Russia) (Заява № 52273/07) : рішення Європейського суду з прав людини від 09 трав. 2020 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-182731

184. Справа «Таганрог ЛРО проти Росії 2» (Taganrog LRO and Others v. Russia2) (Заява № 32401/10) : рішення Європейського суду з прав людини від 07 черв. 2022 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-217535

185. Справа «Фон Ганновер проти Німеччини 2» (Von Hannover v. Germany 2) (Заяви № 40660/08 та 60641/08) : рішення Європейського суду з прав людини від 07 лют. 2012 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-109029

186. Справа «Ченгіз проти Туреччини» (Cengiz and Others v. Turkey) (Заяви № 48226/10 та 14027/11) : рішення Європейського суду з прав людини від 01 груд. 2015 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng-press?i=003-5241080-6502267

187. Справа «Шачашвілі проти Німеччини» (Schatschaschwili v. Germany) (Заява № 9154/10) : рішення Європейського суду з прав людини від 15 груд. 2015 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/fre?i=001-159566

188. Справа «Шенк проти Швейцарії» (Schenk v. Switzerland) (Заява № 10862/840) : рішення Європейського суду з прав людини від 12 лип. 1988 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=001-76800

189. Справа «Янковскіс проти Литви» (Jankovskis v. Lithuania) (Заява № 21575/08) : рішення Європейського суду з прав людини від 17 груд. 2017 р. *European Court of Human Rights* : [сайт]. URL: https://hudoc.echr.coe.int/eng?i=002-11349

190. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : дис. … д-ра юрид. наук : 12.00.09. Дніпро, 2018. 648 с.

191. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : автореф. дис. … д-ра юрид. наук : 12.00.09.

Дніпро, 2018. 42 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/auto/20/3.pdf

192. Столітній А. В. Електронне кримінальне провадження: передумови виникнення, сучасний стан та перспективи розвитку : монографія. Київ : АртЕк, 2016. 724 с.

193. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. 07 черв. 2022 р. *Верховний суд* : [сайт]. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

194. Судді ВС розповіли про останні тенденції у сфері кримінального права України. 28 груд. 2023 р. *БОРГ.ЕКСПЕРТ* : [сайт]. URL: https://borgexpert.com/news/suddi-vs-rozpovily-pro-ostanni-tendentsii-u-sferi-kryminalnoho-prava-ukrainy

195. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28 жовт. 2021 р. *Верховний суд* : [сайт]. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

196. Судова практика ККС Верховного Суду щодо допустимості електронних доказів : презентація / підгот. суддею Верховного Суду Н. Стефанів. В*ерховний суд* : [сайт]. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf

197. Схеми. *Радіо Свобода* : [сайт]. URL: https://www.radiosvoboda.org/skhemy

198. Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридич. часопис Нац. академії внутр. справ.* 2019. № 2 (18). С. 24–32.

199. Тимофеєв А. О. Проблеми практичної реалізації процедури спеціального досудового розслідування (in absentia) в Україні. *Наук. записки НаУКМА.* Серія : Юридичні науки. 2021. Т. 8. С. 60–68. URL: http://nrplaw.ukma.edu.ua/article/view/254047

200. 34 країни в Гаазі підписали Конвенцію про співпрацю в розслідуванні міжнародних злочинів. 14 лют. 2024 р. *Європейська Правда* : [сайт]. URL: https://www.eurointegration.com.ua/news/2024/02/14/7179625/

201. Тлумачний словник з інформатики / [Г. Г. Півняк, Б. С. Бусигін, М. М. Дівізінюк та ін.]. Дніпропетровськ : Нац. гірнич. ун-т, 2010. 600 с.

202. Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. 19 лип. 2022 р. *Софтліст* : [сайт]. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/

203. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024.

204. У МВС ідентифікували понад 232 тисячі військових злочинців та зрадників. 03 серп. 2023 р. *Урядовий портал* : [сайт]. URL: https://www.

kmu.gov.ua/news/u-mvs-identyfikuvaly-ponad-232-tysiachi-viiskovykh-zlochyntsiv-ta-zradnykiv

205. Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. *Штучний інтелект у правовій практиці: межі та можливості* : матеріали Всеукр. кругл. столу, (15 берез. 2024 р.) / ЛьвДУВС. Львів : ЛьвДУВС, 2024.

206. Узагальнення судової практики щодо розгляду слідчим суддею клопотань про застосування заходів забезпечення кримінального провадження, проведене Вищим спеціалізованим судом України з розгляду цивільних і кримінальних справ від 07 лют. 2014 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/n0001740-14#Text

207. Україна підпише Любляно-Гаазьку конвенцію про співпрацю в розслідуванні міжнародних злочинів. Українська Правда. 08 січ. 2024 р. *Європейська Правда* : [сайт]. URL: https://www.eurointegration.com.ua/news/2024/01/8/7177007/

208. Україна розширила інструменти захисту авторських прав в інтернет-просторі. 30 берез. 2024 р. *Я і Закон* : [сайт]. URL: https://yaizakon.com.ua/ukrayina-rozshirila-instrumenti-zahistu-avtorskih-prav-v-internet-prostori/

209. Ухвала Апеляційного суду Житомирської області від 09 груд. 2016 р. у справі № 295/15419/16-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/63335901

210. Ухвала Вільнянського районного суду Запорізької області від 08 квіт. 2024 р. у справі № 314/1565/24. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/118189336

211. Ухвала Галицького районного суду м. Львова від 12 груд. 2023 р. у справі № 461/10189/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/115578469

212. Ухвала Дарницького районного суду м. Києва від 08 листоп. 2023 р. у справі № 753/12538/16-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/114779246

213. Ухвала Дніпровського апеляційного суду від 29 черв. 2023 р. у справі № 932/3698/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/111950943

214. Ухвала Комунарського районного суду м. Запоріжжя від 03 квіт. 2023 р. у справі № 333/2408/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/109981556

215. Ухвала Корольовського районного суду м. Житомира від 31 берез. 2023 р. у справі № 296/2927/23. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/110121449

216. Ухвала Красногвардійського районного суду м. Дніпропетровська від 31 жовт. 2022 р. у справі № 204/8858/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/107362235

217. Ухвала Красногвардійського районного суду м. Дніпропетровська від 20 жовт. 2022 у справі № 204/8197/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/107223204#

218. Ухвала Ленінського районного суду м. Кіровограда від 21 січ. 2022 р. у справі № 405/8268/21. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/102696510

219. Ухвала Личаківського районного суду м. Львова від 10 листоп. 2022 р. у справі № 463/1712/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/107356174

220. Ухвала Новомосковського міськрайонного суду Дніпропетровської області від 05 груд. 2022 р. у справі №183/6587/22. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/107959506

221. Ухвала Орджонікідзевського районного суду м. Запоріжжя від 16 верес. 2022 р. у справі № 335/1262/19. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/106354358

222. Ухвала Печерського районного суду м. Києва від 13 січ. 2022 р. у справі № 757/63763/21-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/104512262

223. Ухвала слідчого судді Печерського районного суду м. Києва від 08 жовт. 2020 р. у справі № 757/42166/20-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/92178885

224. Ухвала Слов'янського міськрайонного суду Донецької області від 15 черв. 2020 р. у справі № 243/3303/20. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/89806902

225. Ухвала Шепетівського міськрайонного суду від 28 квіт. 2022 р. у справі № 688/3180/21. *Єдиний державний реєстр судових рішень* : [сайт]. URL: https://reyestr.court.gov.ua/Review/104146087

226. Федоренко І. Л. Міжнародний розшук, процедура in absentia в українському законодавстві. Презентація. 9 с. *Асоціація правників України* : [сайт]. URL: https://uba.ua/documents/events/2020/Kate/UBA%20Knowledge%20Hub/%D0%A4%D0%B5%D0%B4%D0%BE%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%86%D0%B3%D0%BE%D1%80.pdf

227. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісн. ХНУВС–Bulletin of KhNUIA.* 2023. № 3 (102). С. 209–210. DOI: https://doi.org/10.32631/v.2023.3.43

228. Фундація DEJURE : [сайт]. URL: https://dejure.foundation/

229. ЦГП «Альменда» : [сайт]. URL: https://almenda.org/

230. Центр «Миротворець» : [сайт]. URL: https://myrotvorets.center/

231. Цивільний процесуальний кодекс України : Закон України № 1618-IV від 18 берез. 2004 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

232. Цифрова колекція. Викрадена історія. *Херсонський обласний краєзнавчий музей* : [сайт]. URL: https://hokm.ks.ua/category/czyfrova-kolekcziya/vykradena-istoriya/

233. Штучний інтелект. *Словник з інформатики* : [сайт]. URL: http://xn--r1a3b.xn--b1amgblet.xn--j1amh/index.php/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82

234. Шутяк С. Перспективи справ «in absentia» для кримінальних правопорушень проти довкілля. 13 груд. 2023 р. *Національна асоціація адвокатів України* : [сайт]. URL: https://unba.org.ua/publications/8597-perspektivi-sprav-in-absentia-dlya-kriminal-nih-pravoporushen-proti-dovkillya.html

235. Що таке авторське право? *Youtube Довідка* : [сайт]. URL: https://support.google.com/youtube/answer/2797466?hl=uk

236. Що таке веб-скрейпінг і як він пов'язаний з проксі. 05 квіт. 2022 р. *Astro* : [сайт]. URL: https://astroproxy.com/ua/terms-of-use

237. Що таке діпфейк і як його розпізнати. URL: https://ua.hive-mind.community/blog/383,shho-take-dipfeik-i-yak-iogo-rozpiznati (дата звернення: 23.05.2024).

238. Як надіслати запит на видалення відео через порушення авторських прав. Youtube Довідка : [сайт]. URL: https://support.google.com/youtube/answer/2807622?hl=uk

239. Як розпізнати діпфейк: конспект вебінару Михайла Кольцова. URL: https://www.jta.com.ua/knowledge-base/instrumenty-dlia-perevirky-dipfeykiv-konspekt-vebinaru-mykhayla-koltsova (дата звернення: 23.05.2024).

240. Seeking Justice or Shielding Suspects? An analysis of the Malabo Protocol on the African Court. 23.11.2016. *Kenyans for Peace with Truth and Justice* (KPTJ) : [website]. URL: http://kptj.africog.org/seeking-justice-or-shielding-suspects-an-analysis-of-the-malabo-protocol-on-theafrican-court

241. Access to Internet and freedom to receive and impart information and ideas. Factsheet. September 2022. *European Court of Human Rights* : [website]. URL: https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf

242. Berkeley Protocol on Digital Open Source Investigations / A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York and Geneva : OHCHR ; Human Rights Center, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

243. Bihus.Info : [website]. URL: https://bihus.info/

244. Bing Maps : [website]. URL: https://www.bing.com/maps

245. Bing. Retrieved from https://uk.wikipedia.org/wiki/Bing

246. Chauhan S., Panda N. K. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Elsevier Science & Technology Books, 2015. 306 p.

247. Chris Hoofnagle. Dark Web Intelligence: Methods & Legal Issues. BCLT Research2Practice. July 16, 2020. Presentation. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/darknet_intel.pdf

248. Clarity Project : [website]. URL: https://clarity-project.info/
249. Covert Shores: H I Sutton. URL: http://www.hisutton.com/
250. CyberSec's Bot. *Telegram* : [website]. URL: https://t.me/cybersecs
251. DataLeakBot. *Telegram* : [website]. URL: https://telegram.im/@safe_search_bot
252. DuckDuckGo. URL: https://uk.wikipedia.org/wiki/DuckDuckGo
253. Facebook. Інструкція для початківців. URL: http://ipress.ua/ljlive/facebook_instruktsiya_dlya_pochatkivtsiv_2326.html
254. Gill R. What is Open-Source Intelligence? 23.02.2023. URL: https://www.sans.org/blog/what-is-open-source-intelligence/
255. Global Investigative Journalism Network : [website]. URL: https://gijn.org/ua/
256. Google Chrome Довідка. Як переглядати сторінки пізніше й без підключення до Інтернету. URL: https://support.google.com/chrome/answer/7343019?hl=uk&co=GENIE.Platform%3DAndroid&oco=1
257. Google Earth Pro : [website]. URL: https://www.google.com/intl/ru/earth/about/
258. Google Maps : [сайт]. URL: https://www.google.com.ua/maps/
259. Hostiq блог. Що таке веб-архів і як його використовувати. URL: https://hostiq.ua/blog/ukr/web-archive/
260. ILIA (International Law in Advocacy) is a collaborative platform, developed organically by Human Rights House Foundation and Houses over the course of over a decade. URL: https://ilia.humanrightshouse.org/course/view.php?id=430
261. ICC Prosecutor Karim A. A. Khan KC announces launch of advanced evidence submission platform : OTPLink. *International Criminal Court* : [website]. URL: https://www.icc-cpi.int/ news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submissionplatform-otplink
262. Intelligence Community Directive Number 301. NATIONAL OPEN SOURCE ENTERPRISE. EFFECTIVE : JULY 11, 2006. 8 p. URL: https://irp.fas.org/dni/icd/icd-301.pdf
263. Intellectual Property Policy. Last updated: June 7, 2021. *Tiktok* : [website]. URL: https://www.tiktok.com/legal/page/global/copyright-policy/en
264. IOM. Україна : [website]. URL: https://ukraine.iom.int/uk
265. Jeremy McBride. Судова палата Монктону у Великій Британії. URL: https://www.monckton.com/barrister/jeremy-mcbride/
266. Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources. Cybersecurity Unit. Computer Crime & Intellectual Property Section. Criminal Division U.S. Department of Justice. February 2020. 15 p. URL: https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl
267. LiveUAMap : [website]. URL: https://liveuamap.com/uk
268. Ljubljana-The Hague Convention on International Cooperation in the Investigation and Prosecution of the Crime of Genocide, Crimes against Humanity, War Crimes, and other International Crimes. 26.05.2023. URL:

https://www.gov.si/assets/ministrstva/MZEZ/projekti/MLA-pobuda/The-Ljubljana-TheHague-MLA-Convention-English-v5.pdf

269. Max du Plessis Implications of the AU Decision to Give the African Court Jurisdiction Over International Crimes. черв. 2012. № 235. *Institute for Security Studies* : [website]. URL: https://issafrica.s3.amazonaws.com/site/uploads/Paper235-AfricaCourt.pdf

270. Mozilla Support. Збереження веб-сторінки. URL: https://support.mozilla.org/uk/kb/%D0%97%D0%B1%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%B2%D0%B5%D0%B1-%D1%81%D1%82%D0%BE%D1%80%D1%96%D0%BD%D0%BA%D0%B8

271. NASA Earthdata Search. URL: https://search.earthdata.nasa.gov/search

272. Open-source intelligence. 02.05.2022. *European Union* : [website]. URL: https://data.europa.eu/en/publications/datastories/open-source-intelligence

273. OSINT FLOW bot. *Telegram* : [website]. URL: https://t.me/osintflow_find_bot

274. OSINT: Навчання, Інструкція та Відео для Професіоналів Кібербезпеки : [сайт]. URL: https://hackyourmom.com/osvita/navchannya-instrukcziyi-posibnyky-ta-video-po-osint/

275. Red Cross Society : [website]. URL: https://redcross.org.ua/

276. Review for “Optimal location and operation of battery energy storage system in the distribution system for reducing energy cost in 24-hour period”. 21 лют. 2021. DOI:10.1002/2050-7038.12861/v3/review1

277. Serhii Ablamskyi, Volodymyr Galagan, Iryna Basysta, Zhanna Udovenko Detention of a person suspected of committing a criminal offense during martial law in Ukraine (Detenção de uma pessoa suspeita de cometer um crime durante a lei marcial na Ucrânia). *Revista Brasileira de Políticas Públicas.* 2023. V. 13, № 3. P. 452–467. URL: https://www.rel.uniceub.br/RBPP/article/view/9129/pdfDOI: https://doi.org/10.5102/rbpp.v13i3.9129

278. Virtual machine (VM). 21 May 2020. *Techopedia* : [website]. URL: www.techopedia.com/definition/4805/virtual-machine-vm

279. The Internet Archive Wayback Machine : [website]. URL: https://help.archive.org/

280. Ukraine War Archive. : [website]. URL: https://ukrainewararchive.org/

281. UNICEF : [website]. URL: https://www.unicef.org/ukraine/

282. USGS Earth Explorer. URL: https://earthexplorer.usgs.gov/

283. Wikimapia : [website]. URL: https://wikimapia.org/

284. YouControl : [website]. URL: https://youcontrol.com.ua/

ГЛОСАРІЙ

Dark Web	«Тіньовий Інтернет», та частина Інтернету, яка доступна лише за допомогою спеціального програмного забезпечення, що дозволяє користувачам та операторам вебсайтів залишатися анонімними і не підлягати відстеженню [3, с. 110]
Deep Web	Частина Інтернету, яка не проіндексована стандартними пошуковими системами [4]
OSINT	Збирання та використання інформації з відкритих джерел для конкретних цілей допомоги у розробленні політики та прийнятті рішень, найчастіше у військовому чи політичному контексті [1, с. 25]
OTPLink	Платформа для подання доказів онлайн та електронною поштою всіма зовнішніми зацікавленими сторонами та свідками до офісу прокурора МКС [2]
Surface Web	«Поверхневий Інтернет», та частина Інтернету, до якої можна отримати доступ за допомогою будь-якого браузера і здійснювати пошук за допомогою традиційних пошукових систем [3, с. 110]
Автор	Фізична особа, яка своєю творчою діяльністю створила твір [5]
Автентичність	Здатність продемонструвати, що цифровий елемент залишається незмінним з моменту його збирання [3, с. 89]
Бінарний код	Мова, яка використовується в комп'ютерах. Він заснований на двійковій системі числення, яка використовує лише 0 та 1 як символи для подання тексту [6]

Вебсайт	Сукупність даних, електронної (цифрової) інформації, зокрема об'єктів авторського права та/або суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси вебсайту та/або облікового запису власника такого вебсайту, доступ до яких здійснюється через адресу в мережі «Інтернет», що може складатися з доменного імені, записів про каталоги або виклики та/або числової адреси за Інтернет-протоколом [5]
Вебсторінка	Складова частина вебсайту, розміщена за спеціальною адресою в мережі «Інтернет» [5]
Верифікація (перевірка)	Встановлення відповідності прийнятій інформації щодо переданої за допомогою логічних методів [7, с. 279]
Вікдриті джерела цифрової інформації	Медіа, соціальні медіа, вебсайти, геопросторові платформи, бази даних, офіційні дані та інші платформи, на яких можна спостерігати, купувати або запитувати загальнодоступну інформацію
Відкрите програмне забезпечення	Побудоване з вихідного коду, який кожний, хто має доступ, може перевірити, змінити чи покращити. Код не бачать користувачі, але він підпадає під вказані маніпуляції програмістом. На відкрите програмне забезпечення не поширюються авторські права, патенти чи інші юридичні засоби контролю [3, с. 25]
Відтворюваність	Властивість процесу отримувати однакові тестові результати в різному тестовому середовищі (різні комп'ютери, жорсткий диск, режим роботи тощо) [8, с. 217–218]

Віртуальна особистість (цифрова особистість)	Об'єктивна форма особистості у цифровому середовищі. Вона може бути представлена фізичною, юридичною особою, а також бути індивідуальною чи колективною. Для неї властиві виникнення, виконання певних функцій та припинення існування. Залежно від цифрової платформи віртуальна особистість створюється у результаті здійснення певного комплексу дій, а ось припинення її дії може бути і не передбачене умовами відповідного цифрового середовища [9, с. 53]
Геолокація	Ідентифікація або оцінка розміщення об'єкта, діяльності чи місця, з якого створено елемент [3, с. 96]
Гіперпосилання	Формалізований відповідно до стандартів мережі «Інтернет» запис адреси вебсайту або його частини (вебсторінки, даних). Якщо гіперпосилання адресує до частини вебсайту (вебсторінки), крім домену та/або числової адреси за Інтернет-протоколом, воно може містити додаткові записи про каталоги або виклики та умови доступу до вебсторінки, що може бути відтворена або збережена на пристроях, які можуть зчитувати та відтворювати електронну (цифрову) інформацію з використанням мережі «Інтернет» [5]
Дезінформація	Неправдива інформація, яка навмисно створюється та поширюється з явною метою заподіяння шкоди [3]
Добросовісне використання	Юридичний принцип, відповідно до якого захищені авторським правом матеріали за певних умов можна використовувати без дозволу правовласника [10]

Докази з відкритих джерел	Інформація у відкритому доступі з доказовою цінністю, яка може бути допущена для встановлення фактів у судовому процесі [3]
Електронний документ	Спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості у бінарному вигляді, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [11]. Його особливості: 1) характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія [12]; 2) допустимість електронного документа як доказу не можна заперечувати винятково на підставі того, що він має електронну форму [13]; 3) у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа [13]; 4) один і той самий електронний документ може зберігатися на різних носіях [12]
Запит	Спосіб отримання цифрової інформації у відкритому доступі через подачу запиту щодо публічної інформації до державних органів відповідно до законів про свободу інформації або доступу до інформації. Взаємодія із зовнішніми джерелами за допомогою сервісу обміну повідомленнями, чатів, форумів або електронної пошти виходить за межі розслідування з використанням даних у відкритому доступі [3]
Ідентифікація	Процес підтвердження достовірності повноважень користувача [7]

Інформаційна конфіденційність	Охоплює інформацію про людину, яка існує або може бути отримана [3]
Інформація із закритих джерел	Інформація з обмеженим доступом або доступом, що охороняється законом (наприклад, конфіденційна, таємна інформація) [3]
Комп'ютерні дані	Будь-яке подання фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою [14]
Комп'ютерна система	Будь-який пристрій чи група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких відповідно до певної програми виконує автоматичну обробку даних [14]
Комп'ютерна програма	Набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером (настільним комп'ютером, ноутбуком, смартфоном, ігровою приставкою, смарт-телевізором тощо), які приводять його у дію для досягнення певної мети або результату, зокрема операційна система, прикладна програма, виражені у вихідному або об'єктному кодах [5]
Купівля	Спосіб отримання цифрової інформації у відкритому доступі, який полягає в оплаті (повній або частковій) за можливість доступу до певної інформації. Ця платна послуга має бути доступна для всіх представників громадськості, але не як послуга, доступ до якої мають лише певні групи (співробітники правоохоронних органів або ліцензовані приватні слідчі) [3]

Машинний носій	*Див. «носії цифрових даних»*
Метадані	Дані про дані, тобто: каталоги, довідники, реєстри, бази метаданих (metadata base) та інші форми опису (метасупроводження) наборів цифрових і аналогових даних, що містять відомості про їх склад, зміст, статус (актуальність та оновлюваність), походження (способи та умови отримання), місцезнаходження, якість (повнота, несуперечність, достовірність), формати й форми подання, умови доступу, придбання й використання, авторські, майнові й суміжні з ними права на дані та ін. [7, с. 416–417]
Накопичувачі цифрових даних	*Див. «носії цифрових даних»*
Незмінність	Додатковий критерій достовірності цифрового доказу, який полягає у тому, що доказ не змінюється або не може змінюватися [15]
Неправдива інформація	Недостовірна інформація, що не призначена для заподіяння шкоди. Наприклад, люди, не знаючи про її неправдивість та маючи на меті бути корисними, поширюють таку інформацію в Інтернеті, соціальних мережах [3]
Нестійкі дані	Дані, специфічно схильні до змін та які може бути легко модифіковано [16]
Носії для збереження цифрових даних	*Див. «носії цифрових даних»*
Носії цифрових даних	Технічні засоби, що призначені для передачі цифрових сигналів у часі та просторі [17, с. 88]

Носії цифрової інформації	Файл, якому притаманні такі характерні риси, як опосередкованість через машинний (фізичний) носій; відсутність жорсткої позиційної прив'язки до тієї чи іншої ділянки машинного носія; можливість одночасного існування на різних носіях (мультиплікативність); можливість багаторазового запису на машинні носії [17, с. 86; 88; 98]
Обліковий запис	Формалізований згідно зі стандартами мережі «Інтернет» запис на комп'ютерному обладнанні (комп'ютерах, серверах), підключеному до мережі «Інтернет», що ідентифікує користувача (наприклад, власника вебсайту) на такому обладнанні, містить дані про доступ до частини каталогів і комп'ютерної програми, комп'ютерного обладнання, а також визначає права такого доступу, що надають можливість володільцю облікового запису додавати, видаляти, змінювати цифровий контент і дані вебсайту, надавати доступ до вебсайту або його частини, окремих даних іншим особам, припиняти функціонування такого вебсайту або його частини в межах облікового запису [5]
Онлайн-дані	*Див. «цифрова інформація у відкритому доступі»*
Онлайн-контент	*Див. «цифрова інформація у відкритому доступі»*
Онлайн-матеріал	*Див. «цифрова інформація у відкритому доступі»*
Оригінал електронного (цифрового) документа	Відображення, якому надається таке саме значення, як документу [11]
Парсинг	Аналіз отриманої інформації для наступного використання [18]

Пентестер	Фахівець, який шукає та використовує вразливості IT-інфраструктури компанії, щоб виявити слабкі місця системи раніше, ніж якийсь кібер-зловмисник захоче ними скористатися [19]
Розвідка з (за) відкритих(-ми) джерел(-ами)	*Див. «OSINT»*
Розслідування з використанням даних у відкритому доступі	Використання інформації у відкритому доступі для функцій збору інформації та доказів [3]
Скрейпінг (вебскрейпінг)	Збирання даних в Інтернеті за заданими параметрами, в основному через індивідуальні проксі [18]
Скриншот	Знімок екрана пристрою у певний момент часу
Спостереження	Спосіб отримання цифрової інформації у відкритому доступі [3]
Суміжне право	Права виконавців, виробників фонограм і відеограм на результати творчої діяльності, їх спадкоємців та осіб, яким на законних підставах передано суміжні майнові та немайнові права, а також організацій мовлення та їх право-наступників [20]
Твір	Оригінальне інтелектуальне творіння автора (співавторів) у сфері науки, літератури, мистецтва тощо, виражене в об'єктивній формі [5]
Цифрова бібліотека	*Див. «цифровий архів»*

Цифрова інформація	Збережувана (статична) і подана (динамічна) у формі файлу (на фізичному і логічному рівнях) цілісна сукупність даних, які мають смисл у виг-ляді, придатному для сприйняття людиною [17]
Цифрова інформація з відкритих джерел	*Див. «цифрова інформація у відкритому доступі»*
Цифрова інформація у відкритому доступі	Інформація, що є у відкритому доступі в Інтернеті та розміщена на загальнодоступних вебсайтах, у базах даних або на платформах соціальних ме-діа [3]
Цифровий архів	Колекція документів, вебсторінок або елек-тронних записів. Цей термін також може стосуватися офіційної чи неформальної органі-зації, яка бере на себе відповідальність за збереження інформації та надання її доступним авторизованим користувачам [3]
Цифровий контент	Будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі «Інтернет» [5]
Цифрові дані	Дискретні сигнали магнітної, оптичної, електронної природи [17]
Цифровий доказ	Інформація або дані, збережені чи передані в бінарному вигляді, на які можна посилатися як на докази [16]

Цифровий самозахист	Реалізації права будь-якими незабороненими законом засобами захищати свої права і свободи від порушень та протиправних посягань [17, с. 142; 21]
Штучний інтелект (AI)	Розділ комп'ютерної лінгвістики та інформатики, що займається формалізацією проблем та завдань, які нагадують завдання, виконувані людиною [22]

СПИСОК ВИКОРИСТАНИХ У ГЛОСАРІЇ ДЖЕРЕЛ

1. OSINT при розслідуванні кримінальних правопорушень: підручник / О. О. Торбас. Одеса : Вид-во «Юридика», 2024.

2. ICC Prosecutor Karim A. A. Khan KC announces launch of advanced evidence submission platform : OTPLink. *International Criminal Court* : website. URL: https://www.icc-cpi.int/ news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submissionplatform-otplink)

3. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних : практ. посіб. щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / [неофіц. пер. з англ. О. В. Зюзь]. Нью-Йорк і Женева : Центр з прав людини Каліфорн. ун-ту ; Берклі : Юрид. шк. ; ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

4. Chris Hoofnagle. Dark Web Intelligence: Methods & Legal Issues. BCLT Research2Practice. July 16, 2020. *Presentation*. URL: https://www.law.berkeley.edu/wp-content/uploads/2020/08/darknet_intel.pdf

5. Про авторське право і суміжні права: Закон України № 2811-20 від 01.12.2022 (редакція від 15.04.2023). URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

6. Бінарний перекладач. URL: https://charactercalculator.com/uk/binary-translator/

7. Тлумачний словник з інформатики / Г. Г. Півняк, Б. С. Бусигін, М. М. Дівізінюк та ін. Дніпропетровськ, Нац. гірнич. ун-т, 2010. 600 с.

8. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посіб. / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM). 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

9. Аврамова О. Є. Віртуальна (цифрова) особистість: суб'єктивний та об'єктивний аспект. *Зб. наук. пр. НДІ ПЗІР НАПрН України. Вип. : Інноваційний процес: виклики воєнного часу, проблеми, перспективи євроінтеграції*: за матеріалами Кругл. столу (м. Харків, 02 груд. 2022 р.) / за ред. С. В. Глібка, І. В. Подрез-Ряполової. Харків : НДІ ПЗІР НАПрН України, 2022.

10. Добросовісне використання на YouTube. Довідковий центр. *Youtube Довідка*. URL: https://support.google.com/youtube/answer/9783148?hl=uk

11. Кримінальний процесуальний кодекс України: Закон України № 4651-VI від 13.04.2012 (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/4651-17

12. Постанова Об'єднаної палати ККС ВС від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878кмо20). URL: https://reyestr.court.gov.ua/Review/96074938

13. Про електронні документи та електронний документообіг: Закон України № 851-IV від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

14. Конвенція про кіберзлочинність (дата підписання: 23.11.2001, дата набрання чинності в Україні: 01.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

15. Онлайн-бібліотека «Горох». URL: https://goroh.pp.ua/%D0%A2%D0%BB%D1%83%D0%BC%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F/%D0%BD%D0%B5%D0%B7%D0%BC%D1%96%D0%BD%D0%BD%D0%B8%D0%B9

16. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Вид. офіц. Київ : УкрНДНЦ, 2018. VI. 31 с.

17. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 88.

18. Що таке веб-скрейпінг і як він пов'язаний з проксі. *Astro* : вебсайт. 05.04.2022. URL: https://astroproxy.com/ua/terms-of-use

19. Пентестер: професія етичного хакера. *10guards* : вебсайт. 21.02.2022. URL: https://10guards.com/ua/articles/pentester-the-profession-of-ethical-hacker/

20. Правова охорона авторських і суміжних прав, прав інтелектуальної власності в Україні. *ЮК «УНІЛАВ»* : вебсайт. URL: https://unilaw.com.ua/pravova-ohorona-avtorskyh-i-sumizhnyh-prav/

21. Конституція України: Закон № 254к/96-ВР від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

22. Штучний інтелект. *Словник з інформатики* : веб-сайт. URL: http://xn--r1a3b.xn--b1amgblet.xn--j1amh/index.php/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82

ДОДАТОК

ПРОТОКОЛ ОГЛЯДУ

інформації з відкритих джерел мережі «Інтернет»

місто _____ «___» _____20__ року

Огляд почато о «____» год. «____» хв.

Огляд закінчено о «____» год. «____» хв.

_____

(слідчий, найменування органу, прізвище, ім'я, по батькові)

у кримінальному провадженні № _____ від _____ за ознаками кримінального правопорушення, передбаченого ст. _____ КК України у приміщенні_____ за адресою _____відповідно до ст. 104, 105, 106, 223, 237 КПК України та з урахуванням стандартів, викладених у Протоколі Берклі з ведення розслідувань з використанням відкритих цифрових даних, провів огляд інформації з відкритих джерелах мережі «Інтернет».

Під час огляду використовується комп'ютер / ноутбук *(технічні характеристики, операційна система, програмне забезпечення),* флеш-диск, інші носії інформації, на які здійснюватиметься копіювання інформації, що оглядається, принтер (*серійний номер, назва та модель принтера*), колонки, інші технічні засоби фіксації _____ _____.

У присутності понятих / без присутності понятих згідно з ч. 7 ст. 223 КПК України.

Огляд проводився без участі спеціаліста / за участю спеціаліста:

_____,

(прізвище, ім'я, по батькові, посада, документи, що підтверджуть фах)

якому відповідно до ч. 4, 5 ст. 71 КПК України роз'яснено його права та обов'язки.

За участю інших учасників:

1) _____,

(прізвище, ім'я, по батькові, дата народження, місце проживання)

2) _____.

(прізвище, ім'я, по батькові, дата народження, місце проживання)

Перед початком огляду зазначеним вище особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться у процесі огляду, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні огляду, також роз'яснено вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії, а також про застосування технічних засобів фіксації, умови та порядок їх використання: _____ _____.

(підписи осіб)

Здійснюється поетапний опис послідовності дій під час огляду інформації з вебсторінки, з чітким описом інформації, що оглядається, та графічним копіюванням оглянутих вебсторінок. Зазначається також: 1) інформація про утворений файл з назвою збереженої сторінки із розширенням «HTML» (у разі його створення або відмітка про його відсутність) і папка з назвою та часом її створення і розміром електронних файлів на визначеному носії та відомості про нього, в якій містяться автоматично створені файли цієї сторінки; 2) інформація про здійснення архівування потрібної сторінки в мережі «Інтернет» (у разі проведення архівування, опису процесу архівування із графічним зображенням процесу та логічними взаємозв'язками описаних дій та відомостями про розміщення файлу на фізичному носії). Якщо проводилось хешування файлу з метою отримання хеш-коду, зазначити результати вказаної операції.

Огляд проведено при штучному / денному освітленні. Будь-які зміни в ході огляду до зображень не вносилися.

Під час огляду фото-/відеозйомка застосовувалась / не застосовувалась.

Протокол прочитаний, від учасників слідчої дії зауважень не надійшло.

До протоколу огляду додаються додатки: _____

_____

(носій, на якому зберігається записана

_____

інформація (відео, фото, скріншоти))

Учасники:

1. _____ /_____/

(прізвище, ім’я, по батькові) (підпис)

2. _____ /_____/

(прізвище, ім’я, по батькові) (підпис)

Огляд провів:

_____

(слідчий, найменування органу, підпис, ініціали, прізвище)

АВТОРСЬКИЙ КОЛЕКТИВ

Гаврилюк Л. В. – начальник 3-го науково-дослідного відділу науково-дослідної лабораторії проблем правового та організаційного забезпечення діяльності Міністерства Державного науково-дослідного інституту Міністерства внутрішніх справ України, кандидат юридичних наук, старший дослідник

Басиста І. В. – професор кафедри кримінального процесу та криміналістики факультету № 1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ Міністерства внутрішніх справ України, доктор юридичних наук, професор

Афонін Д. С. – завідувач науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Шевчишен А. В. – заступник начальника Головного слідчого управління Національної поліції України, доктор юридичних наук, професор, заслужений юрист України

Хитра А. Я. – завідувач кафедри кримінального процесу та криміналістики факультету № 1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ Міністерства внутрішніх справ України, кандидат юридичних наук, доцент

Ліснiченко Д. В. – доцент кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Гутник А. В. – доцент кафедри кримінального процесу та криміналістики факультету № 1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ, доктор філософії у галузі права

Биков І. О. – старший науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, кандидат юридичних наук

Бурлака В. В. – начальник 3-го відділу управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, кандидат юридичних наук

Дрозд В. Г. – головний спеціаліст консультативно-контрольного відділу Департаменту забезпечення діяльності Голови Національної поліції України, доктор юридичних наук, професор, заслужений юрист України

Корнійко С. М. – науковий співробітник 1-го науково-дослідного відділу науково-дослідної лабораторії криміналістичної та спеціальної техніки Державного науково-дослідного інституту Міністерства внутрішніх справ України, кандидат юридичних наук

Пелехатий В. Т. – старший слідчий в особливо важливих справах 3-го відділу управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України

AUTHORS

Havryluk L. V. – Head of the 3d problems of legal and organizational support of the Ministry's activities' research and development division of the State Research and Development Institute of the Ministry of Internal Affairs of Ukraine, PhD in Law, senior researcher

Basysta I. V. – Professor of the Department of Criminal Procedure and Forensics, Faculty No. 1 of the Institute for the Training of Specialists for National Police Units of Lviv SUIA, D.J.S., professor

Afonin D. S. – Head of the research laboratory on problematic issues of criminal analysis of Odesa SUIA, PhD in Law, associate professor

Shevchyshen A. V. – Deputy Head of the Main Investigative Department of the National Police of Ukraine, D.J.S., professor, Honored Lawyer of Ukraine

Khytra A. Ya. – Head of the Department of Criminal Procedure and Forensics, Faculty No. 1 of the Institute for Training Specialists for National Police Units of Lviv SUIA, PhD in Law, associate professor

Lisnichenko D. V. – associate professor of the Department of Criminal Procedure and Forensics, Faculty of Training Specialists for Pre-trial Investigation Bodies of Odesa SUIA, PhD in Law, associate professor

Hutnyk A. V. – associate professor of the Department of Criminal Procedure and Forensics, Faculty No. 1 of the Institute for the Training of Specialists for National Police Units of Lviv SUIA, PhD in Law

Bykov I. O. – senior researcher of the research laboratory on problematic issues of criminal analysis of Odesa SUIA, PhD in Law

Burlaka V. V. – Head of the 3rd department of the department of the activity organization and methodological support of the CID, PhD in Law

Drozd V. G. – chief desk officer of the advisory and control department of the Department for ensuring the activities of the Head of the National Police of Ukraine, D.J.S., professor, Honored Lawyer of Ukraine

Korniiko S. M. – staff scientist of the 1st scientific and research division of forensic and special equipment's scientific and research laboratory of the State Research and Development Institute of the Ministry of Interior Affairs of Ukraine, PhD in Law

Pelekhatyi V. T. – senior investigator in particularly important cases of the 3rd department of the department of the activity organization and methodological support of the CID

Довідкове видання

Гаврилюк Людмила Володимирівна
Басиста Ірина Володимирівна
Афонін Дмитро Сергійович
Шевчишен Артем Вікторович
Хитра Андрій Ярославович
Лісніченко Дмитро Вікторович
Гутник Аліна Володимирівна
Биков Ігор Олегович
Бурлака Владислав Васильович
Дрозд Валентина Георгіївна
Корнійко Станіслав Миколайович
Пелехатий Віталій Тадейович

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ (ПРОТОКОЛ БЕРКЛІ)

Науково-практичний порадник

За загальною редакцією
доктора юридичних наук, професора,
заслуженого юриста України Максима Сергійовича Цуцкіридзе

Коректура *Наталії Мурашової*
Комп'ютерне верстання
Марини Марченко, *Анатолія Мушницького*

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Берестейський, 37, м. Київ, 03056

Підп. до друку 23.09.2024. Формат $60\times84^{1}/_{16}$. Папір офс. Гарнітура Calibri.
Спосіб друку – електрографічний. Ум. друк. арк. 15,07. Обл.-вид. арк. 14,09.
Поз. 24-1-1-011. Наклад 70 пр. Зам. № 24-070.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
03056, м. Київ
тел. (044) 204-81-78

View publication stats