ЗБИРАННЯ ТА ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

**ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

ЗБИРАННЯ ТА ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Методичні рекомендації

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

Київ – 2025

УДК 343.14+343.98]:004
З-41

Рекомендовано до друку рішенням Вченої ради Державного науково-дослідного інституту МВС України (протокол № 7 від 30 жовтня 2024 р.)

Авторський колектив:

Шевчишен А. В., доктор юридичних наук, професор, заслужений юрист України (ГСУ НПУ); ***Гаврилюк Л. В.***, кандидат юридичних наук, старший дослідник (ДНДІ МВС України); ***Ангеленюк А.-М. Ю.***, кандидат юридичних наук, старший дослідник (ДНДІ МВС України); ***Дрозд В. Г.***, доктор юридичних наук, професор, заслужений юрист України (ДЗДГ НПУ); ***Бурлака В. В.***, кандидат юридичних наук (ГСУ НПУ); ***Подиряко Х. В.*** (ГСУ НПУ); ***Пелехатий В. Т.*** (ГСУ НПУ); ***Віткалова А. Є.*** (ГСУ НПУ); ***Калантай І. М.*** (ГСУ НПУ); ***Дулкай І. І.*** (ГСУ НПУ)

Рецензенти:

Чорноус Ю. М. – професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктор юридичних наук, професор.

Мірковець Д. М. – керівник Головного слідчого управління Державного бюро розслідувань, доктор юридичних наук, професор, заслужений юрист України.

Пантелеєв С. М. – перший заступник начальника Головного слідчого управління Національної поліції України, доктор філософії (081 «Право»).

З-41 **Збирання та дослідження електронних доказів у кримінальному провадженні** : метод. рекомендації / А. В. Шевчишен, Л. В. Гаврилюк, А. М.-Ю. Ангеленюк, В. Г. Дрозд та ін. ; за заг. ред. М. С. Цуцкіридзе. – Київ : ДНДІ МВС України, Вид-во «Політехніка», 2025. – 165 с.

ISBN 978-966-990-142-2

Розкрито сутність, види і форми подавання електронних доказів у кримінальному провадженні. Визначено способи збирання і дослідження електронних доказів, особливості огляду, вилучення та упакування їх носіїв, підстави, процесуальний порядок призначення судових експертиз електронних носіїв інформації та інформації в електронній (цифровій) формі, а також види експертиз та орієнтовний перелік питань, що можуть бути поставлені під час проведення відповідного виду експертизи.

Методичні рекомендації розраховані для використання слідчими, дізнавачами, працівниками оперативних підрозділів, а також іншими зацікавленими особами у збиранні та дослідженні електронних доказів у кримінальному провадженні. Робота може бути корисною для науковців, викладачів, аспірантів, студентів закладів вищої освіти та іншим.

ISBN 978-966-990-142-2

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
STATE RESEARCH INSTITUTE

CENTRAL INVESTIGATION DEPARTMENT
OF THE NATIONAL POLICE OF UKRAINE

COLLECTION AND EXAMINATION OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

Methodical recommendations

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

Kyiv – 2025

UDC 343.14+343.98]:004
Z-41

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 (minutes No 7 as of 30 October 2024)

Authors:

Shevchyshen A. V., D.J.S., Professor, an Honored Lawyer of Ukraine (Main Investigative Department of the National Police of Ukraine); ***Havryliuk L. V.***, PhD in Law, senior researcher (State Research and Development Institute of the Ministry of Internal Affairs of Ukraine); ***Anheleniuk A.-M. Yu.***, PhD in Law, senior researcher (State Research and Development Institute of the Ministry of Internal Affairs of Ukraine); ***Drozd V. H.***, D.J.S., Professor, an Honored Lawyer of Ukraine (Department for ensuring the activities of the Head of the National Police of Ukraine); ***Burlaka V. V.***, PhD in Law (Main Investigative Department of the National Police of Ukraine); ***Podyriako Kh. V.*** (Main Investigative Department of the National Police of Ukraine); ***Pelekhatyi V. T.*** (Main Investigative Department of the National Police of Ukraine); ***Vitkalova A. Ye.*** (Main Investigative Department of the National Police of Ukraine); ***Kalantai I. M.*** (Main Investigative Department of the National Police of Ukraine); ***Dulkai I. I.*** (Main Investigative Department of the National Police of Ukraine)

Reviewers:

Chornous Yu. M. – Professor of the Department of Criminology and Forensic Medicine, National Academy of Interior Affairs of Ukraine, D.J.S., Professor.

Mirkovets D. M. – Head of the Main Investigative Department of the State Bureau of Investigation, D.J.S., Professor, an Honored Lawyer of Ukraine.

Panteleyev S. M. – Deputy Head of the Main Investigative Department of the National Police of Ukraine, PhD in Law.

Z-41 **Collection and examination of digital evidence in criminal proceedings :** methodical recommendations / A. V. Shevchyshen, L. V.Havryliuk, A.- M. Yu. Anheleniuk, V. H. Drozd et al. ; under the editorship of M.S. Tsutskiridze. – Kyiv : Ministry of the Internal Affairs of Ukraine's State Research and Development Institute, Publishing House «Polytechnica», 2025. – 165 p.

ISBN 978-966-990-142-2

The book outlines the essence, types and forms of digital evidence submission in criminal proceedings. The guidelines specify the methods for collecting and studying digital evidence, characteristic features of examining, removing and packaging of its media, the grounds and procedure for ordering forensic examinations of digital media and electronic (digital) data, as well as the types of examinations and a list of provisional questions that can be asked during the corresponding type of examination.

The guidelines are intended for the use by investigators, prosecutors, operational units' employees and other persons interested in the collection and application of digital evidence in criminal proceedings. The book can also be of use to scientists, lecturers, postgraduate students, and students of higher education institutions.

ISBN 978-966-990-142-2

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БПЛА	–	безпілотний літальний апарат
ГПК	–	Господарський процесуальний кодекс України
ЄРДР	–	Єдиний реєстр досудових рішень
КАС	–	Кодекс адміністративного судочинства України
ККС ВС	–	Касаційний кримінальний суд у складі Верховного Суду
КК	–	Кримінальний кодекс України
КПК	–	Кримінальний процесуальний кодекс України
КУ	–	Конституція України
НСРД	–	негласні слідчі (розшукові) дії
СРД	–	слідчі розшукові дії
ЦПК	–	Цивільний процесуальний кодекс України
IMEI	–	International Mobile Equipment Identifier (міжнародний ідентифікатор мобільного обладнання)
SIM	–	Subscriber Identification Mobile (ідентифікаційний модуль абонента)
абз.	–	абзац
п.	–	пункт
ст.	–	стаття
ч.	–	частина

ВСТУП

В сучасних умовах активного розвитку комп'ютерних і технічних інновацій матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) відіграють важливу роль у процесі доказування у кримінальному провадженні. Однією з умов успішної праці у практичних підрозділах є вміння обирати ту чи іншу тактику проведення процесуальних або слідчих (розшукових) дій, враховуючи особливості збирання електронних доказів. Утім, під час застосування норм Кримінального процесуального кодексу України (КПК), які регламентують правовідносини, пов'язані зі збиранням і дослідженням інформації в електронній (цифровій) формі у кримінальному провадженні, наявними є проблеми як правового, так і організаційного характеру, вирішення яких вимагає поєднання теоретичного осмислення проблеми із практичними рекомендаціями щодо збирання та дослідження електронних доказів у кримінальному провадженні.

У пропонованих методичних рекомендаціях авторами розкрито сутність електронних доказів у кримінальному провадженні, охарактеризовано їх види, визначено вимоги щодо допустимості електронних доказів. Приділено увагу способам збирання електронних доказів з урахуванням слідчої ситуації, формам подавання електронних доказів у суді, наведено методологію роботи із зображеннями на фото та методи роботи з відео, а також особливості пошуку й аналізу за фрагментарними даними фізичних осіб з використанням соціальних мереж тощо.

Також на підставі комплексного вивчення наукового матеріалу, аналізу практики реалізації положень КПК у процесі доказування у кримінальному провадженні, опрацювання рішень суду, систематизовано, акумульовано та узагальнено теоретичні та практичні аспекти щодо процедури збирання і дослідження електронних доказів у кримінальному провадженні.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ІНСТИТУТУ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

1.1. Електронні докази у системі процесуальних джерел доказів у кримінальному провадженні

Будь-яка наука повинна мати чітку систему понять, в якій усі поняття пов'язані одне з одним і є елементами одного нерозривного ланцюга[1]. Зважаючи на те, що термін «електронні докази» у кримінальному процесуальному законодавстві загалом не визначено, перш ніж розкрити кримінальні процесуальні та криміналістичні особливості збирання і дослідження електронних доказів у кримінальному провадженні вважаємо за необхідне з'ясувати та структуровано висвітлити, які саме об'єкти згідно із законодавством України підпадають під категорію «електронні докази» та що треба розуміти під «електронними доказами» у кримінальному процесі України.

На сьогодні термін «електронні докази» на законодавчому рівні визначений у Цивільному процесуальному кодексі України (ЦПК), Господарському процесуальному кодексі України (ГПК) та Кодексі адміністративного судочинства України (КАС). Так, згідно із ч. 1 ст. 100 ЦПК, ч. 1 ст. 96 ГПК та ч. 1 ст. 99 КАС **електронними доказами** є інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема електронні документи (у тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах,

[1] Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази: навч. посіб. / за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Львів: ЛНУ ім. Івана Франка, 2022. С. 124. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 11.04.2024).

системах резервного копіювання, в інших місцях зберігання даних в електронній формі (у тому числі в мережі «Інтернет»)[2; 3; 4].

Водночас слід зазначити, що визначення електронного доказу у кримінальному процесуальному законодавстві України немає. Згідно з ч. 2 ст. 84 КПК процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Відповідно до ч. 2 ст. 98 КПК *документи* є речовими доказами, якщо вони були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Отже, зазначенні у ч. 2 ст. 84 КПК джерела доказів та унормована у КПК процедура збирання, використання та їх оцінка не дають можливості розглядати електронні докази як окреме процесуальне джерело доказів, ознаки якого проглядаються у різних його нормах, які регламентують питання доказування у кримінальному провадженні.

Зокрема, у ч. 1 ст. 99 КПК зазначається, що *документом* є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження[5]. Окрім цього, згідно з ч. 2 ст. 99 КПК такі носії інформації, як матеріали фотозйомки, звукозапису, відеозапису, інші носії інформації, у тому числі комп'ютерні дані, віднесені до категорії «документ», який відповідно до ч. 2 ст. 98 КПК є речовим доказом, якщо він був знаряддям вчинення кримінального правопорушення, зберіг на собі його сліди або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

---

[2] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40–41, 42. Ст. 492. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 11.01.2024).

[3] Господарський процесуальний кодекс України: Закон України від 06.11.1991 р. № 1798-XII. *Відомості Верховної Ради України*. 1992. № 6. Ст. 56. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (дата звернення: 05.03.2024).

[4] Кодекс адміністративного судочинства України: Закон України від 06.07.2005 р. № 2747-IV. *Відомості Верховної Ради України*. 2005. № 35–36, 37. Ст. 446. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 01.02.2024).

[5] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

Виходячи із цього констатуємо, що *передбачені ЦПК, ГПК та КАС види електронних доказів у КПК віднесені до категорії «документ», який за певних умов набуває статусу речового доказу і може бути доказом у кримінальному провадженні за умови, якщо:*

1) був засобом чи знаряддям вчинення кримінального правопорушення;

2) зберіг електронно-цифрові сліди кримінального правопорушення;

3) містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час досудового розслідування.

З огляду на зазначене вище **до категорії «електронні докази» у кримінальному процесі України слід віднести інформацію в електронній (цифровій) формі, що зафіксована**:

1) в електронному документі;

2) у матеріалах фотозйомки;

3) у матеріалах звукозапису;

4) у матеріалах відеозапису;

5) на інших носіях інформації (у тому числі комп'ютерні дані).

Такий перелік не є класифікацією електронних доказів, оскільки охоплює види носіїв та джерела інформації в електронній (цифровій) формі. Цей перелік є орієнтовним для учасників кримінального провадження щодо того, які фактичні дані в електронній (цифровій) формі можуть бути визнані електронними доказами у суді та де їх слід шукати.

1.2. Види електронних доказів у кримінальному провадженні

Наведений у підрозд. 1.1 перелік носіїв інформації в електронній (цифровій) формі не є вичерпним, що пов'язано із постійним розвитком інформаційно-комунікаційних технологій, які дозволяють користувачам створювати, отримувати доступ, зберігати, передавати і змінювати інформацію. Щоб з'ясувати суть кожного із них, пропонуємо більш детально їх охарактеризувати.

Електронний документ

Електронний документ – це документ, інформація в якому зафіксована у вигляді *електронних даних*, включаючи обов'язкові реквізити документа (ч. 1 ст. 5 Закону України «Про електронні документи

та електронний документообіг»)[6]. Згідно з абз. 3 ст. 1 цього закону *дані* – це інформація, яка подана у формі, придатній для її оброблення електронними засобами. Склад і порядок розміщення обов'язкових реквізитів електронних документів визначаються законодавством України.

Під час використання електронного документа як доказу у кримінальному провадженні слідчий має врахувати, що:

- *Електронний документ* є різновидом документа як процесуального джерела доказу (ст. 99 КПК), який *набуває процесуального значення доказу після його огляду*, за умови виявлення слідчим, прокурором, під час такого огляду відомостей щодо обставин вчинення кримінального правопорушення, які мають бути належним чином зафіксовані у протоколі огляду (ч. 1, абз. 2 ч. 2 ст. 237 КПК).
- *Електронний документ* може бути створений, переданий, збережений і перетворений електронними засобами у *візуальну форму*.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною.

Стаття 6 Закону України «Про електронні документи та електронний документообіг» передбачає, що для ідентифікації автора електронного документа може бути використаний електронний підпис, а для підтвердження достовірності походження та цілісності електронного документа може використовуватися електронна печатка[7].

Звертаємо увагу на підпис в електронних документах, оскільки він є одним з обов'язкових його реквізитів. Таким підписом може бути електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України[8] «Про електронну ідентифікацію та електронні довірчі послуги» (кваліфікований електронний підпис, удосконалений електронний підпис).

---

[6] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 15.02.2024).

[7] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 15.02.2024).

[8] Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII (станом на 01.01.2024 р.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 29.04.2024).

Електронний підпис – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і які підписувач використовує як підпис.

Кваліфікований електронний підпис – удосконалений електронний підпис, що створюється з використанням засобу кваліфікованого електронного підпису і ґрунтується на кваліфікованому сертифікаті електронного підпису.

Удосконалений електронний підпис, що ґрунтується на кваліфікованому сертифікаті електронного підпису, – удосконалений електронний підпис, що створюється з використанням кваліфікованого сертифіката електронного підпису, виданого кваліфікованим надавачем електронних довірчих послуг, і не містить відомостей про те, що особистий ключ зберігається у засобі кваліфікованого електронного підпису.

Матеріали фотозйомки, відеозапису, звукозапису

У кримінальному провадженні матеріали фотозйомки, відеозапису і звукозапису досить часто є носіями інформації про обставини кримінального правопорушення та можуть вказувати на причетність певної особи до його вчинення.

Фотозображеннями можуть бути фотокартки, діапозитиви, негативи, мікрофільми, мікрофіші, кінофільми, відеозаписи тощо. До фотознімків належать також фотозображення, отримані без використання мокрого фотопроцесу шляхом друку на сучасних електронних засобах, але при цьому формування самого зображення обов'язково включає оптичний канал [9].

Загалом *фотознімок* за природою є технічним носієм з інформацією про зовнішній стан середовища (об'єкта) у конкретний момент часу, при цьому інформація про це може фіксуватись на технічному носії як у неперервній (аналоговій), так і в дискретній (цифровій) формі. Ступінь відповідності інформації оригіналу визначається технічними характеристиками пристрою, який фіксує та записує на носій цю інформацію[10].

---

[9] Фототехнічна експертиза. URL: https://kndise.gov.ua/fototehnichna/ (дата звернення: 02.08.2023).

[10] Фототехнічна експертиза. URL: https://kndise.gov.ua/fototehnichna/ (дата звернення: 02.08.2023).

Фотографії та зображення в електронному вигляді мають безліч позитивних властивостей під час доказування. Зображення, зафіксоване статично, дає можливість оцінити інформацію, яка має доказове значення у кримінальному провадженні. Сприйняття доказу особисто покращує розуміння ситуації, обстановки та обставин події, які відбулись. Під час огляду фотографії є можливість збільшити, зменшити зображення і привернути увагу до важливих деталей на ній. Метадані, що містяться у файлі цифрової фотографії, дають можливість встановити час і дату фотографування та технічний пристрій, за допомогою якого проводилось фотографування[11].

Звукозапис – це результат фіксування в об'єктивній (матеріальній або електронній (цифровій) тощо) формі за допомогою технічних пристроїв звуків чи відображень звуків, що дозволяє за допомогою відповідних пристроїв здійснювати їх сприйняття, відтворення, передавання тощо (п. 22 ч. 1 ст. 1 Закону України «Про авторське право і суміжні права» від 01 грудня 2022 р., № 2811-IX)[12].

Наприклад, звукозаписами, які використовують як доказ у кримінальному провадженні, можуть бути аудіоповідомлення, записи телефонних розмов тощо.

Відеозапис – це результат фіксування в об'єктивній (матеріальній або електронній (цифровій) тощо) формі за допомогою технічних пристроїв зображень або зображень зі звуком (відеозвукозапис), що дозволяє за допомогою відповідних пристроїв здійснювати їх сприйняття, відтворення, передавання тощо (п. 22 ч. 1 ст. 1 Закону України «Про авторське право і суміжні права» від 01 грудня 2022 р., № 2811-IX)[13].

Наприклад, відеозаписами можуть бути різноманітні відео із камер відеоспостереження, мобільних телефонів, різного типу відеореєстраторів, із безпілотних літальних апаратів (БПЛА), портативних відеореєстраторів тощо.

Однією з особливостей відео- та звукозаписів є їх динамічність. Відбувається безперервне відображення, збереження та наступне відтворення, а також зорове і слухове сприйняття учасниками процесу

---

[11] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. / А. В. Гутник, А. Я. Хитра. Львів: ЛьвДУВС, 2022. С. 55.

[12] Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 28.06.2024).

[13] Там само.

обставин дійсності в якісних, кількісних і просторових змінах, що відбувались з людьми та предметами матеріального світу протягом певного проміжку часу. Саме фіксація в динаміці всіх відомостей про обставини кримінального правопорушення надає можливість отримати найповнішу інформацію про них слідчому, дізнавачу, суду та іншим особам, які беруть участь у кримінальному провадженні[14].

На відміну від показань чи речових доказів матеріали звукозапису, відеозапису та відеозвукозапису, на яких зафіксована інформація про обставини вчинення злочину, дають можливість слідчому, суду та особам, які беруть участь у провадженні, безпосередньо сприйняти в динаміці та об'єктивно оцінити обставини вчинення кримінального правопорушення.

Беручи до уваги наведене в Законі України «Про інформацію» визначення терміна «документ», під яким слід розуміти матеріальний носій, що містить інформацію, основними функціями якого є її збереження й передавання у часі та просторі, а також визначення терміна «доказ», яке наведено у ст. 84 КПК, у кримінальному провадженні:

Матеріали фотозйомки, відеозапису та звукозапису – це носії інформації, які містять фактичні дані, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню.

Як було зазначено вище, матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) згідно з ч. 2 ст. 99 КПК також віднесені до категорії «документ», утім, на відміну від електронного документа, законодавством України не передбачено окремий порядок ідентифікації автора і підтвердження достовірності походження та цілісності матеріалів фотозйомки, звукозапису, відеозапису. У зв'язку із цим досить часто виникають проблеми зі встановленням особи, яка їх створила.

Встановити оригінальність, автентичність, ознаки монтажу, а також ряд інших питань, які треба з'ясувати з метою встановлення способу походження цих матеріалів тощо, можна шляхом проведення експертного дослідження.

[14] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. / А. В. Гутник, А. Я. Хитра. Львів: ЛьвДУВС, 2022. С. 54.

Інші носії інформації (у тому числі комп'ютерні дані)

Стаття 99 КПК передбачає, що до документів, за умови наявності в них відомостей, передбачених ч. 1 цієї статті, можуть належати інші носії інформації (у тому числі комп'ютерні дані). На сьогодні відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, можуть міститися в електронних повідомленнях, пристроях GPS, хмарних сховищах, у відкритих джерелах мережі «Інтернет», у комп'ютерних даних тощо.

Електронне повідомлення – це інформація, надана споживачу через телекомунікаційні мережі, яка може бути у будь-який спосіб відтворена або збережена споживачем в електронному вигляді (п. 10 ч. 1 ст. 1 Закону України «Про захист прав споживачів» від 12 травня 1991 р., № 1023-XII)[15].

Електронні повідомлення можуть бути текстовими, голосовими і мультимедійними.

Для *прикладу* наведемо такі види електронних повідомлень:

1) електронні листи, обмін якими здійснюється з використанням електронної пошти;

2) СМС-повідомлення, обмін якими здійснюється з використанням мобільного телефону;

3) повідомлення, обмін якими здійснюється з використанням безкоштовних месенджерів* (наприклад, «Telegram», «Viber», «WhatsApp», «Signal» тощо), які доступні на різних платформах, включаючи смартфони, планшети і комп'ютери, також для передавання повідомлень можуть використовуватись соціальні мережі (наприклад, «Facebook», «Youtube», «Instagram» тощо).

Зміст електронних повідомлень може містити інформацію про:

– особу, яка вчинила кримінальне правопорушення, співучасників, потерпілого та свідків;

– про обставини вчинення кримінального правопорушення тощо.

---

[15] Про захист прав споживачів: Закон України від 12.05.1991 р. № 1023-XII. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text (дата звернення: 28.06.2024).

* *Месенджер* – це програма, мобільний додаток або вебсервіс для миттєвого обміну повідомленнями.

Інформація, що міститься на портативних пристроях GPS

GPS – це спеціальна система навігації, яка працює за допомогою супутників. Завдяки її застосуванню можна досить швидко визначити фактичне розташування конкретного об'єкта, на якому розміщено приймач. Системи GPS можуть бути встановлені у планшетах, телефонах. Також для цього використовують спеціальні трекери, якими на сьогодні обладнано більшість мобільних телефонів, планшетів, ноутбуків та інших пристроїв.

Пристрої GPS на відкритій місцевості можуть визначати фактичне розташування предмета/людини з точністю 1-2 метри. Якщо об'єкт перебуває у лісовій місцевості чи густо забудованому середмісті, показники точності можуть бути знижені до 3-20 метрів. Якщо використовувати додаткові пристрої, то точність місця, де перебуває об'єкт, можна збільшити[16].

Інформація, що міститься на портативних пристроях GPS, у сукупності з іншими доказами (показання свідків, потерпілого, підозрюваного, результати проведених СРД, НСРД) можуть використовуватися як доказ під час розслідування різних видів кримінальних правопорушень.

Інформація, розміщена у хмарних сховищах

На сьогодні провайдери хмарних послуг розширили можливості мобільних пристроїв, що дозволяє зберігати й отримувати доступ до даних поза межами внутрішньої пам'яті пристрою у хмарних сховищах, які надають можливість доступу користувачам до одних і тих самих даних на кількох платформах або пристроях.

Хмарне сховище – це місце на віддаленому сервері, де користувач може зберігати, надсилати та отримувати файли, цифрові об'єкти і документи.

Найбільш популярні хмарні сховища – «Google Drive» від Google; «OneDrive» від Microsoft; MEGA; Dropbox; Samsung Cloud; iCloud від Apple; Xiaomi Cloud; GigaCloud[17].

Комп'ютерні дані

Під **комп'ютерними даними** слід розуміти будь-яке подання фактів, інформації або концепцій у формі, яка є придатною для оброб-

[16] GPS: що це, і який принцип роботи. URL: https://gpsuaservice.com.ua/gps-shcho-tse-i-yakyi-pryntsyp-roboty/

[17] ТОП-7 хмарних сховищ. URL: https://gigacloud.ua/blog/navchannja/top-7-hmarnih-shovisch

ки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб забезпечити виконання певної функції *комп'ютерною системою*[18]. *Комп'ютерна система* – це будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких відповідно до певної програми виконує автоматичну обробку даних[19].

Будь-які дії користувача, які пов'язані з використанням можливостей електронно-обчислювальних пристроїв, приводять до утворення в їх пам'яті нових чи зміни наявних комп'ютерних даних, за якими можна відстежити будь-які дії правопорушника, що були пов'язані з використанням можливостей комп'ютерної техніки.

Комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки унаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення, утворюють цифрові (електронні) сліди[20].

Комп'ютерні дані можуть бути джерелом криміналістичної інформації, як відносно злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, так і інших видів злочинів, де вони присутні.

Цифрові (електронні) сліди як комп'ютерні дані мають певні властивості, що є суттєвими для їх розуміння і використання під час розслідування кримінальних правопорушень[21].

Окрім, такі сліди кримінального правопорушення мають певні особливості, які повинні бути враховані під час їх пошуку, збирання та дослідження.

Зважаючи на технічні особливості, комп'ютерні дані не можуть бути безпосередньо сприйняті органами чуття людини і завжди потребують інтерпретації (перетворення у прийнятну для людини форму) з використанням комп'ютерної техніки. Інформацію, що містить подібний слід, може бути відображено на екрані комп'ютера чи роздруковано у закодованій формі (байт-код, бінарний код, синтаксичний запис тощо). Комп'ютерні дані, що містять текст, зображення, звуки

---

[18] Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 01.02.2024).

[19] Там само.

[20] Криміналістика: криміналістична техніка: навч. посіб. /Р. Л. Степанюк та ін.; МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2023. С. 114.

[21] Криміналістика: криміналістична техніка … . С. 114.

та інші аудіовізуальні форми інформації, можуть бути відтворені через пристрої виведення даних, а код, що містить алгоритми дій, може бути виконано (запущено програму). Аудіовізуальна форма відображення даних найчастіше доступна через використання спеціального (асоційованого) програмного забезпечення[22].

Інформація з відкритих джерел мережі «Інтернет»

Велику кількість інформації (публікації, фото, відео тощо), яка може містити фактичні дані про вчинення різного виду кримінальних правопорушень, розміщено у мережі «Інтернет», її відносять до категорії цифрової інформації з відкритих джерел. На практиці досить часто виникають проблеми щодо розуміння «відкритих джерел», їх переліку та способів отримання.

За змістом Протоколу Берклі[23] залежно від способу отримання інформацією з відкритих джерел мережі «Інтернет» є та:

1) яку можна отримати, перейшовши на відповідний сайт з використанням будь-якого безкоштовного веб-браузера;

2) яку можна отримати шляхом входу або зареєструвавшись на онлайн-платформі з метою доступу до нього та його перегляду;

3) яка міститься на платних платформах або на платформах, в яких додаткові функціональні можливості та доступ до даних є платними;

4) яка міститься у базах даних і на платформах, які можуть бути доступними для всіх представників громадськості лише на платній основі;

5) яку можна отримати за запитом, з яким може звернутися будь-яка особа до державних органів, що мають юридичні зобов'язання відповідати однаково всім особам щодо публічної інформації відповідно до законодавства про інформацію.

---

[22] Там само.

[23] 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-ProtocolUkrainian.pdf

До видів «відкритих джерел цифрової інформації»[24; 25; 26] відносять:

1. ***Медіа*** – різні матеріали (стаття, фоторепортаж, відео- та аудіозаписи), які створені чи отримані під час журналістської діяльності. Можуть бути опубліковані на вебсайтах, у *Telegram*, *Youtube*, *Twitter*, *Facebook*, *Instagram*.

2. ***Соціальні медіа*** – платформи, створені для комунікації між користувачами, які включають обмін повідомленнями, зображеннями, фото, відео, аудіо та іншими творами (блоги, соціальні мережі (*Telegram, Youtube, Twitter, Facebook, Instagram; медіа-платформи*)).

3. ***Вебсайти*** – 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. Вебсторінка – складова частина вебсайту, розміщена за спеціальною адресою в мережі «Інтернет»[27].

4. ***Геопросторові платформи*** (супутникові знімки; карти).

5. ***Бази даних*** (державні; приватні).

6. ***Офіційні дані*** (міжнародних організацій; органів державної влади та місцевого самоврядування; незалежних і приватних організацій)[28].

7. ***Інші платформи***, на яких можна спостерігати, купувати або запитувати загальнодоступну інформацію.

---

[24] Протокол Берклі … . С. 25–26.

[25] 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. Цуцкірідзе. Київ: ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с..

[26] 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. 223.

[27] Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 28.06.2024).

[28] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі). … .

1.3. Форми подання електронних доказів у кримінальному провадженні

Відповідно до ст. 99 КПК формами подання документа у кримінальному провадженні (матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі комп'ютерних даних)), є надання:

1) оригіналу документа;

2) оригіналу електронного документа;

3) дубліката документа, виготовленого слідчим, прокурором із залученням спеціаліста таким самим способом, як і його оригінал (ч. 3 ст. 99 КПК);

4) копії інформації, у тому числі комп'ютерних даних, що міститься:

– в інформаційних (автоматизованих) системах;

– електронних комунікаційних системах;

– інформаційно-комунікаційних системах;

– комп'ютерних системах;

– їх невід'ємних частинах.

Такі копії виготовляють слідчий, прокурор із залученням спеціаліста.

Сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал документа.

Отже, для того, щоб електронні докази відповідали вимогам кримінального процесуального законодавства, вони можуть бути надані до суду в одній із таких форм:

• ***В оригіналі.***

Оригіналом електронного документа є його відображення, якому надається таке саме значення, як документу з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (ч. 3 ст. 99 КПК, ч. 1 ст. 7 Закону України «Про електронні документи та електронний документообіг»).

Оригінал електронного документа повинен давати змогу довести його цілісність і справжність у порядку, визначеному законодавством.

Якщо автор створює ідентичні за документарною інформацією та реквізитами електронний документ і документ на папері, кожний з документів є оригіналом і має однакову юридичну силу (ст. 7 Закону України «Про електронні документи та електронний документообіг»[29]).

Слід зауважити, що у деяких випадках використовують скановані документи з «мокрими» реквізитами (рукописними записами, підписами, відбитками печаток) без накладання кваліфікованого електронного підпису. У такому випадку під час збирання доказів слід до матеріалів кримінального провадження долучити як доказ паперовий документ, з якого була виготовлена сканована копія електронного документа, оскільки у експертів щодо електронних документів, які не мають паперового оригіналу, під час проведення експертизи можуть виникати сумніви щодо ідентифікації особи-підписанта[30].

Перевірити електронний цифровий підпис та електронну печатку можна за допомогою державного онлайн-сервісу (Державний засвідчувальний орган Міністерства цифрової трансформації України), скориставшись визначеними у таблиці рекомендаціями.

---

[29]Про електронні документи та електронний документообіг»: Закон України від 22.05.2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text(дата звернення: 15.02.2024).

[30] Юзишина Т. В. Проблематика проведення судово-почеркознавчої експертизи при ідентифікаційному дослідженні почерку та підписів в електронних документах. *Експерт: парадигми юридичних наук і державного управління*. № 1 (25). 2023. С. 56–61. URL: https://doi.org/10.32689/2617-9660-2023-1(25)-56-61(дата звернення: 28.06.2024).

Рекомендації щодо перевірки кваліфікованого електронного підпису (печатки)

1. Отриманий засобами електронного поштового зв'язку документ – сертифікат суб'єкта оцінювальної діяльності в електронній формі, підписаний кваліфікаційним електронним підписом та засвідчений кваліфікованою електронною печаткою, потрібно зберегти на «Робочому столі» персонального комп'ютера (ноутбука).

2. Зайти на головну сторінку державного онлайн-сервісу за електронною адресою czo.gov.ua, на якій знайти рубрику «Довірчі послуги».

3. У рубриці «Довірчі послуги» знайти підрубрику «Перевірити підпис».

4. Після відкриття підрубрики «Перевірити підпис» у запропоноване сервісом вікно треба завантажити файл з електронним сертифікатом за допомогою вікна вибору файлу з файлової системи комп'ютера.

5. Натиснути кнопку «Перевірити».

6. Після успішної перевірки сервіс надасть результати перевірки електронної печатки. При цьому візуально можна буде побачити чотири вікна, які містять файли: «Файл з підписом», «Файл без підпису», «Протокол створення та перевірки кваліфікованого електронного підпису» та інформацію щодо кваліфікованої електронної печатки у вікні «Підписувачі». «Файл з підписом» містить файл із кваліфікованим електронним підписом і накладеною кваліфікованою печаткою підписанта; «Файл без підпису» – файл із кваліфікованим електронним підписом.

7. Скачати «Файл без підпису», натиснувши на стрілку навпроти нього.

8. Правою кнопкою миші (на файлі на нижній панелі) натиснути на клавішу «Показати в папці».

9. У папці «Загрузки» («Downoluads») відкрити файл за допомогою архіватора 7-Zip → Open archive → *

10. У вікні архіву слід скопіювати файл з електронним сертифікатом і зберегти на робочому столі.

11. Зазначений вище файл містить файл із кваліфікованим електронним підписом підписанта та оригінальний файл електронного сертифіката.

Оригіналом матеріалів фотозйомки, відеозапису та звукозапису є інформація, розміщена на технічному пристрої, з використанням якого вона була зафіксована.

Наприклад, оригінал відеозапису з камер відеоспостереження зберігається на носії інформації, на який вперше було записано відео.

Оригіналом текстових, мультимедійних і голосових повідомлень є інформація на відповідному акаунті або пристрої, на якому вона була створена.

Для *інформації із вебсайтів оригіналом* буде інформація створена/розміщена на вебсторінці у мережі «Інтернет».

- ***Копія документа.***

Під *копією (документа)* слід розуміти документ, що містить точне знакове відтворення змісту чи документної інформації іншого документа, а в окремих випадках – деяких його зовнішніх ознак (п. 3.10 ДСТУ 2732:2004).

Відповідно до ч. 4 ст. 99 КПК *копії інформації,* у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінали документа.

Наприклад, переміщені фото, звукозапис та відеозапис із носія інформації, на якому вони були створенні, на інший, слід вважати копією. Така копія може бути використана як доказ у кримінальному

провадженні за умови, що вона виготовлена слідчим, прокурором із залученням спеціаліста.

• ***Дублікат документа.***

У КПК поняття «*дублікат документа*» визначено у ч. 4 ст. 99 як документ, виготовлений таким самим способом, як і його оригінал. Враховуючи, що під документом як джерелом доказів законодавець розуміє спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, у тому числі матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема й електронні), складені в порядку, передбаченому КПК, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (ч. 1, пп. 2, 3 ч. 2 ст. 99 КПК), колегія суддів не вбачає жодних перепон у можливості надання до суду дублікатів протоколів процесуальних дій, а також матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (зокрема й електронних), виготовлених слідчим, прокурором із залученням спеціаліста, які визнаються судом як оригінал документа[31; 32].

Щоб підтвердити зміст документа, можуть бути визнані допустимими й інші відомості, якщо:

1) оригінал документа втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його надає;

2) оригінал документа не може бути отриманий за допомогою доступних правових процедур;

3) оригінал документа перебуває у володінні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони (ч. 5 ст. 99 КПК).

Також ч. 6 ст. 99 КПК передбачає, що сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право надати витяги, компіляції,

---

[31] Копія та дублікат службового документа: ВС розбирався, чи є між ними різниця. URL: https://sud.ua/ru/news/sudebnaya-praktika/208995-kopiya-ta-dublikat-sluzhbovogo-dokumenta-vs-rozbiravsya-chi-ye-mizh-nimi-riznitsya(дата звернення: 21.05.2024).

[32] Надія Стефанів. Суддя Верховного Суду. Судова практика ККС Верховного Суду щодо допустимості електронних доказів. С. 12. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf.

узагальнення документів, які незручно повністю досліджувати у суді, а на вимогу суду зобов'язані надати документи у повному обсязі.

Витяг з електронного документа – це певна частина змісту електронного документа, яка може підтверджувати чи спростовувати відомості, які підлягають доказуванню. У витягу з електронного документа частину інформації та зміст ідентично відтворено з основного документа[33].

Узагальнення та компіляція інформації в електронній (цифровій) формі потрібні тоді, коли вся інформація є важливою та не підлягає окремому виділенню частини. Обсяг і форму такого виокремлення інформації чітко не встановлено, їх фактично визначає за внутрішнім переконанням особа, яка проводить таке виокремлення. Головним завданням є відсіяти інформацію, яка не є суттєвою, і виявити інформацію, яка має значення під час доказування. *Наприклад*, це може бути вирізання частини звукозапису чи відеозапису, збільшення частини фотографії чи зображення, узагальнення змісту сторінки вебсайту тощо. Ця дія є суб'єктивною, тому оцінити правильність складання скороченого чи узагальненого електронного документа може лише суд. Таким чином, якщо зроблено витяг, компіляцію чи узагальнення електронного документа, то його разом із повним за обсягом і змістом оригіналом необхідно долучати до матеріалів кримінального провадження[34].

Судова практика

Серед питань, зумовлених оцінюванням процесуальних джерел в електронній формі, які виникають під час розгляду кримінальних проваджень, важливими є визначення співвідношення оригіналу та копії електронного доказу, правове оцінювання тверджень щодо цілісності електронного доказу, що міститься на диску або флешкарті, відмінностей між різними файлами, а також оцінювання скріншота.

За словами голови Касаційного кримінального суду у складі Верховного суду (ККС ВС), у судах першої та апеляційної інстанцій поширена практика заявлення клопотань захисниками про недопустимість електронного доказу на підставі того, що він є копією невідповідного

[33] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. / А. В. Гутник, А. Я. Хитра. Львів: ЛьвДУВС, 2022. С. 48.

[34] Там само.

оригіналу, оскільки було копіювання з карти пам'яті на комп'ютер, а лише після цього записано на оптичний диск, унаслідок чого, на думку сторони кримінального провадження, порушено цілісність електронного доказу. Утім, копії файлів, які є оригіналом доказу, може бути записано за допомогою технічних засобів, відмінних від тих, на які здійснюється запис оригіналу, унаслідок чого є відмінності у форматах запису файлів або поділ запису на декілька файлів без втрати його змісту.

З матеріалів судової практики випливає, що відмінності у форматі запису розглядалися стороною захисту як можливість умисного технічного втручання і підробки електронного доказу. Лише у деяких випадках суди визнавали докази недопустимими, погоджуючись із доводами сторони захисту про те, що відмінність у форматі запису може свідчити про редагування електронного доказу. Натомість суди переважно беруть до уваги процесуальну поведінку сторони: чи було подано клопотання про проведення експертизи та чи висловлювала сторона захисту заперечення щодо долучення відомостей в електронній формі як доказу.

Ще одним із проблемних питань є оцінювання скріншота. Трапляються справи, в яких усе провадження побудовано на скріншотах, публічних виступах на заходах, на новинах. Суд визначив *скріншот* як відображення електронного документа незалежно від електронної чи паперової форми. Утім, скріншот може відображати не лише електронний документ у розумінні ст. 5 Закону України «Про електронні документи та електронний документообіг», а й окремі кадри відеозаписів, фрагменти контенту вебсайтів, сторінок у соціальних мережах, порядок виготовлення копій яких (як і їх засвідчення) не регламентовано законом.

Попри те, що суди посилалися у своїх вироках на скріншоти зображень з електронних носіїв інформації, вебсторінок із мережі «Інтернет» як у цифровій, так і в паперовій формі, питання оцінювання допустимості скріншотів як доказів у судовій практиці на сьогодні залишається суперечливим і потребує додаткового регулювання. Таким чином, переважна більшість питань, пов'язаних з оцінюванням електронних доказів, вирішується судами під час правозастосування у процесуальному порядку[35].

[35] Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/(дата звернення: 28.06.2024).

РОЗДІЛ 2. ПРОЦЕСУАЛЬНІ МЕХАНІЗМИ ЗБИРАННЯ ТА ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

2.1. Допустимість електронних доказів у кримінальному провадженні

Згідно із Законом України «Про інформацію» від 02 жовтня 1992 р., № 2657-XII будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, відносять до категорії «інформація». Створення, збирання, отримання, зберігання, використання, поширення, охорона та захист інформації мають здійснюватися відповідно до законодавства України. Отже, інформація в електронній (цифровій) формі підпадає під категорію, на яку розповсюджується ряд правових гарантій. Зважаючи на зазначене та на зміст ст. 84–86 КПК, **інформація в електронній (цифровій) формі набуде статусу доказу, якщо:**

1) прямо чи непрямо підтверджує 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;

2) отримана у порядку, встановленому КПК.

Електронний доказ має відповідати загальним критеріям допустимості доказів відповідно до КПК й має бути отриманий:

1) належним суб’єктом;

2) із дотриманням процесуальної форми збирання та фіксації;

3) із належного процесуального джерела.

Недопустимий доказ не може бути використаний під час прийняття процесуальних рішень, на нього не може посилатися суд під час ухвалення судового рішення.

Недопустимими є докази, отримані унаслідок істотного порушення прав і свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій унаслідок істотного порушення прав і свобод людини (ч. 1 ст. 87 КПК).

У ч. 2 ст. 87 КПК, зокрема, зазначено, що *суд зобов'язаний визнати істотними порушеннями прав людини та основоположних свобод такі діяння:*

1) здійснення процесуальних дій, які потребують попереднього дозволу суду, без такого дозволу або з порушенням його суттєвих умов;

2) отримання доказів унаслідок катування, жорстокого, нелюдського або такого, що принижує гідність особи, поводження, або погрози застосування такого поводження;

3) порушення права особи на захист;

4) отримання показань або пояснень від особи, якій не було повідомлено про її право відмовитися від давання показань та не відповідати на запитання, або їх отримання з порушенням цього права;

5) порушення права на перехресний допит.

Окрім цього, за ч. 3 ст. 87 КПК[36] *недопустимими є також докази, що були отримані*:

1) з показань свідка, який надалі буде визнаний підозрюваним або обвинуваченим у цьому кримінальному провадженні;

2) після початку кримінального провадження шляхом реалізації органами досудового розслідування або прокуратури своїх повноважень, не передбачених КПК, для забезпечення досудового розслідування кримінальних правопорушень;

3) під час виконання ухвали про дозвіл на обшук житла чи іншого володіння особи у зв'язку з недопущенням адвоката до цієї слідчої (розшукової) дії (факт недопущення до участі в обшуку адвокат зобов'язаний довести у суді під час судового провадження);

4) під час виконання ухвали про дозвіл на обшук житла чи іншого володіння особи, якщо така ухвала винесена слідчим суддею без проведення повної технічної фіксації засідання.

Норми КПК передбачають змагальність сторін кримінального провадження у процесі доказування та свободу в поданні ними суду своїх доказів і у доведенні перед судом їх переконливості (п. 15 ч. 1 ст. 7 КПК[37]), що проявляється у можливості здійснювати збирання доказів як стороною обвинувачення, так і стороною захисту.

---

[36] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

[37] Там само.

Процес доказування слідчим полягає у збиранні, перевірці та їх оцінці з метою встановлення обставин, що мають значення для кримінального провадження.

Для роботи з цифровими (електронними) слідами слідчий повинен володіти знаннями щодо особливостей механізму їх утворення з урахуванням специфіки вчиненого кримінального правопорушення й уміти[38]:

- виявляти їх, правильно фіксувати інформацію, яку вони несуть;
- визначати та усувати можливі ризики під час роботи з ними (*наприклад*, ймовірність знищення особою, яка їх залишила, або самознищення, кодування цифрової інформації тощо);
- побудувати версію вчиненого кримінального правопорушення у сфері інформаційних технологій або його фрагмент, побудувати загальну модель злочинної діяльності;
- визначити мету злочинної діяльності з використанням інформаційних технологій або шляхом їх руйнування

Виготовлення слідчим, прокурором дубліката документа, а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, має здійснюватися із залученням спеціаліста, що є умовою визнання їх судом як оригіналу документа.

Вказані правила регулюють порядок роботи з електронними доказами на основних етапах їх збирання:

– пошук/отримання/створення;

– копіювання;

– збереження.

[38] Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: моногр. / 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. С. 433.

Збирання доказів є одним з основних етапів розслідування кримінальних правопорушень і має здійснюватися у передбаченому КПК порядку.

З огляду на те, що згідно з ч. 1 ст. 99 КПК матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) віднесені до категорії «документ» як процесуального джерела доказу, а за умови, якщо вони містять ознаки, зазначені у ч. 1 ст. 98 КПК, – до речового доказу, на них поширюються загальні вимоги щодо порядку збирання доказів у кримінальному провадженні.

Так, згідно зі ст. 93 КПК **сторона обвинувачення здійснює збирання доказів шляхом:**

– проведення СРД;

– проведення НСРД;

– витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових і фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок;

– проведення інших процесуальних дій, передбачених КПК (ч. 2 ст. 93 КПК).

Окрім цього, ст. 107 КПК передбачено можливість фіксування процесуальної дії за допомогою технічних засобів під час досудового розслідування.

Згідно з ч. 1 ст. 107 КПК рішення про фіксацію процесуальної дії за допомогою технічних засобів під час досудового розслідування приймає особа, яка проводить відповідну процесуальну дію. За клопотанням учасників процесуальної дії застосування технічних засобів фіксування є обов'язковим. Виконання ухвали слідчого судді, суду про проведення обшуку в обов'язковому порядку фіксується за допомогою звуко- та відеозаписувальних технічних засобів.

Незастосування технічних засобів фіксування кримінального провадження у випадках, якщо воно є обов'язковим, тягне за собою недійсність відповідної процесуальної дії та отриманих внаслідок її проведення результатів, за винятком випадків, якщо сторони не заперечують проти визнання такої дії та результатів її здійснення чинними.

Згідно з п. 3 ч. 2 ст. 105 КПК аудіо-, відеозаписи, отримані під час проведення процесуальних дій, є додатками до протоколу слідчих (розшукових) дій і мають бути належним чином виготовлені, упаковані з метою надійного збереження, а також засвідчені підписами слід-

чого, прокурора, спеціаліста, інших осіб, які брали участь у виготовленні та/або вилученні таких додатків. Відповідно до ч. 3 ст. 107 КПК у матеріалах кримінального провадження зберігаються оригінальні примірники технічних носіїв інформації зафіксованої процесуальної дії, резервні копії яких зберігаються окремо[39].

Окрім того, інформація в електронній (цифровій) формі, яка може бути доказом у кримінальному провадженні, може міститися у матеріалах, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, які зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам ст. 99 КПК, є документом та може використовуватися у кримінальному провадженні як доказ.

Отже, резюмуємо.

Допустимість електронного доказу

визначається відповідністю порядку його отримання положенням КПК (ст. 86 КПК)

Умови допустимості доказів

- ***одержання фактичних даних із належного джерела***
- ***одержання фактичних даних від належного суб'єкта***
- ***одержання фактичних даних у належному процесуальному порядку (з дотриманням передбаченої законом процедури)***
- ***належне оформлення джерела фактичних даних***

[39] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

Умовно електронні докази вчинення кримінального правопорушення можна поділити на такі дві групи:

1. Електронні докази, створення яких перебуває у прямому причинно-наслідковому зв'язку з діями підозрюваної особи.

У разі вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку електронні (цифрові) сліди вчинення кримінального правопорушення можуть бути залишені підозрюваною особою під час несанкціонованого втручання у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; створення вебсайтів, що копіюють зовнішній вигляд справжніх сайтів банківських установ; створення телеграм-ботів, ведення переписки з потенційною жертвою з використанням різних месенджерів тощо.

2. Електронні докази, створення яких не залежало від незаконних дій підозрюваної особи, але на них зафіксована інформація, яка може бути використана у кримінальному провадженні як доказ.

Такими доказами можуть бути відеозаписи із камер відеоспостереження, на яких зафіксовані обставини вчинення злочину, інформація, яка відображає геолокацію об'єкта та його пересування тощо.

Описану градацію слідчий може використати під час обрання способу збирання та визначення мети фіксації електронних доказів у матеріалах кримінального провадження.

Приклад. Якщо електронний доказ утворився у зв'язку з конкретними діями підозрюваної особи, то слідчий має встановити і зафіксувати процес, спосіб його створення, визначити електронний пристрій, за допомогою якого це було вчинено, та встановити усіх осіб, причетних до протиправних дій.

Якщо слідчий досліджує електронний доказ, до створення якого непричетна підозрювана особа, але на ньому зафіксовано її протиправні дії, то методи, цілі, способи збирання і дослідження такої інформації будуть різнитися від попередньої ситуації. У такому випадку слідчий буде досліджувати зафіксовану інформацію, яка буде підтверджувати чи спростовувати якісь факти у сукупності з іншими доказами щодо вчиненого кримінального правопорушення, а також спосіб її походження.

Такими носіями інформації можуть бути:

– подані потерпілим, підозрюваним, свідком, іншими учасниками кримінального провадження. Це можуть бути фото, відеозаписи,

скріншоти фото, окремих кадрів відеозаписів, фрагменти контенту вебсайтів, сторінок у соціальних мережах тощо;

– отриманні слідчим у результаті проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій;

– отримані слідчим у результаті фіксування процесуальної дії за допомогою технічних засобів фіксації кримінального провадження відповідно до вимог ст. 107 КПК;

– ті, які надійшли з матеріалами, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, які зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність» тощо.

Оцінювання інформації в електронній (цифровій) формі, яку слідчому необхідно буде зібрати, дає можливість визначити методику роботи з нею. З точки зору невідкладності, визначаючи спосіб і які докази слід отримати першочергово, треба керуватися наявною інформацією про ймовірність приховування, знищення, зміну інформації в електронній (цифровій) формі, яка містить фактичні дані, що мають значення для кримінального провадження і підлягають доказуванню.

2.2. Застосування заходів забезпечення кримінального провадження як способів збирання електронних доказів

Тимчасовий доступ до речей і документів

Досить часто інформація в електронній (цифровій) формі, яка міститься в електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, відомості про банківські рахунки клієнтів, інформація про операції, проведені на користь чи за дорученням клієнта банку тощо, має важливе значення на початковому етапі розслідування для встановлення підозрюваної особи у вчиненні кримінального правопорушення, встановлення обставин вчинення кримінального правопорушення тощо. Також для ефективного проведення НСРД, *наприклад* для установлення місцезнаходження радіообладнання (радіоелектронного засобу) відповідно до ст. 268 КПК попередньо треба отримати відомості про ідентифікаційні ознаки радіообладнання (радіоелектронного засобу) тощо. Згідно із законодавством України така інформація в електронній

(цифровій) формі може містити охоронювану законом таємницю. *Відповідно до ст. 162 КПК до такої інформації належать*:

– інформація, що перебуває у володінні засобу масової інформації або журналіста і надана ним за умови нерозголошення авторства або джерела інформації;

– відомості, які можуть становити лікарську таємницю;

– відомості, які можуть становити таємницю вчинення нотаріальних дій;

– конфіденційна інформація, зокрема така, що містить комерційну таємницю;

– відомості, які можуть становити банківську таємницю;

– особисте листування особи та інші записи особистого характеру;

– інформація, яка перебуває в операторів та провайдерів телекомунікацій, інформація про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо;

– персональні дані особи, що перебувають у її особистому володінні або в базі персональних даних, яка перебуває у володільця персональних даних;

– державна таємниця;

– таємниця фінансового моніторингу;

– відомості, що становлять професійну таємницю відповідно до Закону України «Про ринки капіталу та організовані товарні ринки».

Одним зі способів отримання такої інформації є застосування слідчим передбаченого п. 5 ч. 2 ст. 131 КПК заходу забезпечення кримінального провадження – **тимчасовий доступ до речей і документів**.

Під *річчю* слід розуміти предмет матеріального світу, щодо якого можуть виникати цивільні права та обов'язки.

Документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, що можуть бути використані як доказ факту чи обставини (матеріали фото-, відеозйомки, звукозапису тощо).

Для прикладу, залежно від виду кримінального правопорушення та електронних (цифрових) слідів, які міг залишити підозрюваний, документами, до яких може виникнути необхідність отримати тимчасовий доступ, можуть бути ті, які містять вичерпну структуровану інформацію:

– щодо банківських рахунків платіжної (кредитної) картки, а також щодо банківських рахунків та платіжних (кредитних) карток осіб;

– щодо здійснення розрахунково-касових операцій за рахунками (про переказ та отримання коштів з рахунку), грошовими чеками, платіжними дорученнями із зазначенням адреси відділення банку, терміналу або банкомата, його номера, часу вчинення банківської операції;

– фото- та відеоінформацію щодо особи, яка у відділеннях банку, через термінали, банкомати здійснювала переказ або отримувала грошові кошти з рахунків і банківської платіжної (кредитної) картки;

– щодо відновлення та/чи заміни SIM-карти (Subscriber Identification Mobile – ідентифікаційний модуль абонента) мобільного номера телефону;

– про зв'язок абонентів, надання телекомунікаційних послуг, у тому числі отримання послуги, вхідних та вихідних дзвінків, текстових повідомлень (у тому числі нульових з'єднань), їх тривалість, із зазначенням IMEI (International Mobile Equipment Identifier – міжнародний ідентифікатор мобільного обладнання) терміналів, номерів телефонів і ретрансляційних антен, у зоні покриття яких виходили на зв'язок абоненти, географічне місцезнаходження базових станцій (місто, вулиця, будинок), маршрути передавання на носії інформації тощо.

Тимчасовий доступ до речей і документів **(ч. 1 ст. 159 КПК) полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи,** ***можливості здійснити з ними одну із таких дій:***

- ***ознайомитися з ними;***
- ***зробити їх копії;***
- ***вилучити їх (здійснити їх виїмку).***

Тимчасовий доступ як захід забезпечення кримінального провадження **не застосовується до інформації з відкритих джерел мережі «Інтернет».**

Під час застосування слідчими тимчасового доступу до речей і документів можуть виникнути такі слідчі ситуації.

Перша слідча ситуація. *Тимчасовий доступ до документів здійснюється в особи, яка не заперечує щодо надання тимчасового доступу до документів.*

Така слідча ситуація характеризується насамперед тим, що у зацікавленої особи, у володінні якої перебувають речі чи документи, відсутня протидія розслідуванню. *Наприклад*, подібною ситуація може бути тоді, коли слідчому потрібний доступ до документів, інформаційний вміст яких (фактичні дані) має значення для кримінального провадження і які містять охоронювану законом таємницю та інші документи. Це можуть бути документи, що зберігаються у операторів телекомунікаційного зв'язку та містять інформацію про трафік абонента, або документи, які зберігаються у банківських установах: документи, що містять інформацію щодо здійснення розрахунково-касових операцій за рахунками (про переказ та отримання коштів з рахунку); інформація про термінал або банкомат, його номер, час вчинення банківської операції, суми виданих коштів; фото- та відеоінформацію щодо особи, яка у відділеннях банку, через термінали, банкомати здійснювала переказ або отримувала грошові кошти з рахунків та банківської платіжної (кредитної) картки тощо.

Зазвичай у клопотанні про тимчасовий доступ до речей і документів зазначається необхідність надання доступу до оригіналів документів, а у разі їх відсутності належним чином завірених копій документів, а також зобов'язання виготовити на паперових та електронних носіях документи, що містять вичерпну структуровану потрібну інформацію для встановлення фактичних даних у кримінальному провадженні.

Сприятливою перша ситуація може бути й тоді, коли документи, до яких треба отримати доступ, перебувають у володінні особи, яка є потерпілим чи свідком у кримінальному провадженні, й не заперечують щодо надання необхідних для встановлення обставин кримінального правопорушення документів.

Є випадки, коли інформація, яка містить фактичні дані про обставини вчинення кримінального правопорушення, розміщена у хмарних сервісах зберігання інформації, й одним із способів отримати слідчому доступ до такої інформації є отримання тимчасового доступу до електронних ін-

формаційних систем компанії, що надає послуги хмарного зберігання інформації. У цьому випадку «зазначена процесуальна дія може бути ускладненою через те, що не всі компанії, які надають послуги хмарного зберігання інформації, мають представництва на території України, а звернення до їх іноземних представництв у порядку запиту про міжнародну правову допомогу (ст. 551 КПК) може призвести до затягування строків досудового розслідування. Оскільки відповідно до п. 7 ч. 1 ст. 164 КПК строк дії ухвали слідчого судді про тимчасовий доступ до речей і документів не може перевищувати одного місяця із дня постановлення ухвали, звернення до іноземних представництв компаній у порядку міжнародного співробітництва з такою постановою є практично неможливим[40]. Така слідча ситуація є проблемною й вимагає від слідчого вжити додаткові заходи щодо пошуку, збирання і дослідження потрібної інформації про фактичні дані у кримінальному провадженні у межах міжнародного співробітництва.

Щоб отримані під час застосування цього заходу забезпечення кримінального провадження документи були визнані допустимими доказами у суді, слідчий має дотримуватися визначеного нормами КПК порядку звернення до слідчого судді (під час досудового розслідування) чи до суду (під час судового провадження) із клопотанням про тимчасовий доступ до речей і документів, а також порядку здійснення тимчасового доступу.

Друга слідча ситуація. *Коли відсутні підстави вважати, що особа, у якої планується здійснювати тимчасовий доступ до документів, може відмовлятися від їх видачі та від виготовлення копій, але під час здійснення цього заходу забезпечення кримінального провадження виникли підстави вважати, що потрібні документи не будуть видані.*

Така слідча ситуація характеризується тим, що особа, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, відмовляється надати тимчасовий доступ до зазначених в ухвалі речей і документів слідчому, посилаючись на те, що вони містять охоронювану законом таємницю, на необхідність узгодження видачі документів із керівництвом тощо.

У такому випадку рекомендуємо слідчому:

– встановити психологічний контакт з цією особою;

– детально роз’яснити зміст ухвали слідчого судді про тимчасовий доступ до зазначених у ній документів;

[40] Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров’я журналіста. *Вісн. Нац. акад. правових наук України.* № 1 (88). 2017. С. 188–189.

– посилаючись на положення Кримінального кодексу України (КК) та КПК переконати цю особу у важливості та необхідності ознайомлення зі змістом документів;

– вжити інші заходи.

Зазвичай налагодження психологічного контакту з володільцем документів сприяє тому, що він видає потрібні для кримінального провадження документи слідчому.

Якщо ж після вжитих заходів особа й надалі відмовляється від виконання ухвали слідчого судді/суду про тимчасовий доступ до речей і документів, слідчий має звернутися до слідчого судді/суду із клопотанням про дозвіл на проведення обшуку згідно з положеннями КПК з метою відшукання та вилучення зазначених в ухвалі слідчого судді документів й на підставі винесеної ухвали провести обшук з метою відшукання потрібних документів.

Така ситуація є несприятливою, оскільки за час звернення слідчого до слідчого судді із клопотанням про проведення обшуку після того, як особа не надала тимчасового доступу до документів, існує реальна загроза зміни або знищення зазначених в ухвалі слідчого судді документів особою, у володінні якої вони перебувають.

Третя слідча ситуація. Нормами КПК передбачено, що у випадках, коли сторона кримінального провадження, яка звернулася із клопотанням, доведе наявність достатніх підстав вважати, що існує реальна загроза зміни або знищення речей чи документів, клопотання може бути розглянуто слідчим суддею, судом без виклику особи, у володінні якої вони перебувають (ч. 2 ст. 163 КПК). Утім, якщо слідчому завчасно відомо, що існує така загроза, то *ситуація в подальшому може призвести до відмови* особи, яка зазначена в ухвалі як володілець речей і документів, виконувати таку ухвалу слідчого судді. У разі невиконання ухвали про тимчасовий доступ до речей і документів слідчому доведеться звертатися до слідчого судді, суду із клопотанням про дозвіл на проведення обшуку.

Така ситуація є несприятливою, оскільки за час звернення слідчого до слідчого судді із клопотанням про проведення обшуку існує реальна загроза зміни або знищення зазначених в ухвалі слідчого судді документів особою, у володінні якої вони перебувають, що може призвести до втрати доказів. *Тому, якщо у слідчого є достатньо підстав вважати, що існує реальна загроза зміни або знищення речей чи документів, йому доцільно відразу звертатися до слідчого судді із клопотанням про проведення обшуку.*

Резюмуємо.

1. З огляду на описані вище слідчі ситуації застосування тимчасового доступу має сенс у тих випадках, коли слідчий впевнений, що особа-володілець добровільно надасть доступ до речей і документів й відсутні підстави вважати, що вони будуть змінені, знищені чи приховані.

2. Якщо у слідчого виникають сумніви щодо добровільного надання особою-володільцем тимчасового доступу до речей і документів, доцільно відразу звертатися до слідчого судді/суду із клопотанням про проведення обшуку.

3. **Перш ніж звернутися до слідчого судді/суду із клопотанням про тимчасовий доступ до речей та документів слідчий має*:***

● ***з'ясувати:***

– хто володілець речей чи документів, до яких треба отримати тимчасовий доступ;

– місце зберігання речей чи документів, до яких треба отримати тимчасовий доступ;

– чи є ймовірність зміни чи знищення документів їх володільцем;

– можливість виготовлення копій документів (за потреби) з використанням копіювальної техніки володільця документів (згідно з ч. 4 ст. 165 КПК за згодою володільця копії документів, які вилучаються або оригінали яких вилучаються, можна виготовляти з використанням його копіювальної техніки та електронних засобів) або вжити заходи щодо забезпечення наявності технічних засобів для їх виготовлення;

● ***врахувати, що:***

– доступ до речей і документів, що містять відомості, які становлять державну таємницю, не може надаватися особі, що не має до неї допуску відповідно до вимог закону (абз. 2 ч. 6 ст. 163 КПК);

– речами і документами, до яких заборонено доступ, є листування чи інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги, а також об'єкти, які додані до такого листування або інших форм обміну інформацією (ст. 161 КПК);

– забороняється вилучення (виїмка) матеріальних носіїв інформації, пов'язаних із веденням Центральним депозитарієм цінних паперів та депозитарними установами системи депозитарного обліку цінних паперів, облікової системи часток товариств з обмеженою відповідальністю та товариств із додатковою відповідальністю (далі – облікова система часток) і внесенням змін до них (ст. 159 КПК);

– згідно із ч. 4 ст. 99 КПК копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, лише за умови виготовлення їх слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Також ч. 2 ст. 71 КПК передбачає, що під час досудового розслідування спеціаліст може бути залучений для надання безпосередньої технічної допомоги сторонами кримінального провадження. Отже, у визначених випадках слід вживати заходи щодо забезпечення участі спеціаліста для виготовлення копій документів.

4. **Алгоритм дій слідчого з отримання тимчасового доступу до речей і документів.**

Згідно зі ст. 159–166 КПК типовим алгоритмом дій слідчого з отримання тимчасового доступу до речей і документів є:

• ***підготовка клопотання про тимчасовий доступ, у якому згідно з ч. 2 ст. 160 КПК зазначають:***

1) короткий виклад обставин кримінального правопорушення, у зв'язку з яким подається клопотання;

2) правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність;

3) речі й документи, тимчасовий доступ до яких планується отримати;

4) підстави вважати, що речі й документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;

5) значення речей і документів для встановлення обставин у кримінальному провадженні;

6) можливість використання як доказів відомостей, що містяться в речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів, у випадку подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю;

7) обґрунтування необхідності вилучення речей та оригіналів або копій документів, якщо відповідне питання порушується стороною кримінального провадження.

• ***звернення із зазначеним клопотанням до прокурора для його погодження;***

• ***звернення до слідчого судді із погодженим прокурором клопотанням про тимчасовий доступ до речей і документів під час досудового розслідування чи суду під час судового провадження;***

Важливо довести/обґрунтувати у клопотанні наявність достатніх підстав вважати, що ці речі або документи:

1) перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;

2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні;

3) не становлять собою або не включають речей і документів, *які містять охоронювану законом таємницю*;

4) у випадку, якщо тимчасовий доступ треба отримати до *документів, які містять охоронювану законом таємницю, слідчому, крім обставин, зазначених у ч. 5 ст. 163 КПК, треба довести можливість використання як доказів відомостей, що містяться у цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів (абз. 1 ч. 6 ст. 163 КПК)*;

• ***участь у розгляді клопотання про надання тимчасового доступу до речей і документів;***

• ***отримання ухвали слідчого судді/суду про тимчасовий доступ до речей і документів;***

Важливо! Ухвала слідчого судді, суду про тимчасовий доступ до речей і документів набирає законної сили із дня її постановлення, строк її дії не може перевищувати одного місяця (п. 7 абз. 1 ч. 1 ст. 164 КПК) і є обов'язковою для виконанням усіма зазначеними в ній особами.

• ***виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів, що відповідно до абз. 2 ч. 1 ст. 159 КПК та ст. 165 КПК здійснюється у такій послідовності:***

1) зазначений в ухвалі слідчого судді, суду слідчий пред'являє особі, яка зазначена в ухвалі як володілець речей і документів, оригінал ухвали про тимчасовий доступ до речей і документів та вручає її копію;

2) особа, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана надати тимчасовий доступ до зазначених в ухвалі речей і документів слідчому, який зазначений у відповідній ухвалі слідчого судді, суду;

3) слідчий, який зазначений у відповідній ухвалі слідчого судді, суду вилучає зазначені в ухвалі про тимчасовий доступ до речей і документів речі та документи й залишає володільцю речей та оригіналів або копій документів опис речей і оригіналів або копій документів, які були вилучені на виконання ухвали слідчого судді, суду.

Тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення (абз. 2 ч. 1 ст. 159 КПК);

4) слідчий, який пред'являє ухвалу про тимчасовий доступ до речей і оригіналів або копій документів, зобов'язаний залишити володільцю речей і оригіналів або копій документів опис речей і оригіналів або копій документів, які були вилучені на виконання ухвали слідчого судді, суду;

5) на вимогу володільця слідчий, який пред'являє ухвалу про тимчасовий доступ до речей і документів, має залишити копію вилучених оригіналів документів.

Копії документів, які вилучаються або оригінали яких вилучаються, виготовляються з використанням копіювальної техніки, електронних засобів володільця (за його згодою) або копіювальної техніки, електронних засобів особи, яка пред'являє ухвалу про тимчасовий доступ до речей і документів.

Важливо! Нормами КПК, якими врегульовано порядок здійснення тимчасового доступу до речей і документів, не передбачено можливість слідчого:

1) самостійно шукати ці речі й документи;

2) оглядати приміщення, де вони можуть зберігатися;

3) відчиняти сейфи, тумби, шафи, в яких можуть зберігатися ці документи;

4) оглядати вміст комп'ютерної техніки;

5) здійснювати будь-які інші пошукові дії.

• ***складання протоколу тимчасового доступу до речей і документів;***

• ***у разі невиконання ухвали про тимчасовий доступ до речей і документів звернутися до слідчого судді, суду із клопотанням про дозвіл проведення обшуку згідно з положеннями КПК.***

Тимчасове вилучення майна

Під **тимчасовим вилученням майна** слід розуміти фактичне позбавлення підозрюваного або осіб, у володінні яких перебуває зазначене у ч. 2 ст. 167 КПК майно, можливості володіти, користуватися та розпоряджатися певним майном до вирішення питання про арешт майна чи його повернення, або його спеціальну конфіскацію в порядку, встановленому законом (ч. 1 ст. 167 КПК). Тимчасово вилученим може бути майно у вигляді речей, документів.

Підстави, порядок тимчасового вилучення майна, а також припинення тимчасового вилучення майна, визначено у гл. 16 КПК.

Тимчасове вилучення речей, документів можуть здійснювати слідчий, прокурор, інша уповноважена службова особа під час затримання підозрюваної особи або під час проведення СРД обшуку, огляду.

Зважаючи на зміст ст. 167 і 168 КПК під час прийняття рішення щодо вилучення *матеріальних носіїв інформації в електронній (цифровій) формі слідчий має врахувати, що вилученню підлягають лише ті речі, документи, щодо яких є достатні підстави вважати, що вони:*

– підшукані, виготовлені, пристосовані чи використані як засоби чи знаряддя вчинення кримінального правопорушення та/або зберегли на собі його сліди;

– призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення;

– є предметом кримінального правопорушення;

– отримані унаслідок вчинення кримінального правопорушення та/або є доходами від них.

Забороняється вилучення (виїмка) матеріальних носіїв інформації, пов'язаних із веденням Центральним депозитарієм цінних паперів та депозитарними установами системи депозитарного обліку цінних паперів, облікової системи часток і внесенням змін до них.

Отже, резюмуємо: **тимчасовий доступ до речей і документів, а також тимчасове їх вилучення**, – це заходи забезпечення кримінального провадження, за результатами здійснення яких слідчий, дізнавач отримує об'єкти, документи, які в подальшому підлягають огляду або експертному дослідженню. Саме за результатами огляду або експертизи слідчий, дізнавач може виявити й закріпити фактичні дані та відомості про їх джерела для отримання доказів або для перевірки цих доказів.

2.3. Процесуальний порядок і тактика проведення окремих слідчих (розшукових) дій як способи збирання електронних доказів

Процесуальний порядок і тактика проведення СРД-огляду

Одним зі способів виявлення та фіксації електронних (цифрових) слідів вчинення кримінального правопорушення є проведення СРД-огляду. У більшості кримінальних проваджень ця СРД проводиться невідкладно після надходження заяви, повідомлення про кримінальне правопорушення.

Матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема комп'ютерні дані) можуть бути виявлені під час огляду місця події, яким може бути місцевість, житло чи інше володіння особи, службове приміщення тощо. Окрім цього, з метою виявлення і фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор може проводити огляд

речей, документів і комп'ютерних даних (ч. 1, 2, 5, 7 ст. 237 КПК)[41]. Під час проведення огляду матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (зокрема комп'ютерних даних) слід керуватися вимогами ст. 99, 214, 223, 237 КПК з урахуванням особливостей самих носіїв інформації в електронній (цифровій) формі.

Залежно від обставин вчинення кримінального правопорушення, виду цифрових (електронних) слідів, які треба виявити і зафіксувати, огляду можуть піддаватися комп'ютери/комп'ютерні системи, ноутбуки, мобільні пристрої* тощо. Для огляду кожного носія інформації слід враховувати певні особливості, що визначають тактику його проведення, зазвичай їх огляд проводять під час огляду місця події.

Для ефективного проведення СРД-огляду місця події, яке пов'язане із вчиненням кримінального правопорушення з використанням комп'ютерних технологій, треба вжити такі підготовчі заходи.

До проведення СРД-огляду:

***1. З'ясувати такі дані*:**

– інформацію про комп'ютерні системи або їх частини та інші потрібні відомості про носії інформації, які можуть міститися на місці події й бути об'єктом огляду;

– хто відповідає за комп'ютерну систему та/або мережу;

– відомості про вид інформації в електронній (цифровій) формі (дані), яка підлягає огляду, її об'єм.

2. Вжити заходи щодо підготовки й забезпечення наявності потрібного інструментарію та обладнання для збирання електронних (цифрових) доказів, а саме:

– носії інформації, на які безпосередньо копіюватимуться дані (жорсткі диски (вінчестери); змінні носії (CD-DVD-диски) тощо) (переконатися, що на них немає ніякої інформації);

– інструменти для демонтажу обладнання (викрутки (плоскі й фігурні), кусачки, плоскогубці, пінцет тощо);

---

[41] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

* Під *мобільними пристроями* слід розуміти портативні переносні пристрої (наприклад, планшети, смартфони тощо), які мають вбудовану систему, здатність обробляти інформацію, вбудовану пам'ять, і деякі із них призначенні для здійснення телефонних розмов, обміну текстовими і мультимедійними повідомленнями тощо. Зазвичай більшість із них оснащені різними типами безпровідних технологій (Wi-Fi, Bluetooth, GPS).

– інструменти для документування процесу (фото- та відеокамера; бирки для нумерування доказів);

– матеріали для упаковки та транспортування вилучених об'єктів;

– інші потрібні засоби і матеріали[42].

3. Вжити заходи щодо залучення відповідного спеціаліста. Не кожний слідчий має спеціальні знання у сфері сучасних інформаційно-комунікаційних технологій у достатній мірі, щоб успішно організувати розслідування. У зв'язку із цим бажана допомога відповідного фахівця, який є достатньо підготовленим у цій сфері, оскільки навіть незначна некваліфікована дія з доказами в електронній формі може спричинити незворотну втрату цінної інформації[43]. Окрім цього, така вимога передбачена ч. 4 ст. 99 КПК, згідно з якою дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом, як оригінал документу.

Перед початком огляду треба:

- поінформувати спеціаліста про те:

– яке кримінальне правопорушення вчинено;

– наскільки досвідчений підозрюваний (за наявності такої інформації);

– чи можна прив'язати цифрові сліди вчиненого кримінального правопорушення до підозрюваного;

– з якими носіями інформації він буде працювати;

– про вид інформації в електронній (цифровій) формі, яка є об'єктом огляду;

- ознайомити спеціаліста з матеріалами кримінального провадження, в яких міститься інформація про електронні докази, з вилученою документацією і її копіями;

- обговорити, які докази можуть бути виявлені та вилучені, можливе місце їх розміщення;

---

[42] Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рек. / М. В. Гуцалюк та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. С. 13.

[43] Там само … . С. 12.

- скласти та обговорити зі спеціалістом план проведення огляду (як безпечно для збереження комп'ютерної інформації увійти до приміщення, правильно взаємодіяти під час проведення СРД тощо).

Спеціаліст, зі свого боку, відповідно до поставлених перед ним завдань та інформації про комп'ютерну систему, може надати слідчому рекомендації щодо особливостей проведення слідчої дії[44].

Безпосередньо на робочому етапі проведення слідчої дії спеціаліст надає допомогу слідчому:

– у виявленні засобів комп'ютерної техніки, її окремих компонентів, документації, інших об'єктів, які можуть містити сліди неправомірних дій;

– у коректному (з точки зору збереження слідів злочину) відключенні засобів комп'ютерної техніки від енергопостачання;

– в описі засобів комп'ютерної техніки, її окремих компонентів і документації, що вилучаються;

– під час вирішення питання визначення складу комплекту комп'ютерної техніки або окремих її компонентів, що підлягають вилученню або ізолюванню від вільного доступу;

– у підготовці засобів комп'ютерної техніки до транспортування (їх упаковці, опечатуванні)[45].

Залучений спеціаліст повинен мати при собі спеціальне програмно-технічне забезпечення та знімні носії інформації, що дозволить зробити безпечне копіювання вмісту оперативної пам'яті з метою її наступного дослідження уже в лабораторії.

4. За потреби залучити спеціаліста-криміналіста для надання технічної допомоги з відео, фотофіксації перебігу проведення СРД-огляду тощо (ч. 2 ст. 79 КПК).

За його допомогою вжити заходи щодо виявлення і фіксації на місці події (на зовнішніх поверхнях комп'ютера, периферійних пристроях і магнітних носіях) наявних слідів пальців рук, мікрочастинок тощо.

Важливо! Застосування найпоширеніших на практиці механічних методів виявлення слідів може призвести до потрапляння порошку у вентилятор, дисковод, роз'єми, на робочу поверхню дисків і порушити роботу ЕОМ або знищити інформацію, тому для виявлення

[44] Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів: посібник / МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2010. С. 54–55.

[45] Там само. С. 55.

слідів пальців рук, мікрочастинок доцільно використовувати сучасні немеханічні методи й дуже обережно працювати з порошками[46].

Окрім цього, під час проведення СРД-огляду спеціаліст-криміналіст:

– за дорученням слідчого може проводити вимірювання, фотографування, звуко- чи відеозапис, виготовляти відбитки та зліпки наявних слідів, за потреби складати плани і схеми, виготовляти графічні зображення оглянутого місця події чи окремих речей;

– під час фіксації слідчим виявленої слідової інформації у протоколі огляду місця події надавати допомогу щодо опису специфічних ознак (вид та кількість виявлених слідів, їх локалізація, способи виявлення та фіксації);

– за дорученням слідчого виготовляти фототаблицю огляду місця події, стенограму, аудіо-, відеозапис процесуальної дії, схеми, зліпки, здійснювати упакування носіїв комп'ютерної інформації та інших об'єктів і матеріалів, які долучаються як додатки до протоколу огляду місця події[47].

Прибувши на місце події для проведення СРД-огляду, треба:

1. Вжити заходи щодо збереження всієї обстановки на місці події:

– вивести усіх сторонніх осіб із зони доступу до комп'ютерної техніки;

– забезпечити неможливість втручання будь-яким способом сторонніх осіб у роботу комп'ютерної техніки (системи);

– якщо комп'ютерів декілька, здійснити їх нумерацію із периферійними приладами відповідно до їх розміщення на місці події[48; 49]. Позначити усі порти та обидва кінці підключених кабелів кольором або номером. Про що зазначити у протоколі огляду.

---

[46] Там само. С. 58–59.

[47] Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, яка затверджена наказом Міністерства внутрішніх справ України від 07 лип. 2017 р. № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text (дата звернення: 09.03.2024).

[48] Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології* та *захист інформації*: зб. наук. пр. Запоріжжя, 1998. 70–79 с.

[49] Icove D., Seger K., Von Sorsh W. Computer Crime: A Crime fighter's Handbook / O'Reylli &Associates, Ins., 1995. 437 p.

2. Враховуючи нестабільність даних, щоб запобігти їх зміні/ знищенню з'ясувати такі питання:

• Чи увімкнений/вимкнений пристрій?

• Чи підключений пристрій до мережі/Wi-Fi?

• Чи підключені до пристрою запам'ятовувальні пристрої?

3. Якщо пристрій вимкнено, залишити його у такому стані. Це обумовлено тим, що на ньому може бути встановлено систему захисту на вході до нього (наприклад, пароль) і його включення може викликати знищення інформації, що міститься на жорсткому диску. Завантаження такого комп'ютера має здійснювати спеціаліст, тому його не вмикають, а розбирають для транспортування й транспортують для проведення дослідження (детально описано у пп. 6–7).

4. Якщо пристрій увімкнено, треба залишити його у такому стані. Це обумовлено тим, що іноді лише в оперативній пам'яті працюючого комп'ютера може міститись дуже важлива інформація – облікові дані, ключі шифрування, паролі доступу до хмарних сховищ, будь-яка інша інформація, яка під час вимикання комп'ютера може бути видалена. Треба провести огляд (виїмку) комп'ютерних даних у режимі реального часу. Насамперед треба не дати можливості його заблокувати або вимкнути чи зашифрувати. В увімкнених пристроях є дуже нестійкі «енергозалежні дані», і якщо їх не зберегти правильно та швидко, вони можуть бути втрачені[50].

Слід дотримуватися таких рекомендацій:

– не вводьте текст, не клацайте мишею та не досліджуйте файли, якщо не маєте відповідних знань, чи без попередньої консультації зі спеціалістом;

– з'ясуйте інформацію про можливі паролі та/або шифрування системи;

– почніть огляд комп'ютерної техніки, інформації/даних, що мають значення для кримінального провадження, зі спеціалістом;

– подивіться на екран і з'ясуйте, чи є будь-які запущені програми, які вказують на доступ до облікових записів в Інтернеті, відкриті файли чи дані, які мають доказове значення;

– з'ясуйте й зафіксуйте детальну інформацію про кожний пристрій (тип пристрою, марку, номер моделі, серійний номер, обсяг

[50] Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рек. / М. В. Гуцалюк та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. С. 13.

пам’яті, стан пристрою, місцезнаходження пристрою, паролі або PIN-коди), які могли бути отримані;

– з використанням спеціальної програми з’ясуйте апаратне і програмне забезпечення комп’ютера;

– здійсніть огляд комп’ютерних даних, відобразивши у протоколі огляду інформацію, 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) (ч. 1–2 ст. 237 КПК)[51];

– за потреби під час здійснення огляду запустіть програму запису зображення екрана монітора, *що можна здійснити скориставшись програмними засобами мережі «Інтернет»*;

Назва програми	**Стислий зміст**
Wave.video	Цей вебвідеореєстратор дозволяє легко записувати відео у режимі онлайн за допомогою будь-якого браузера з будь-якого місця. Жодних завантажень або установок непотрібно.
https://wave.video/ua/live-streaming/online-video-recorder	
CamStudio	Безкоштовна комп’ютерна програма для запису того, що відбувається на екрані комп’ютера у файл AVI або SWF (флеш) разом зі звуком.
http://camstudio.org/	

– якщо бачите на екрані інформацію, яку треба зберегти, проконсультуйтесь зі спеціалістом як це зробити/скопіюйте за допомогою спеціаліста;

– зробіть скріншоти оглянутих документів, а також скопіюйте файли/дані, які мають значення для кримінального провадження,

[51] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

та збережіть їх на носій, призначений для запису і збереження доказової інформації[52];

– окрім основних комп'ютерних даних, криміналістично значущу інформацію можуть містити й *метадані* (від давньогрец. μετά – після, за межами й англ. data – дані) – додаткову інформацію, 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[53].

Метадані зазвичай потрібно досліджувати за допомогою програми для їх вилучення та інтерпретації. Залежно від того, який переглядач метаданих використовують, результати можуть дещо різнитися[54].

В операційних системах Microsoft Windows метадані файлу можна відобразити на екрані за кліком по ньому правою кнопкою 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[55].

Для верифікації найбільш цінними є інструменти, які вбудовують метадані, що криптографічно хешуються у момент збирання, а не на більш пізній стадії.

Хеш-значення – це унікальна форма цифрової ідентифікації (буквено-цифровий рядок), яка за допомогою криптографії підтверджує, що зібраний контент не був змінений з моменту обчислення хешу. Хеш-значення можуть бути присвоєні об'єкту, щоб допомогти встано-

---

[52] Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рек. / М. В. Гуцалюк та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. С. 13.

[53] Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 207. DOI: 10.21564/2414-990X.161.278117

[54] Оцінювання цифрових зображень з відкритих джерел: Посібник для суддів та дослідників фактів (2024), опублікований онлайн на сайті URL: https://www.trueproject.co.uk/osguide, 2024. С. 16.

[55] Криміналістика: криміналістична техніка … . С. 115.

вити, що він не піддавався фальсифікації з моменту застосування хешу до моменту його передачі до суду або іншого органу, який встановлює факти. Якщо цифрове зображення хоч трохи змінити, це призведе до абсолютно нового хеш-значення[56];

– сфотографуйте екран.

Після закінчення огляду:

– вимкніть комп'ютер, витягніть вилку із задньої панелі комп'ютера/вийміть акумулятор із ноутбука;

– забезпечте належне упакування і транспортування.

5. Зафіксуйте порядок проведення СРД-огляду.

Фіксуванню у протоколі огляді підлягають:

– обстановка місця події;

– весь порядок дій та перебіг СРД;

– порядок з'єднання між собою складових комп'ютерної системи (місця з'єднань), із зазначенням особливостей (колір, серійні номери комп'ютерного обладнання, кількість з'єднувальних роз'ємів, їх специфікація), з'єднувальні проводи й кабелі[57];

– ланцюжок зберігання даних, що мають значення для кримінального провадження, місцезнаходження та інші важливі деталі щодо вилучених предметів.

Також здійснюють фото-, відеофіксацію проведення СРД-огляду, огляду комп'ютерного обладнання та даних.

У протоколі зазначають зауваження, клопотання чи доповнення учасників (за наявності).

6. Розберіть і запакуйте систему перед транспортуванням.

Під час проведення огляду дозволяється вилучати лише речі та документи, які мають значення для кримінального провадження, та речі, вилучені з обігу. Усі вилучені речі та документи підлягають негайному огляду й опечатуванню із завіренням підписами осіб, які брали участь у проведенні огляду. Якщо огляд речей і документів на місці здійснити неможливо або їх огляд пов'язаний з ускладненнями, їх тимчасово опечатують і зберігають у такому вигляді доти, поки не буде здійснено їх остаточні огляд і опечатування (ч. 5 ст. 237 КПК).

---

[56] Оцінювання цифрових зображень з відкритих джерел … . С. 18–19.

[57] Лісовий В. В. Огляд місця події при розслідуванні «комп'ютерних» злочинів. *Право України*. 2001. № 1. С. 53.

Перед розбиранням:

– сфотографуйте систему з усіх ракурсів;

– від'єднайте та закріпіть кабелі;

– перевірте носійні порти (USB) та лотки для CD/DVD на наявність знімних носіїв.

Перед вилученням, упакуванням та перевезенням потрібно дати засобу комп'ютерної техніки охолонути.

Під час розбирання, упакування та вилучення:

– співпрацюйте із спеціалістом;

– для транспортування комп'ютер/комп'ютерні системи треба розібрати з урахуванням того, наскільки це полегшить транспортування;

– кабелі, шнури, клавіатури, миші, невеликі периферійні пристрої доцільно упакувати разом;

– щоб уникнути пошкоджень, носії інформації, такі як USB-накопичувачі, DVD-диски, компакт-диски тощо треба упакувати окремо[58].

Вилученню підлягають усі оглянуті елементи комп'ютерних технологій: системний блок, монітор, клавіатура і маніпулятор «миша», усі сполучні шнури (включаючи кабель живлення), джерела живлення, модеми, зовнішні носії комп'ютерної інформації та інші зовнішні пристрої. До зовнішніх носіїв, зокрема, належать: дискети, магнітні стрічки, компакт-диски, жорсткі диски, не підключені до комп'ютера, флеш-карти тощо[59].

Довідково. Під час огляду слід врахувати, що будь-які інші носії інформації, що містяться на місці проведення слідчих дій, можуть містити сліди злочину або криміналістично значущу інформацію. Такими носіями можуть бути електронні органайзери, мобільні телефони, пейджери, звичайні телефони, автовідповідачі, факси, диктофони, цифрові камери. Оцінивши зв'язок цих предметів зі справою, що може випливати з результатів досліджень, огляду їх спеціалістом чи інших обставин, що стали відомі на певний момент, вони мають бути відділені від джерел живлення, помічені, сфотографовані та зафіксовані у протоколі. Після того, як усі названі предмети оглянуті, сфотографовані, зафіксовані у протоколі, їх треба упакувати й опечатати. Для транспортування системного блока використовують спеціальні упаковки. Портативні комп'ютери, дискети, зовнішні жорсткі диски, носії

[58] SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020).

[59] Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів: посібник / МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2010. С. 59.

інформації вміщують в окремі опечатані пакети чи коробки. Для транспортування носіїв інформації треба застосовувати упаковки, які не несуть заряду статичної електрики. Магнітні носії упаковують і транспортують у спеціальних екранованих контейнерах або у стандартних дискетних чи алюмінієвих футлярах заводського виготовлення, які виключають руйнівний вплив електромагнітних і магнітних полів, направлених випромінювань. Опечатують тільки контейнери або футляри[60].

Упакування.

Систему і периферійні пристрої для транспортування упаковують за допомогою сумок для транспортування (сумок для ноутбуків, якщо є), коробок або сумок для доказів, паперових пакетів, оригінальних упаковок, картонних коробок.

Вилучені пристрої ізолюють від вологи, температурного впливу та електростатичних (магнітних) полів.

Важливо! Поліетиленові пакети є неналежним упакуванням.

Зібрані інші сліди кримінального правопорушення, такі як відбитки пальців, біологічні зразки тощо, також упаковують належним чином і оформлюють як додатки до протоколу огляду.

Довідково. На місці події виявлення, фіксацію, вилучення і пакування матеріальних об'єктів, які несуть на собі слідову інформацію вчиненого кримінального правопорушення, здійснює спеціаліст-криміналіст, який відповідає за якісну фіксацію всієї слідової інформації, повноту відображених про це даних у протоколі огляду та схемі (плані) до нього[61].

Упаковки з вилученими носіями інформації опечатують й оформлюють як додатки, про що зазначають у протоколі.

Зі змістом протоколу ознайомлюють усіх учасників, демонструють їм текст протоколу огляду, за потреби відтворюють збережені файли з доказовою інформацією, після чого надають протокол учасникам на засвідчення підписами.

7. Транспортування.

Під час транспортування комп'ютерного обладнання слід поводитися з ним обережно, оскільки інформація на жорсткому диску

---

[60] Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів: посібник / МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2010. С. 60.

[61] Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, яка затверджена наказом Міністерства внутрішніх справ України від 07 лип. 2017 р. № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text

може бути пошкоджена під час транспортування. Для транспортування великих комп'ютерних систем слід підготувати транспорт і спеціальні упаковки.

Після транспортування треба вжити заходи щодо належного збереження комп'ютерного обладнання, усіх вилучених об'єктів, що містять на собі слідову інформацію про вчинене кримінальне правопорушення/якнайшвидше доставити до експертної установи для проведення експертного дослідження.

Важливо! Під час проведення слідчих дій щодо комп'ютерної інформації або самих комп'ютерів (серверів, робочих станцій, ноутбуків) ніколи й за жодних умов не працювати на вилученому комп'ютері. *Це правило встановлює,* що вилучений комп'ютер насамперед є об'єктом дослідження для спеціалістів, речовим доказом.

Особливості огляду мобільних пристроїв

Стрімкі зміни в технологіях сприяють появі нових моделей мобільних пристроїв, робота з якими потребує спеціальних знань і покрокових інструкцій щодо порядку і методів збирання електронних доказів із цих пристроїв. Базові рекомендації щодо методів роботи з мобільними пристроями під час збирання електронних доказів наведено у SWGDE[62], згідно з якими **слідчий під час прийняття рішення щодо збирання електронних доказів з мобільних пристроїв має врахувати такі фактори:**

- ***Компетентність.*** Збирання, аналізування та перевірку даних з мобільних пристроїв має здійснювати слідчий, який спеціалізується на розслідуванні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) й має знання та навики щодо:

– застосування механізмів блокування/розблокування мобільного пристрою (наприклад, «розпізнавання контакту з тілом», «надійні місця», «кнопки блокування пристрою», «довірені пристрої» тощо);

[62] SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020).

– пошуку «резервної копії» інформації, збереженої на комп'ютері, синхронізованих пристроях, таких як смарт-годинники, планшети, у хмарних сховищах тощо;

– відключення мобільних пристроїв від їх мереж;

– збереження і підтримання цілісності даних тощо.

Описані дії може також виконувати слідчий із залученням відповідного спеціаліста у сфері інформаційних технологій. Неналежне поводження з мобільним пристроєм під час зберігання і збирання електронних доказів може призвести до втрати його цифрових даних.

- ***Динамічний характер даних.*** Дані на активних (увімкнених) мобільних пристроях постійно змінюється.
- ***Шифрування.*** Дані можуть зберігатися у зашифрованому стані, що є перешкодою доступу до них або їх аналізу.
- ***Виробники можуть використовувати запатентовані методи для зберігання даних*** (наприклад, закриті операційні системи, приватні з'єднання даних тощо).
- ***Втрата живлення.*** Багато мобільних пристроїв можуть втратити дані або застосувати додаткові заходи безпеки після вимикання.
- ***Паролі.*** Механізми автентифікації можуть обмежувати доступ до пристрою та його даних. Традиційні методи злому паролів можуть призвести до недоступності або знищення даних.
- ***Пошкодження.*** Сторонні предмети на мобільному пристрої або всередині нього, інші пошкодження мобільного пристрою можуть викликати ускладнення під час збирання електронних доказів. Треба вжити відповідних заходів безпеки для захисту мобільного пристрою від пошкоджень, перевірки його цілісності.
- ***Хмарні послуги для мобільних пристроїв.*** Провайдери хмарних послуг розширили можливості мобільних пристроїв кількома способами. Одне із доповнень дозволяє мобільному пристрою зберігати й отримувати доступ до даних поза межами внутрішньої пам'яті пристрою. Крім того, хмарні сервіси надають можливість доступу користувачів до однієї й тієї самої частини даних на кількох платформах або пристроях, що підвищує ризик їх зміни/знищення.
- ***Стандартні експертно-криміналістичні процеси.*** Виявлена й зафіксована слідова інформація (відбитки пальців рук, мікрочастинки тощо) може знадобитися у процесі встановлення зв'язку між мобільним пристроєм і його власником або користувачем. Фіксацію слідової

інформації на мобільних пристроях треба здійснити до початку збирання електронних доказів[63].

Для збереження даних на мобільних пристроях під час підготовки до їх огляду, вилучення і транспортування слід керуватися такими правилами[64]:

- заблокувати вхідні й вихідні сигнали. Для цього можна використовувати радіочастотні блокувальні контейнери (наприклад, сумку Faraday*);
- щоб запобігти знищенню даних, якомога швидше мобільний пристрій має бути ізольований від усіх мереж (наприклад, оператора, Wi-Fi, Bluetooth). Це пов'язано з тим, що:

– є методи локального і віддаленого знищення даних на мобільному пристрої;

– мобільна операційна система може мати автоматизовані процеси, які знищують дані під час увімкнення тощо;

- знайти й підготовити потрібні драйвери, які можуть бути включені до криміналістичного інструменту або завантажені з вебсайту.

Довідково. У разі використання сумки Faraday слід врахувати, що контейнери, які блокують радіочастотний сигнал, можуть розрядити батарею, що може спричинити зміну даних. Якщо треба, щоб пристрій залишався увімкненим, перед тим, як покласти у сумку Faraday, його підключіть до зовнішнього джерела живлення, наприклад портативної батареї. Можна покласти мобільний пристрій разом із зарядним пристроєм в сумку Faraday. Якщо джерело заряджання не вміститься в сумці Faraday, кабель може виконувати роль антени, унаслідок чого пристрій може підключитися до мережі[65].

Алгоритм дій під час збирання і збереження електронних доказів із мобільних пристроїв[66]

1. Підготовка:

– наявність законної підстави для збору електронних доказів;

---

[63] SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020).

[64] Там само.

[*] *Сумка Faraday* – це сумка, яка спеціально призначена для захисту електронних пристроїв від радіочастотного сигналу.

[65] SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020).

[66] Там само.

– визначення потрібного обладнання для використання на місці події.

2. *Фіксація огляду мобільного пристрою*:

– письмовий опис огляду мобільного пристрою, відео-, фотофіксація об'єкта, що оглядається;

– опис стану мобільного пристрою (наприклад, увімкнено/вимкнено, наявність пароля тощо), технічні характеристики кожного пристрою (наприклад, ідентифікаційна інформація, така як марка, модель, серійний номер, будь-які ідентифікаційні знаки, а також з'єднання, пошкодження тощо).

3. *Фіксація ланцюга зберігання інформації в електронній (цифровій) формі, яка включає*:

– опис або унікальний ідентифікатор доказів, а також дату, час її отримання та передачі;

– ПІБ, посада особи, яка зібрала цю інформацію.

4. *Фіксування огляду місця події*:

– точна ідентифікація доказів;

Під час огляду місця події слід детально все оглянути, щоб знайти пов'язані з мобільними пристроями предмети. Сполучені або пов'язані пристрої можуть доповнити інформацію, яка виявлена на мобільному пристрої (наприклад, комп'ютери, розумні годинники, планшети, пристрої Інтернету речей (IoT). Слід звернути увагу на пакувальні матеріали, які можуть містити корисну інформацію про характеристики пристрою, його мережу, пов'язаний обліковий запис, виробника, модель та унікальні ідентифікатори (наприклад, IMEI, MEID, ESN, MAC-адреса), включаючи коди розблокування тощо).

– здійснення фотофіксації у поєднанні з документуванням стану кожного цифрового пристрою.

Фотофіксації підлягають цифрові та периферійні пристрої (наприклад, кабелі, роз'єми живлення, знімні носії та підключені елементи тощо) як невід'ємна частина документації процесу огляду.

Слід уникати торкання і забруднення мобільного пристрою під час його фотографування, а також місця, де його знайдено. Якщо дисплей пристрою перебуває у стані видимості, будь-які зміни слід сфотографувати і задокументувати, доки пристрій не буде вимкнено або увімкнено стан без реакції.

5. *Збереження даних.*

5.1. Алгоритм збереження даних на пристрої з операційною системою iOS*.

- Якщо пристрій увімкнено, він може містити різні дані, зокрема і ключі шифрування, тому його не можна вимикати.
- Щоб запобігти вимкненню пристрою, треба якомога швидше підключити його до джерела живлення з використанням відповідних зарядних приладів.
- Скористатись можливістю подовжити час до автоматичного блокування пристрою, налаштувати функцію автоматичного блокування дисплея.
- Якщо пристрій розблоковано, треба вжити заходи, щоб запобігти його блокуванню, наприклад, вимкнувши функцію блокування або багаторазово взаємодіючи із сенсорним екраном.
- Перевести пристрій у режим «Літак» (провести пальцем по екрану знизу вгору й вибрати режим «Літак») і переконатися, що Wi-Fi та Bluetooth вимкнено. Якщо пристрій неможливо перевести у режим «Літак», є інший варіант, помістити його в сумку Faraday, щоб запобігти потенційній взаємодії з мережею, яка може змінити дані пристрою.
- Якщо пристрій вимкнено, залишити його у такому стані. Зібрати ідентифікаційні дані про пристрій, наприклад номер моделі, носій та унікальні ідентифікатори, які є видимими.

5.2. Алгоритм збереження даних на пристрої з операційною системою Android**.

- Щоб уникнути вимкнення пристрою, треба якомога швидше підключити його до джерела живлення.
- Якщо пристрій розблоковано, треба вжити заходи, щоб запобігти його блокуванню, наприклад вимкнути код блокування (як варіант за можливості налаштувати час очікування екрана дисплея функцією продовження часу до увімкнення автоматичного блокування) або багаторазово взаємодіяти із сенсорним екраном.

---

* *iOS* – це мобільна операційна система, створена та розроблена Apple виключно для своїх мобільних пристроїв, обладнання, включаючи iPhone, iPad та iPod Touch.

** *Android* – це мобільна операційна система на базі Linux, розроблена компанією Google. Android доступний у багатьох різних версіях і, на відміну від iOS, пропонується на пристроях багатьох компаній.

- Перевести пристрій у режим «Літак» (провести пальцем по екрану зверху вниз і вибрати режим «Літак») й переконатися, що Wi-Fi та Bluetooth вимкнено.
- Якщо пристрій не можна перевести у режим «Літак», помістити його у сумку Faraday, щоб запобігти підключенню до мережі. Якщо треба залишити пристрій увімкненим, підключити його до зовнішнього джерела живлення, наприклад портативного акумулятора, який разом із мобільним пристроєм треба помістити всередину сумки Faraday.
- Якщо пристрій вимкнено, залишити його у такому стані, зібрати ідентифікаційні дані про пристрій, наприклад номер моделі, носій та унікальні ідентифікатори, які є видимими. І навпаки, якщо пристрій на момент виявлення був увімкнений, з огляду на те, що він може містити нестабільні дані, зокрема ключі шифрування, вимикати його не можна.

Важливо! Наведені вище алгоритми не є всеохоплюючими для усіх версій iOS та Android. Щоб отримати доступ до даних, які розміщенні на мобільному пристрої, може знадобитися експертиза й, відповідно, вище запропоновані алгоритми з огляду мобільних пристроїв можуть бути змінені.

Окремо слід звернути увагу на **процесуальні особливості огляду матеріалів фото-, відеофіксації, голосових повідомлень тощо, які містяться у пам'яті мобільних пристроїв, або ж на інших носіях інформації, що були виявлені та вилученні під час огляду місця події.**

Однією із слідчих ситуацій може бути така, коли підозрювана особа добровільно дала згоду на проведення огляду особистого мобільного телефону, ноутбука тощо. **У такому випадку слідчий має:**

– прийняти від цієї особи заяву про добровільну видачу мобільного телефону, ноутбука тощо із зазначенням паролю від нього (за наявності);

– увімкнувши пристрій, здійснити пошук та огляд інформації, яка має значення для кримінального провадження (зазвичай огляду піддаються журнал вхідних-вихідних дзвінків, переписки у Telegram, Viber, інших месенджерах за попередньо визначений період часу, контакти мобільних номерів, історія браузерів «Safari», «Google Chrome», фотогалерея, інформація у хмарних сховищах, наприклад Google Drive, Samsung Cloud, iCloud, Xiaomi Cloud тощо).

У протоколі огляду мобільного телефону, окрім визначеної у КПК інформації, зазначають:

– факт добровільного надання мобільного телефону для огляду;
– його модель, колір корпусу;
– номер IMEIL;
– чи вставлена/не вставлена SIM-карта;
– номер SIM-карти;
– пароль для входу (за наявності);
– порядок пошуку та місце виявлення інформації, яка має значення для кримінального провадження;
– яка інформація була скопійована і на які носії;
– після описаної у протоколі інформації за можливості додається скріншот оглянутої сторінки. Також скріншоти можна оформити як додатки до протоколу огляду.

До протоколу додають як додатки носії із скопійованою інформацією і заяву про добровільну видачу мобільного телефону, ноутбука тощо.

Іншою слідчою ситуацією може бути така, коли органом досудового розслідування за підозрою у вчиненні цього злочину затримано підозрювану особу, під час особистого обшуку якої виявлено й вилучено мобільний телефон, який перебуває у вимкненому стані. Оскільки такий мобільний телефон містить відомості, зокрема відеозаписи, фотознімки, листування підозрюваного, що можуть бути використані як докази вчинення ним кримінального правопорушення, а також як доказ причетності інших осіб до вчинення вказаного кримінального правопорушення, цей мобільний телефон має значення речового доказу у кримінальному провадженні. У зв’язку із цим у слідчого виникає необхідність в отриманні дозволу на тимчасовий доступ до змісту мобільного телефону, зокрема до фотогалереї, смс-листування, книги дзвінків, а також до інформації, що міститься у мобільних додатках «Telegram», «Viber», «WhatsUP», «Instagram» тощо з можливістю зняти копії вказаної вище інформації, з метою проведення наступних експертиз або використання вказаної інформації як доказів факту вчинення особою та іншими особами кримінального правопорушення.

У цій ситуації слід врахувати, що огляду підлягає особисте листування підозрюваної особи, що виконане із застосуванням встановлених в операційній системі смартфонів, додатків. Згідно з п. 6 ч. 1 ст. 162 КПК особисте листування особи та інші записи особистого характеру належать до охоронюваної законом таємниці. Копіювання

інформації, що міститься у телефонах та на SIM-карті оператора мобільного зв'язку, слідчий самостійно не може, оскільки абз. 2 ч. 2 ст. 168 КПК дозволяє копіювати інформацію виключно з інформаційних (автоматизованих) систем, телекомунікаційних систем, інформаційно-телекомунікаційних систем, а не з мобільних терміналів, які через їх функціональну приналежність можуть містити охоронювану законом таємницю.

Отже, спочатку треба звернутися до слідчого судді з погодженим із прокурором клопотанням про отримання тимчасового доступу до змісту мобільного телефону та SIM-карти у вигляді особистого листування підозрюваного щодо вчинення ним кримінального правопорушення та у вигляді фотографій, відеозаписів, аудіозаписів, якими зафіксовано подію злочину, й отримати ухвалу слідчого судді про тимчасовий доступ до речей і документів. Тимчасовий доступ до змісту мобільних телефонів і SIM-карт у вигляді особистого листування підозрюваного щодо вчинення ним кримінального правопорушення та у вигляді фотографій, відеозаписів, аудіозаписів, якими зафіксовано подію злочину, чи того майна, яке було предметом злочинного посягання, дозволить органу досудового розслідування виявити й зафіксувати відомості щодо обставин вчинення кримінального правопорушення, встановити коло причетних осіб, виявити місцезнаходження викраденого майна, тобто сприятиме ефективному і повному досудовому розслідуванню у кримінальному провадженні.

Процесуальний порядок і тактика проведення СРД-обшуку

Виявлення комп'ютерної техніки, мобільних пристроїв і носіїв інформації (жорстких дисків, флеш-накопичувачів, зовнішніх накопичувачів інформації тощо), на яких може міститися інформація щодо обставин вчинення кримінального правопорушення, яка може мати доказове значення у кримінальному провадженні, може здійснюватися під час проведення СРД-обшуку.

СРД-обшук проводять на підставі ухвали слідчого судді. Утім, слід зазначити, що у разі надходження заяви, повідомлення про кримінальне правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку з метою виявити сліди вчиненого кримінального правопорушення, а також запобігти витоку інформації про його до-

кументування, досить часто обшук потрібно проводити невідкладно саме на початковому етапі досудового розслідування.

До постановлення ухвали слідчого судді згідно з ч. 3 ст. 233 КПК слідчий, прокурор має право увійти до житла чи іншого володіння особи лише у невідкладних випадках, пов'язаних із врятуванням життя людей і майна чи у процесі безпосереднього переслідування осіб, які підозрюються у вчиненні кримінального правопорушення. У випадку проведення обшуку без ухвали слідчого судді прокурор, слідчий за погодженням із прокурором зобов'язаний невідкладно після проведення обшуку звернутися до слідчого судді із клопотанням про проведення обшуку, який розглядає таке клопотання згідно з вимогами ст. 234 КПК, перевіряючи, крім іншого, чи справді були наявні підстави для проникнення до житла або іншого володіння особи без ухвали слідчого судді.

Підготовчий етап проведення СРД-обшуку передбачає вирішення таких питань:

– з'ясувати інформацію про комп'ютерні системи/їх частини, мобільні термінали систем зв'язку та інші необхідні відомості про носії інформації, які треба відшукати/можуть бути виявлені на місці проведення обшуку;

– визначити тактику проведення цієї слідчої (розшукової) дії залежно від характеру злочинних дій, з огляду на які виникла потреба у її проведенні;

– підібрати потрібні технічні засоби, засоби фото- і відеофіксації тощо;

– отримати якомога більше відомостей про місце, де буде проводитися обшук;

– визначити коло учасників, спеціалістів, які будуть присутні, й тих, які безпосередньо братимуть участь у проведенні обшуку.

Згідно зі ст. 234–236 КПК до типового алгоритму дій слідчого, пов'язаного із проведенням обшуку, слід віднести:

– підготовку клопотання про проведення обшуку із зазначенням відомостей, передбачених ч. 3 ст. 234 КПК. До клопотання також мають бути додані оригінали або копії документів та інших матеріалів, якими прокурор, слідчий обґрунтовує доводи клопотання, а також витяг з Єдиного реєстру досудових рішень (ЄРДР) щодо кримінального провадження, у межах якого подається клопотання. У клопотанні слід зазначити індивідуальні або родові ознаки комп'ютерних систем чи їх частин, мобільних терміналів систем зв'язку тощо, які заплановано

відшукати, а також їх зв’язок із вчиненим кримінальним правопорушенням;

– погодження клопотання про проведення обшуку із прокурором;

– звернення до слідчого судді з погодженим прокурором клопотанням про проведення обшуку, яке розглядає слідчий суддя в суді у день його надходження за участю слідчого або прокурора (з відповідним клопотанням до слідчого судді може звернутися і прокурор);

– проведення обшуку на підставі ухвали, винесеної слідчим суддею в обсязі, необхідному для досягнення його мети, та в порядку, передбаченому ст. 236 КПК. За рішенням слідчого чи прокурора може бути проведено обшук осіб, які перебувають у житлі чи іншому володінні, якщо є достатні підстави вважати, що вони переховують при собі предмети або документи, які мають значення для кримінального провадження. Перебіг і результати особистого обшуку підлягають обов’язковій фіксації у відповідному протоколі.

В абз. 2 та 3 ч. 6 ст. 236 КПК передбачено, що якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп’ютерних систем або їх частин, мобільних терміналів систем зв’язку, для виявлення яких не надано дозволу на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення і фіксацію комп’ютерних даних, що на них містяться, на місці проведення обшуку.

Особи, які володіють інформацією про зміст комп’ютерних даних та особливості функціонування комп’ютерних систем або їх частин, мобільних терміналів систем зв’язку, можуть повідомити про це слідчому, прокурору під час здійснення обшуку, повідомлені дані вносять до протоколу обшуку. Вилучені речі й документи, які не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку та які не належать до предметів, що вилучені законом з обігу, вважають тимчасово вилученим майном;

– фіксацію перебігу і результатів проведення обшуку у протоколі відповідно до вимог ст. 104–107 КПК.

Під час виконання ухвали про дозвіл на обшук житла чи іншого володіння особи слідчий, прокурор під час проведення обшуку має право долати системи логічного захисту, якщо:

– особа, присутня на обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту;

– обшук здійснюється за відсутності осіб, які володіють житлом чи іншим володінням, чи інших осіб у місці проведення обшуку, зазначених у ч. 3 ст. 236 КПК.

Слідчий, прокурор під час проведення обшуку має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення обшуканого житла, іншого володіння особи чи окремих речей, виготовляти відбитки і зліпки, оглядати й вилучати документи, тимчасово вилучати речі, які мають значення для кримінального провадження.

В обов'язковому порядку за допомогою звуко- та відеозаписувальних технічних засобів фіксують виконання ухвали слідчого судді, суду про проведення обшуку житла чи іншого володіння особи. Також право безперешкодного фіксування проведення обшуку за допомогою відеозапису надається стороні захисту (ч. 1 ст. 107 КПК).

Запис, здійснений за допомогою звуко- та відеозаписувальних технічних засобів під час проведення слідчим, прокурором обшуку, є невід'ємним додатком до протоколу. Дії та обставини проведення обшуку, незафіксовані у записі, не можуть бути внесені до протоколу обшуку та використані як доказ у кримінальному провадженні (ч. 2, ст. 104 КПК).

Згідно зі ст. 236 КПК алгоритм доступу слідчого, прокурора до даних, що містяться у комп'ютері, мобільних пристроях під час обшуку, є таким:

1. Пошук комп'ютерних даних. Якщо слідчий суддя не надав дозвіл на відшукання комп'ютерів і мобільних пристроїв, але їх виявлено під час проведення обшуку (слідчий, прокурор виявив доступ чи можливість доступу) і щодо них є достатні підстави вважати, що інформація, яка міститься на них, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них містяться, на місці проведення обшуку (ч. 6 ст. 236 КПК).

2. Повідомлення/встановлення пароля. Особи, присутні під час обшуку, можуть (але не зобов'язані) повідомити слідчому, прокурору «особливості функціонування», зокрема пароль до телефона або комп'ютера. Якщо особа надала такий пароль (або якщо системи логічного захисту немає), проводять пошук, виявлення та фіксацію комп'ютерних даних безпосередньо під час обшуку. Про надання

особою пароля і про повідомлення інформації щодо розміщення даних зазначають у протоколі обшуку.

3. Огляд та фіксація комп'ютерних даних (ч. 7 ст. 236 та абз. 2 ч. 2 ст. 237 КПК).

Якщо володілець надав інформацію про пароль, слідчий, прокурор проводить огляд комп'ютерних даних, відображаючи у протоколі огляду інформацію, 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).

Якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозволу на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення і фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку.

Особи, які володіють інформацією про зміст комп'ютерних даних і про особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчому, прокурору під час здійснення обшуку, і такі відомості вносять до протоколу обшуку.

Якщо особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем чи їх частин, мобільних терміналів систем зв'язку, відмовляються повідомити про це слідчому, прокурору під час здійснення обшуку, у такому випадку після їх вилучення призначають комп'ютерно-технічну експертизу, завданням якої є виявлення інформації та встановлення типу програмного забезпечення, що містяться на комп'ютерних носіях.

Фіксацію комп'ютерних даних здійснюють за допомогою спеціаліста (ч. 2 ст. 168 КПК) шляхом копіювання даних з мобільного телефону або комп'ютера. Такі дані суд визнає як оригінал документа (ч. 4 ст. 99 КПК).

Якщо такі дані неможливо скопіювати під час обшуку і водночас є потреба у призначенні експертизи, через що слідчий, прокурор вважають за потрібне вилучити мобільні пристрої, варто зафіксувати наявність відповідних даних у загальному порядку (у протоколі та на відеозапису).

4. Вилучення мобільних пристроїв, комп'ютерів. Слідчий, прокурор має право вилучити мобільні пристрої, комп'ютери (ч. 2 ст. 168 КПК), зазначивши це у протоколі обшуку:

– якщо вони вказані безпосередньо в ухвалі суду про дозвіл на обшук;

– якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

Тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюють лише у разі, якщо вони безпосередньо зазначені в ухвалі суду.

Забороняється тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження або якщо такі об'єкти отримано у результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

За потреби слідчий чи прокурор виготовляє за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації проводять із залученням спеціаліста.

На вимогу володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з таких комп'ютерних систем або їх частин (за наявності технічної можливості здійснення копіювання) з використанням матеріальних носіїв володільця комп'ютерних систем або їх частин. Копії інформації з комп'ютерних систем або їх частин, які вилучаються, виготовляють з використанням технічних засобів, програмно-технічних засобів, апаратно-програмних комплексів володільця із залученням спеціаліста (абз. 1, 2, 3, 4, 5 ч. 2 ст. 168 КПК).

Копіювання інформації з обмеженим доступом здійснюють так, щоб це не суперечило встановленому законодавством порядку обігу та захисту такої інформації.

5. Накладення арешту. Арешт на комп'ютерні системи чи їх частини накладають лише у випадках, якщо вони отримані унаслідок вчинення кримінального правопорушення чи є засобом чи знаряддям його вчинення або зберегли на собі сліди кримінального правопорушення, або у випадках, передбачених пп. 2, 3, 4 ч. 2 ст. 170 КПК, або якщо їх надання разом з інформацією, що на них міститься, є обов'язковою умовою проведення експертного дослідження, а також якщо доступ до комп'ютерних систем чи їх частин обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту (ч. 3 ст. 170 КПК).

Зняття показань технічних приладів та технічних засобів

Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, полягає в отриманні слідчим, прокурором від особи, яка є власником або володільцем відповідних приладів або засобів, потрібних для з'ясування обставин, що мають значення для кримінального провадження, копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за винятком місць, що належать до приватних помешкань осіб.

Зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюють на підставі постанови слідчого, прокурора та, за потреби, за участю спеціаліста.

Для здійснення зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, особі, яка є власником або володільцем відповідних приладів або засобів, пред'являють постанову слідчого, прокурора.

Постанова слідчого, прокурора про зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, повинна містити:

1) найменування кримінального провадження і його реєстраційний номер;

2) відомості про власника або володільця відповідних приладів або засобів;

3) період часу, за який має бути здійснено зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису чи засобів фото-, кінозйомки, відеозапису.

Зняття показань технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису чи засобів фото-, кінозйомки, відеозапису, здійснюється у присутності слідчого, прокурора шляхом самостійного копіювання особою, яка є власником або володільцем (за її бажанням) відповідних приладів та засобів, або копіювання такою особою за участю спеціаліста відповідних записів на носії, які надає слідчий, прокурор.

Про зняття показань з технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, складають протокол (ст. 245-1 КПК)[67].

Отже, резюмуємо.

1. На початковому етапі розслідування основним завданням слідчого є встановлення усіх джерел доказової інформації та осіб, які вчинили кримінальне правопорушення. Від того, як слідчий вирішить ці завдання, залежить наступний етап розслідування та результати досудового слідства взагалі. На вирішення таких завдань спрямоване правильне застосування заходів забезпечення кримінального провадження, проведення СРД та НСРД. Вибір способу збирання електронних доказів, а також визначення черговості проведення СРД, НСРД, інших процесуальних дій обумовлюється насамперед слідчою ситуацією і тактичним завданням розслідування у конкретному кримінальному провадженні.

2. Огляд комп'ютерних даних проводить 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).

3. Під час проведення СРД-огляду та обшуку особливу увагу треба приділити збору об'єктів, які надалі будуть піддані криміналістичному дослідженню. Найменші некваліфіковані дії з комп'ютерною системою часто закінчуються безповоротною втратою цінної доказо-

[67] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

вої інформації. У зв’язку з цим до збору об’єктів дослідження доцільно залучити спеціаліста.

4. Під час вилучення системних блоків треба коректно завершити їх роботу, повністю знеструмити, відключити, запакувати й опечатати кожний системний блок окремо.

5. Пакування і опечатування слід здійснювати таким чином, щоб унеможливити безпосередній доступ до системного блока та розміщених у ньому носіїв інформації, без можливості пошкодження упаковки та бірок.

6. Крім запобігання безпосередньому доступу до об’єктів дослідження, упаковка повинна забезпечувати їх захист від механічного пошкодження під час транспортування.

7. Для дослідження інформації, що міститься на машинних носіях інформації, експерту надається сам носій, а за потреби й сам системний блок чи комплекс комп’ютерних засобів (до складу якого входить досліджуваний носій).

8. Для встановлення відповідності програмних засобів певним параметрам експерту надається носій із копією досліджуваного програмного засобу або програмного коду.

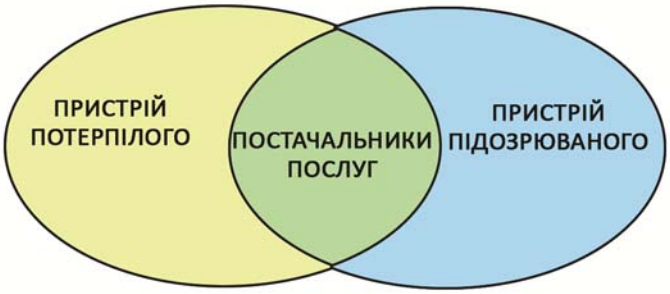
9. Для дослідження робочого стану комп’ютерно-технічних засобів експерту надаються ці комп’ютерно-технічні засоби, а також технічна документація до них.

10. Щоб запобігти зміні/руйнуванню даних дистанційно, треба відключити мобільні пристрої від мережі. Один зі способів ізоляції мобільного пристрою від підключення до мережі – включити на ньому режим «Літак». Ця функція у нових версіях мобільних операційних систем може не вимикати Bluetooth, Wi-Fi або може лише відключати їх тимчасово. Отже, треба перевірити, чи вимкнено підключення до мережі, або розглянути альтернативні способи ізоляції мобільного пристрою від мережі.

11. Збираючи та досліджуючи електронні докази слід врахувати, що дані, пов’язані з мобільним пристроєм, можна знайти на комп’ютері, розумному годиннику, планшеті тощо, які зв’язані із цим мобільним пристроєм через синхронізацію або обмін інформацією через процес резервного копіювання або обліковий запис хмарної служби. Так само дані з комп’ютера чи інших пристроїв, які були синхронізовані, можна знайти на мобільному пристрої.

12. Слід пам’ятати, що зв’язок між пристроєм потерпілого та підозрюваною особою зазвичай забезпечує постачальник послуг, до

якого слідчий має звернутися у визначеному КПК порядку для отримання потрібної інформації.



13. Враховуючи тактику проведення слідчих (розшукових) дій, слід звернути увагу на особливості, що характерні саме для збирання електронних доказів.

Так, якщо технічний носій інформації захищений від будь-якого стороннього доступу до його змісту, то його треба передати експерту для встановлення можливого доступу до інформації на ньому. У разі розміщення електронних доказів на серверах, жорстких дисках підприємств, установ, організацій, рекомендовано здійснити копію цієї інформації, оскільки вилучення майна може призвести до негативних наслідків.

14. Під час пошуку електронних доказів слід мати на увазі, що вони завжди розміщені на окремих фізичних носіях або у мережі «Інтернет», зокрема на спеціальних «хмарних» сервісах зберігання інформації, до яких може бути одночасний доступ різних користувачів, які можуть змінювати, видаляти їх. Отже, важливо вжити всі обов’язкові заходи щодо збереження цієї інформації.

15. На відміну від паперових, електронні документи містять метадані, які у кримінальному процесуальному доказуванні відіграють роль одного із критеріїв належності та допустимості такої електронної форми інформації. Метадані забезпечують інформацію про автора, час створення документа, значення даних у момент отримання (спадковість) даних і про шлях від джерела до поточного місця зберігання. Вони дають можливість ідентифікувати автора, визначити співвідношення інформації у документі до часу, обставин, які мають значення для кримінального провадження, з’ясувати оригінальність даних в електронному документі[68].

[68] Тетерятник Г. К., Виходець Ю. О. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з Інтернет-джерел. *Юрид. наук. електрон. журн*. № 10. 2022. С. 773.

16. Дії з електронними доказами слід проводити лише за допомогою сертифікованого обладнання, оскільки несертифіковане обладнання може призвести до втрати електронних документів, випадкового знищення реквізитів або окремих складових документа.

17. Під час досудового розслідування, якщо це можливо, до збирання електронних доказів треба залучати спеціалістів, які з технічної точки зору допоможуть забезпечити якість збереження електронних доказів[69].

2.4. Проведення окремих негласних слідчих (розшукових) дій як спосіб збирання електронних доказів

Збирання електронних доказів під час досудового розслідування різної категорії кримінальних правопорушень досить часто обумовлює втручання у таємницю спілкування, яке має бути правомірним.

Таємниця спілкування відповідно до пп. 7 та 8 ч. 1 ст. 7 КПК віднесена до переліку загальних засад кримінального провадження, яким має відповідати його зміст і форма. Стаття 14 КПК передбачає, що під час кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених КПК, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети. Інформація, отримана унаслідок втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального провадження[70]. Ці засади кореспондуються зі ст. 31 Конституції України (КУ)[71], згідно з якою кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (ч. 1 ст. 31 КУ).

---

[69] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Сер. Право.* № 4 (58). С. 82–83.

[70] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

[71] Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 01.02.2024).

Згідно зі ст. 258 КПК спілкуванням є передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб.

Втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Згідно з нормами КПК отримати доступ до змісту такого спілкування можна шляхом проведення НСРД, а саме:

1) аудіо-, відеоконтроль особи;

2) арешт, огляд і виїмка кореспонденції;

3) зняття інформації з електронних комунікаційних мереж;

4) зняття інформації з електронних інформаційних систем.

Аудіо-, відеоконтроль особи

Аудіо-, відеоконтроль особи є різновидом втручання у приватне спілкування, яке проводять без її відома на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов'язані з її діяльністю чи місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування (ст. 260 КПК).

Під час проведення аудіо-, відеоконтролю особи застосовують технічні засоби аудіо- чи відеозапису, характерними ознаками яких є невеликі габарити (компактність), хороші звукова чутливість та якість відеозапису, велика ємність пам'яті (як вбудованої, так і додаткової), що обумовлено особливостями тактики проведення цієї негласної слідчої (розшукової) дії та необхідністю використовувати приховану відеозйомку[72].

[72] Брендель О. І. Засоби прихованого відеоспостереження та особливості їх використання в процесі розслідування злочинів і експертного дослідження. *Теорія і практика судової експертизи і криміналістики*. 2016. Вип. 16. С. 240.

Арешт, огляд і виїмка кореспонденції

Згідно зі ст. 261 КПК накладення арешту на кореспонденцію* особи без її відома проводять у виняткових випадках на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб їй може містити відомості про обставини, які мають значення для досудового розслідування, або речі й документи, що мають істотне значення для досудового розслідування.

Накладення арешту на кореспонденцію надає право слідчому здійснювати огляд і виїмку цієї кореспонденції.

Зняття інформації з електронних комунікаційних мереж

Статтею 119 Закону України «Про електронні комунікації» від 16 грудня 2020 р., № 1089-IX передбачено, що постачальники електронних комунікаційних послуг мають забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, отриманих під час укладення договору про надання електронних комунікаційних послуг та надання електронних комунікаційних послуг, у тому числі щодо:

1) персональних даних споживача;

2) факту отримання кінцевим користувачем електронних комунікаційних послуг;

3) змісту інформації, яку передає та/або отримує кінцевий користувач;

4) обсягу, змісту, маршрутів передавання інформації (даних), зокрема даних, що обробляються з метою передавання інформації в електронних комунікаційних мережах або оплати електронних комунікаційних послуг;

5) даних про місцезнаходження, до яких належать будь-які дані, які обробляє постачальник електронних комунікаційних послуг під час надання послуг електронних комунікацій, у тому числі про розташування термінального обладнання;

---

* *Кореспонденцією*, передбаченою статтею 261 КПК, є листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передавання інформації між особами.

6) даних про спроби виклику між певними кінцевими точками електронної комунікаційної мережі, зокрема про невдалі спроби виклику (такі, що були ініційовані та не отримали відповіді) або про перерване з'єднання.

Згідно із зазначеними нормами інформація про електронні комунікаційні послуги, отримані кінцевим користувачем, може надаватися лише за наявності його попередньої згоди, вираженої у письмовій чи будь-якій іншій формі, що дає змогу зробити висновок про факт надання такої згоди або у порядку та відповідно до вимог КУ та законів України.

Згідно зі ст. 121 Закону України «Про електронні комунікації» доступ до інформації про споживача, факти надання електронних комунікаційних послуг, зокрема до даних, які підлягають обробці з метою передачі такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом.

Зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг *забезпечується єдиною системою технічних засобів, яку використовують усі уповноважені законом органи, на умовах автономного доступу до інформації у порядку, визначеному законодавством.*

Постачальник електронних комунікаційних послуг та/або мереж зобов'язаний забезпечити можливість підключення технічних засобів, зазначених у ч. 2 ст. 121 Закону України «Про електронні комунікації», у точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг[73].

Згідно зі ст. 263 КПК зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій і споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, що проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження.

[73] Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 28.06.2024).

Інформацію, яка передається за допомогою електронних комунікаційних мереж, зберігають на спеціальних технічних носіях (серверах) у спеціальному вигляді – log-файлі. Відповідні log-файли можуть бути вилучені в Інтернет-провайдерів[74].

Зняття інформації з електронних інформаційних систем

Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або в її частинах, доступ до електронної інформаційної системи або до її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача можна здійснювати на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її у частині, що має значення для певного досудового розслідування.

Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частин, доступ до яких не обмежується її власником, володільцем чи утримувачем або не пов'язаний з подоланням системи логічного захисту (ст. 264 КПК)[75].

Фіксацію інформації, отриманої з електронних комунікаційних мереж за допомогою технічних засобів та у результаті зняття відомостей з електронних інформаційних систем, здійснюють на відповідному носієві та за допомогою протоколу, у якому зазначають зміст інформації, що передається особами через електронні комунікаційні мережі, з яких здійснюють зняття інформації.

У разі виявлення в інформації відомостей, що мають значення для конкретного досудового розслідування, у протоколі відтворюють відповідну частину такої інформації, після чого прокурор вживає заходи для збереження знятої інформації (ст. 265 КПК).

Встановлення місцезнаходження радіообладнання (радіоелектронного засобу)

Досить часто особи, які вчиняють кримінальні правопорушення у межах протиправної діяльності, використовують засоби мобільного

[74] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Сер. Право.* № 4 (58). С. 83.

[75] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

зв’язку та інші радіовипромінювальні технічні пристрої. Встановивши їх місцезнаходження можна встановити місцеперебування особи, яку підозрюють у вчиненні злочину тощо.

Установлення місцезнаходження радіообладнання (радіоелектронного засобу) є НСРД, що полягає у застосуванні технічних засобів для отримання від мережевої інфраструктури або мобільного кінцевого (термінального) обладнання відомостей про місцезнаходження мобільного кінцевого (термінального) обладнання (точки його підключення до мережі), а в мережі фіксованого зв’язку – даних про фізичну адресу кінцевого пункту мережі, *без розкриття змісту повідомлень, що передаються,* якщо у результаті проведення такої негласної слідчої (розшукової) дії можна встановити обставини, які мають значення для кримінального провадження (ст. 268 КПК).

Під *радіообладнанням* (*радіоелектронним засобом*) слід розуміти «електричний або електронний виріб, призначений для випромінювання та/або приймання радіохвиль з метою радіозв’язку та/або радіовизначення чи укомплектований додатковим пристроєм, призначеним для випромінювання та/або приймання радіохвиль з метою радіозв’язку та/або радіовизначення»[76].

До радіоелектронних засобів належать мобільні термінали систем зв’язку та інші радіовипромінювальні пристрої, активовані у мережах операторів рухомого (мобільного) зв’язку, тобто мобільного телефону, модемів GSM, UMTS, HSDPA, WiMAX, LTE, що забезпечують бездротовий доступ до мережі «Інтернет» та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв’язку тощо[77].

Умовно «усі радіоелектронні засоби, що працюють у мережах стільникового радіозв’язку, можна поділити на такі групи:

1) стільникові радіотелефони, планшети;

2) модеми, роутери, шлюзи тощо;

3) трекери, відслідковувальні пристрої тощо;

---

[76] Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 28.06.2024).

[77] Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал.* № 4. 2014. С. 203. URL: http://www.lsej.org.ua/4_2014/53.pdf

4) датчики сигналізації, системи управління, що працюють у мережах стільникового радіозв'язку тощо»[78].

Таку НСРД доцільно проводити, коли треба:

– отримати дані, що сприятимуть оперативному розшуку особи, підозрюваної або причетної до вчинення кримінального правопорушення, визначення місця знаходження радіообладнання (радіоелектронного засобу), за рахунок установлення місцезнаходження кінцевого обладнання рухомого (мобільного) електрозв'язку, тобто його стільникового радіотелефону;

– встановити місцезнаходження у певний час або проміжок часу до, під час або після вчинення злочину в конкретному місці радіоелектронних засобів та інших радіовипромінювальних, активованих у мережах постачальника електронних комунікаційних послуг (оператора, провайдера) рухомого (мобільного) електрозв'язку, що належать та/або були у користуванні у цей час у осіб, які можуть бути причетними до вчинення кримінального правопорушення, свідків, потерпілого тощо;

– встановити у реальному часі (у режимі онлайн) місцезнаходження радіоелектронних засобів та інших радіовипромінювальних пристроїв, активованих у мережах постачальника електронних комунікаційних послуг (оператора, провайдера) рухомого (мобільного) електрозв'язку, що належать та/або перебувають у користуванні в осіб, які можуть бути причетними до вчинення кримінального правопорушення;

– установити місцезнаходження у визначений проміжок часу радіоелектронних засобів та інших радіовипромінювальних пристроїв, активованих у мережах постачальника електронних комунікаційних послуг (оператора, провайдера) рухомого (мобільного) зв'язку, що належать або використовувались особами, які можуть бути причетними до вчинення кримінального правопорушення, визнані потерпілими

[78] Кобець М. В. Установлення місцезнаходження радіообладнання (радіоелектронного засобу) як метод слідчої (розшукової) дії та оперативно-розшукового заходу з розшуку осіб. *Актуальні питання та перспективи розшукової роботи в діяльності підрозділів кримінальної поліції. Матеріали міжвідомч. наук.-практ. кругл. столу* (Київ, 28 берез. 2024 р.). С. 74–78. URL. https://elar.naiau.kiev.ua/items/4ae4967b-a13d-48b3-89c7-a2472369592b

або свідками, або поточні координати такого радіоелектронного засобу у просторі й часі[79].

***Довідково.** Стільникові телефонні апарати під час виготовлення обладнують спеціальним засобом ідентифікації, яким є унікальний код (індивідуальний номер телефону) – IMEI – міжнародний ідентифікатор мобільного устаткування, який складається з комбінації 15 цифр. Код IMEI виробник відображає у програмному забезпеченні кожного стільникового телефонного апарата, за допомогою якого він в автоматичному режимі передається на технічні засоби оператора зв'язку під час кожного підключення конкретного телефонного апарата в мережу.

Ще одним засобом ідентифікації будь-якого стільникового телефону стандарту GSM є SIM-карта – модуль ідентифікації абонента. SIM-карта призначена для ідентифікації абонента у мережі стільникового зв'язку.

На SIM-карті міститься важлива інформація: ідентифікаційний GSM-номер абонента, пароль блокування клавіатури (PIN-код) та код розблокування (PUK-код), записна книжка. SIM-карта може також зберігати додаткову інформацію: телефонну книжку абонента, списки вхідних/вихідних телефонних номерів, текст смс-повідомлень. Крім того, SIM-карта містить мікросхему пам'яті, яка підтримує цифрування.

Після увімкнення у мобільну мережу номер SIM-карти, так само як і номер IMEI, в автоматичному режимі передається на технічні засоби оператора зв'язку. Номер SIM-карти призначений для ідентифікації в мережі абонента, номер IMEI – телефонного апарата. Оскільки ці номери визначаються у мережі одночасно і перебувають у взаємозв'язку один з одним, то за номером IMEI телефонного апарата можна визначити номер SIM-карти, з яким конкретний телефон використовується[80].

---

[79] Кобець М. В. Установлення місцезнаходження радіообладнання (радіоелектронного засобу) як метод слідчої (розшукової) дії та оперативно-розшукового заходу з розшуку осіб. *Актуальні питання та перспективи розшукової роботи в діяльності підрозділів кримінальної поліції. Матеріали міжвідомч. наук.-практ. кругл. столу* (Київ, 28 берез. 2024 р.). С. 74–78. URL: https://elar.naiau.kiev.ua/items/4ae4967b-a13d-48b3-89c7-a2472369592b

[80] Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал.* № 4. 2014. С. 203. URL: http://www. lsej.org.ua/ 4_2014/53.pdf

НСРД установлення місцезнаходження радіообладнання (радіоелектронного засобу) проводять на підставі ухвали слідчого судді, постановленої у порядку, передбаченому ст. 246, 248–250 КПК

До *постановлення ухвали слідчого судді* НСРД може бути розпочато на підставі постанови слідчого (узгодженої із прокурором), прокурора у випадку, передбаченому ч. 1 ст. 250 КПК:

- у виняткових невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, передбаченого розд. I, II, VI, VII (ст. 201 та 209), розд. IX, XIII, XIV, XV, XVII Особливої частини КК.

Після початку такої НСРД прокурор невідкладно зобов'язаний звернутися з відповідним клопотанням до слідчого судді.

Виконання будь-яких дій із проведення цієї НСРД має бути негайно припинено, якщо слідчий суддя постановить ухвалу про відмову у наданні дозволу на проведення негласної слідчої (розшукової) дії. Отримана унаслідок такої НСРД інформація має бути знищена в порядку, передбаченому ст. 255 КПК.

Не потребує дозволу слідчого судді установлення місцезнаходження радіообладнання (радіоелектронного засобу) за заявою його власника (ч. 5 ст. 268 КПК).

Щоб провести НСРД установлення місцезнаходження радіообладнання (радіоелектронного засобу), слідчий має:

1. Отримати відомості про ідентифікаційні ознаки радіообладнання (радіоелектронного засобу), наприклад номер мобільного телефону, місцезнаходження якого планується встановити.

Таку інформацію можна отримати:

– з показань учасників кримінального провадження;

– за запитом до банківської установи, керуючись п. 6 ст. 23, п. 2 ч. 2 ст. 25 Закону України «Про Національну поліцію», ч. 5 ст. 40, ч. 2 ст. 93 КПК «Про банки і банківську діяльність» (Бланк запиту наведено у дод. 2).

Наприклад, такий запит доцільно подавати, якщо заздалегідь було встановленно ПІБ особи-користувача мобільним телефоном і наявна інформація, що він є клієнтом банку (користувачем банківської картки). За номером банківського рахунку, окрім всіх проведених транзакцій, у тому числі зняття готівки, можна дізнатися номери мобільних телефонів, який підозрюваний використовував для ідентифікації під час здійснення транзакцій, і місце перебування користувача картки (рахунку);

– у результаті здійснення заходу забезпечення кримінального провадження тимчасового доступу документів з метою отримання в оператора мобільного зв'язку документів, що містять таку інформацію.

2. За наявності підстав, передбачених ч. 1 ст. 250 КПК, винести постанову про проведення НСРД й погодити її у прокурора.

Постанова слідчого, прокурора про проведення НСРД має містити:

– найменування кримінального провадження та його реєстраційний номер;

– правову кваліфікацію кримінального правопорушення із зазначенням статті (частини статті) КК;

– відомості про особу (осіб), місце або річ, щодо яких проводитиметься НСРД;

– час початоку, тривалість і мету негласної слідчої (розшукової) дії;

– відомості про особу (осіб), яка буде проводити НСРД;

– обґрунтування прийнятої постанови, у тому числі обґрунтування неможливості отримання відомостей про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб;

– вказівку на вид НСРД, що проводиться.

3. У разі відсутності підстав, передбачених ст. 250 КПК, підготувити клопотання про надання дозволу на проведення НСРД, у якому зазначають:

– найменування кримінального провадження та його реєстраційний номер;

– короткий виклад обставин кримінального правопорушення, у зв'язку з розслідуванням якого подається клопотання;

– правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) КК;

– відомості про особу (осіб), місце або річ, щодо яких треба провести негласну слідчу (розшукову) дію;

– обставини, що дають підстави підозрювати особу у вчиненні кримінального правопорушення;

– вид негласної слідчої (розшукової) дії та обґрунтування строку її проведення;

– обґрунтування неможливості отримання відомостей про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб;

– відомості про ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання тощо;

– обґрунтування можливості отримання під час проведення негласної слідчої (розшукової) дії доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин кримінального правопорушення або встановлення осіб, які його вчинили.

До клопотання слідчого, прокурора додають витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, у межах якого подають клопотання.

4. Звернутися із клопотанням про проведення НСРД установлення місцезнаходження радіообладнання (радіоелектронного засобу) до слідчого судді.

5. Отримати ухвалу слідчого судді про проведення НСРД установлення місцезнаходження радіообладнання (радіоелектронного засобу).

6. Направити до уповноваженого оперативно-технічного підрозділу копії ухвали про проведення НСРД і відповідного завдання, в якому зазначають ідентифікаційні ознаки, за якими можна ідентифікувати абонента спостереження, електронну комунікаційну мережу та кінцеве (термінальне) обладнання.

7. Провести НСРД.

8. Здійснити фіксацію перебігу та результатів НСРД відповідно до вимог ст. 252 КПК.

За результатами проведення НСРД складають протокол, до якого за потреби долучають додатки, зазначають відомості про осіб, які проводили НСРД або були залучені до їх проведення.

9. Протоколи про проведення НСРД із додатками не пізніше ніж через 24 години з моменту припинення зазначених негласних слідчих (розшукових) дій передають прокурору.

Судова практика

З метою удосконалення використання електронних доказів під час доказування у кримінальному провадженні слід брати до уваги судову оцінку щодо допустимості таких доказів, здобутих унаслідок проведення негласних слідчих (розшукових) дій.

Так, відповідно до постанови Верховного Суду від 10 вересня 2019 р. у справі № 761/8589/15-к (провадження № 51-4571км18) суд вважає, що протокол аудіо-, відеоконтролю особи передбачає обов'язкову наявність додатків із аудіо-, відеозаписами. У мотиваційній частині зазначеного суд обґрунтував свою оцінку таким чином: «Положення ч. 1 ст. 270 КПК фактично закріплюють обов'язковість фіксації відомостей за допомогою аудіо-, відеозапису. Однак додатки до протоколу цієї НСРД, а саме, оптичні носії та картка пам'яті, прокурором не було надано суду. Надаючи оцінку такій ситуації суд вважає, що йому не надано жодних доказів, які б підтверджували обвинувачення, пред'явлене особі, у частині розроблення ним злочинного плану для вчинення розбою, наявність попередньої змови з іншими учасниками та розподіл між ними ролей»[81].

Відповідно до постанови Верховного Суду від 03 листопада 2020 р. у справі № 419/2016/19 (провадження № 51-2950км20) суд вважає, що часткова відсутність запису перебігу НСРД не завжди вказує на недопустимість відомостей, отриманих під час її проведення. Утім, потрібно розуміти, що таке бачення суду стосується конкретної ситуації у конкретній справі й може відрізнятись в іншому кримінальному провадженні, враховуючи сукупність доказів у ньому[82].

В окремих випадках невнесення у вступну частину протоколу відомостей щодо характеристики технічних засобів фіксації та носіїв інформації не є підставою для визнання слідчої (розшукової) дії недопустимою. Наприклад,

---

[81] Постанова Верховного Суду від 10.09.2019 р. у справі № 761/8589/15-к (провадження № 51-4571км18). URL: https://reyestr.court.gov.ua/Review/84229858 (дата звернення: 19.04.2024).

[82] Постанова Верховного Суду від 03.11.2020 р. у справі № 419/2016/19 (провадження № 51-2950км20). URL: https://reyestr.court.gov.ua/Review/92765503 (дата звернення: 22.04.2024).

у постанові Верховного Суду від 07 жовтня 2020 р. у справі № 725/1199/19 зазначено: «доводи захисника про те, що протоколи НСРД є недопустимими доказами через те, що додатками до них є неоригінальні примірники технічних носіїв інформації, не спростовують висновків суду про допустимість цих доказів». Також суд вважає, що у разі відсутності у протоколі НСРД інформації щодо назви та серійного номера спецтехніки правоохоронного органу, яка застосовувалась під час процесуальних дій, немає підстав визнавати таку НСРД недопустимою. У цій частині суд мотивує своє рішення тим, що відповідно до пп. 4.5.1, 4.5.6 Зводу відомостей, що становлять державну таємницю, затвердженого наказом голови Служби безпеки України від 12 серпня 2005 р., № 440, державною таємницею є відомості про номенклатуру, фактичну наявність спеціальних технічних засобів чи спеціальної техніки: устаткування, апаратури, приладів, пристроїв, програмного забезпечення, препаратів та інших виробів, призначених (спеціально розроблених, виготовлених, запрограмованих або пристосованих) для негласного отримання інформації, які розкривають найменування, принцип дії чи експлуатаційні характеристики спеціальних технічних засобів чи спеціальної техніки, призначених для здійснення та забезпечення оперативно-розшукової діяльності[83].

Враховуючи наведене, пропонуємо такі рекомендації щодо організації та проведення НСРД з метою збирання електронних доказів у кримінальному провадженні:

1. Фіксація ходу і результатів негласних слідчих (розшукових) дій має відповідати загальним правилам фіксації кримінального провадження, передбаченим КПК.

2. Проведення негласних слідчих (розшукових) дій може фіксуватися за допомогою технічних та інших засобів.

3. За результатами проведення негласної слідчої (розшукової) дії складають протокол, до якого за потреби долучають додатки. Протоколи щодо проведення негласних слідчих (розшукових) дій, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі

[83] Постанова Верховного Суду від 07.10.2020 р. у справі № 725/1199/19 (провадження № 51-5720км19). URL: https://reyestr.court.gov.ua/Review/92173671 (дата звернення: 19.04.2024).

та документи або їх копії можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування.

4. Прокурор вживає заходи щодо збереження отриманих під час проведення негласних слідчих (розшукових) дій речей і документів, які планує використовувати у кримінальному провадженні (ч. 1, 2, 4 ст. 252, ст. 256 КПК).

5. Носії інформації, на яких зафіксовані відомості, отримані у результаті проведення зазначених негласних слідчих (розшукових) дій, треба зберігати у стані, придатному для їх дослідження, до набрання законної сили вироку суду та можуть бути предметом дослідження відповідних спеціалістів або експертів (ст. 266 КПК).

Враховуючи викладене, пропонуємо дотримуватися рекомендацій (наведені на схемі нижче) щодо організації та проведення слідчих і негласних слідчих (розшукових) дій з метою збирання електронних доказів у кримінальному провадженні.

У процесі збирання електронних доказів за допомогою слідчих (розшукових) дій необхідно:

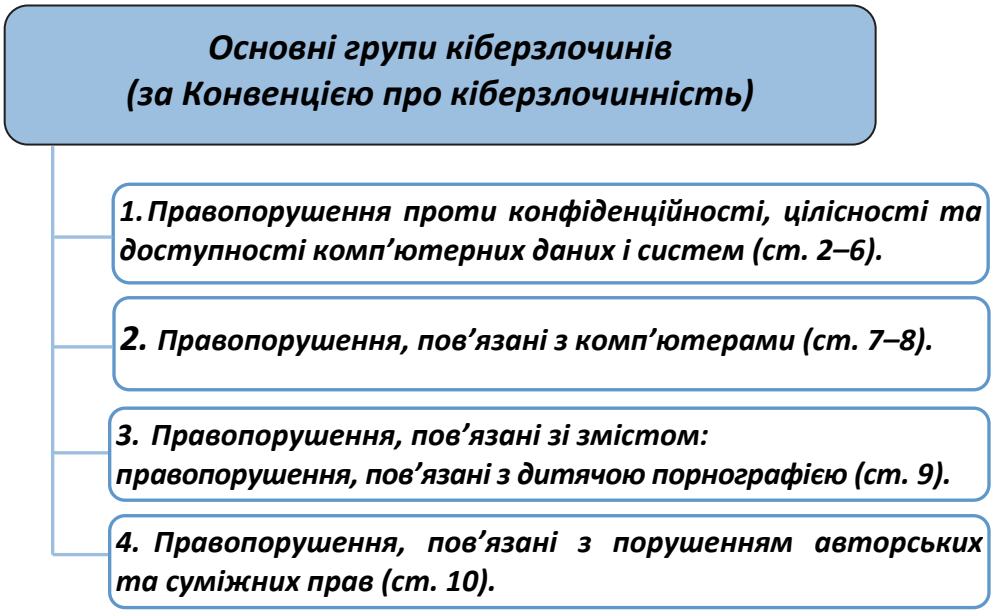
- Вибрати технічні засоби відповідно до потреб та обставин, які продиктовані тактикою проведення слідчої (розшукової) дії.
- У випадках суперечливих питань (прогалин законодавства) звертатись до аналогії права та судової практики, що стосується оцінки судом тих чи інших ситуацій.
- За потреби користуватись допомогою спеціаліста.
- Заздалегідь перевіряти технічні засоби, які заплановано використовувати під час проведення слідчої (розшукової) дії, а саме їх справність, заряд батареї, достатність характеристик для виконання поставлених завдань тощо.
- Вживати заходи щодо збереження доказів, враховуючи особливості їх електронної природи.

РОЗДІЛ 3. ЗБИРАННЯ ТА ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС РОЗСЛІДУВАННЯ ОКРЕМИХ ВИДІВ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

3.1. Особливості збирання електронних доказів щодо вчинення кіберзлочинів

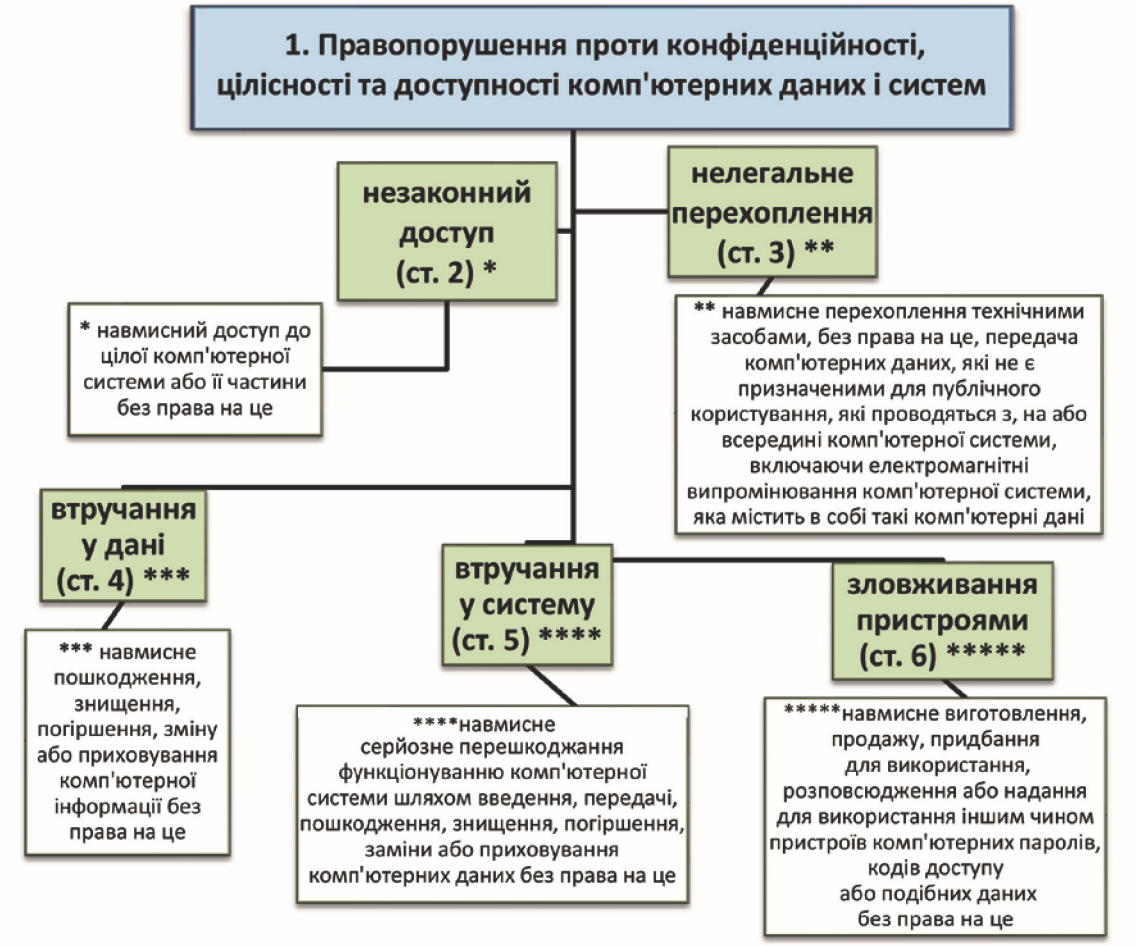
У сучасному світі суспільство стає все більш залежним від роботи автоматизованих комп'ютеризованих систем у різноманітних сферах суспільного життя. Відтак кіберзлочини (комп'ютерні злочини) можуть завдати значних соціальних і економічних збитків. Іноді навіть невеликий збій у функціонуванні автоматизованих комп'ютерних систем, електронних банків даних чи електронних мереж може спричинити реальну загрозу[84].

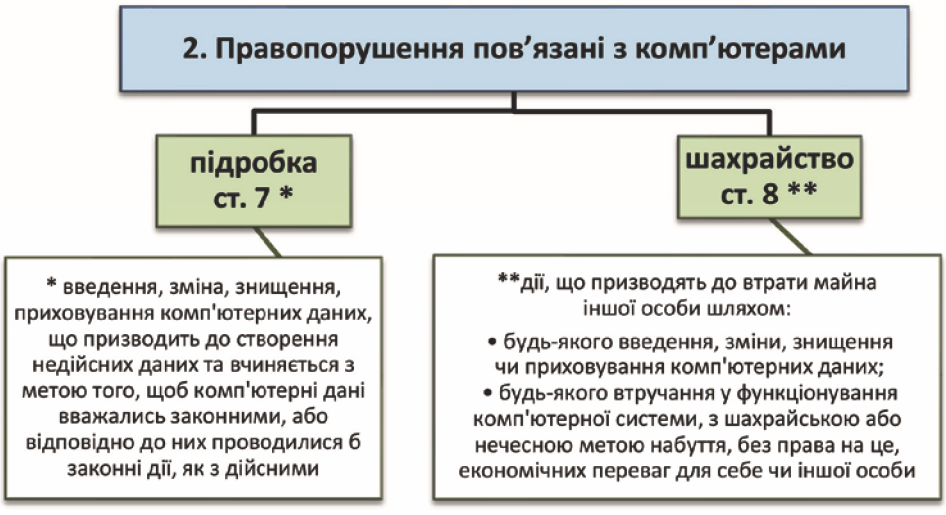
Кіберзлочин (комп'ютерний злочин) – суспільно-небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом про кримінальну відповідальність та/або яке злочином визнано у міжнародних договорах[85].

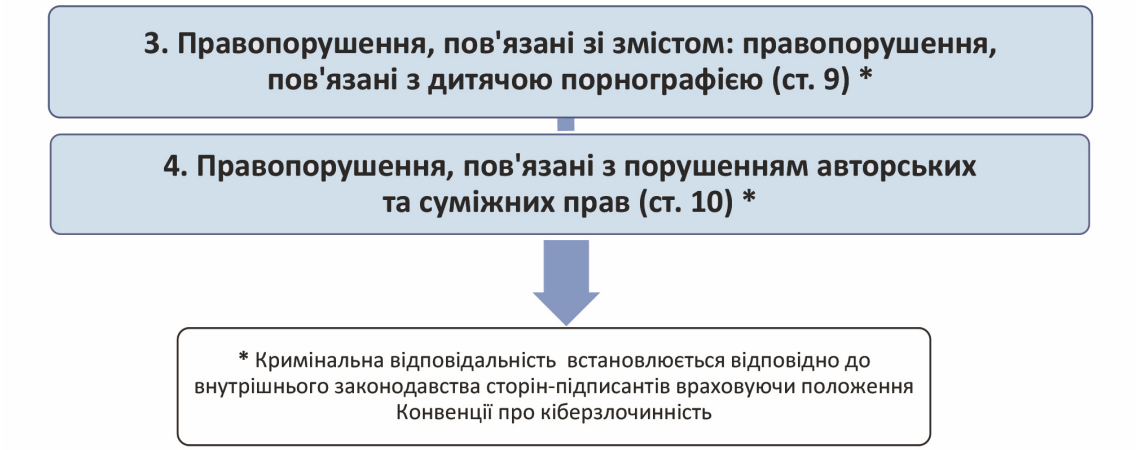


[84] Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження: дис. д-ра філос. 081 / Хмельницьк. ун-т управління та права ім. Леоніда Юзькова, Хмельницький, 2022. С. 120.

[85] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 09.03.2024).


1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
незаконний доступ (ст. 2) *
* навмисний доступ до цілої комп'ютерної системи або її частини без права на це
нелегальне перехоплення (ст. 3) **
** навмисне перехоплення технічними засобами, без права на це, передача комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані
втручання у дані (ст. 4) ***
*** навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це
втручання у систему (ст. 5) ****
****навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це
зловживання пристроями (ст. 6) *****
*****навмисне виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв комп'ютерних паролів, кодів доступу або подібних даних без права на це


2. Правопорушення пов’язані з комп’ютерами
підробка ст. 7 *
* введення, зміна, знищення, приховування комп'ютерних даних, що призводить до створення недійсних даних та вчиняється з метою того, щоб комп'ютерні дані вважались законними, або відповідно до них проводилися б законні дії, як з дійсними
шахрайство ст. 8 **
**дії, що призводять до втрати майна іншої особи шляхом:
• будь-якого введення, зміни, знищення чи приховування комп'ютерних даних;
• будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи



У КК такі діяння отримали назву «кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», у розд. XVI КК до них належать, зокрема, такі:

– несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК);

– створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК);

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового поширення повідомлень електрозв'язку (ст. 363-1 КК).

Згідно з ч. 4 ст. 190 КК одним зі способів вчинення шахрайства є здійснення незаконних операцій з використанням електронно-обчислювальної техніки.

Отже, до кіберзлочинів відносять:

– діяння, об'єктом злочину яких є комп'ютерні дані або системи (їх називають «основними» кіберзлочинами);

– діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину (наприклад, для шахрайства, розкрадання, спричинення шкоди іншим особам та ін.)[86].

Досудове розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюють слідчі, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду.

Особливості організації взаємодії під час досудового розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) врегульовано в Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України у запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, яка затверджена наказом Міністерства внутрішніх справ України № 575 від 07 липня 2017 р.

Матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити:

1) письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм);

2) документи (за наявності), що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби;

3) установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі «Інтернет», IP-адреса, вебадреса, номер абонента мережі електрозв'язку чи

[86] Самойленко О. А. Виявлення та розслідування кіберзлочинів: навч.-метод. посібник. Одеса, 2020. С. 11.

номер телефону, за допомогою яких було здійснено такий доступ, тощо)[87].

Типові ситуації початкового етапу досудового розслідування кіберзлочинів можна класифікувати за такими ознаками.

1. За характером вчиненого діяння:

– встановлені факти перекручення комп'ютерної інформації (зокрема інформації, яка циркулює у кредитно-фінансовій сфері);

– встановлені факти злочинного заволодіння комп'ютерною інформацією;

– встановлені факти злочинного заволодіння комп'ютерною інформацією, під час доступу до якої застосовувався механічний вплив;

– встановлені факти знищення інформації в комп'ютерній системі.

2. За наявністю відомостей про злочин:

– відомості про спосіб доступу до комп'ютерної інформації та про осіб, що вчинили певне діяння, відсутні;

– є відомості про спосіб доступу та про осіб, що вчинили певне діяння.

3. За способом вилучення електронного доказу:

– вилучення інформації з деяких носіїв можливе лише у спеціальних умовах, наприклад, під час проведення експертизи (у такому разі під час проведення відповідної слідчої (розшукової) дії спершу вилучають відповідні матеріальні об'єкти, а згодом – інформацію з них у процесі призначеного експертного дослідження);

– неможливим або процесуально необґрунтованим є вилучення матеріальних об'єктів із місця проведення огляду (обшуку) у кримінальному провадженні.

Результатом аналізу конкретної ситуації є висунення слідчих версій і планування розслідування, тобто визначення першочерговості та послідовності проведення слідчих (розшукових) дій.

У більшості ситуацій під час досудового розслідування кіберзлочинів треба встановити належність певній особі сайту, електронної поштової адреси, з використанням якої було вчинено злочин, ідентифікувати особу правопорушника чи отримати іншу інформацію, яка

[87] Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, яка затверджена наказом Міністерства внутрішніх справ України від 07 лип. 2017 р. № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text (дата звернення: 09.03.2024).

має значення для кримінального провадження, що є можливим з використанням адреси інтернет-протоколу (IP-адреса).

IP-адреса (від англ. *Internet Protocol address*) – унікальний числовий ідентифікатор мережевого рівня, який використовують для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням стека протоколів TCP/IP (наприклад, Інтернет).

Усі дані, що надсилаються через Інтернет, мають містити як IP-адресу, куди дані надходять, так і адресу, звідки вони надходять. Кожний вебсайт також має IP-адресу. Система доменних імен* дозволяє браузерам використовувати доменне ім'я для пошуку IP-адреси та підключення.

Є три типи IP-адрес:

1. Статична. Статично призначені IP-адреси є фіксованими й ніколи не змінюються. Це важливо для пристроїв, яким потрібна узгоджена IP-адреса – наприклад, сервер, на якому розміщено вебсайт, який має підтримувати ту саму IP-адресу, щоб користувачі могли переходити до нього. Статичні IP-адреси також можна використовувати для пристроїв, яким потрібний доступ до конфіденційних систем. Використання пристроїв зі статичними IP-адресами надає ще одну частину інформації, яку система може використовувати для автентифікації того, хто має до неї доступ.

2. Напівстатична. Напівстатично призначені IP-адреси – це адреси, які навряд чи часто змінюватимуться, але не гарантовано, що залишатимуться незмінними.

3. Динамічна. Динамічно призначені IP-адреси – це адреси, які постійно змінюються. Пристрій користувача часто отримує саме динамічну IP-адресу, коли підключається до мережі. Ця IP-адреса зберігається лише для одного сеансу підключення. Коли пристрій відключають і знову підключають до мережі, він отримує іншу IP-адресу. Може бути важко відстежити ці адреси до певного пристрою, але їх часто можна відстежити до локальної мережі, у якій працював пристрій[88].

---

* *Домен* (англ. *Domain*, від лат. *Dominium* – володіння) – частина простору ієрархічних імен мережі "Інтернет", що обслуговується групою серверів системи доменних імен (DNS-серверів) та централізовано адмініструється.

[88] OBTAINING CROSS-BORDER ELECTRONIC EVIDENCE SECTION 1: INVESTIGATIVE TECHNIQUES. This e-Learning course was created as part of INTERPOL's Cyber Capabilities and Capacity Development Project (C3DP), funded by the United States Department of State – Bureau of International Narcotics and Law Enforcement (INL). The e-Learning course was jointly developedwith the National White Collar Crime Center (NW3C). ©2023.

Також, використовуючи IP-адресу пристрою, можна отримати його приблизну геолокацію. Різні компанії надають комерційні послуги геолокації для адміністраторів вебсайтів, які з різних причин хочуть знати, де перебувають їхні користувачі. Таку інформацію можна вважати достовірною лише для тих випадків, коли треба звузити місцезнаходження до країни, регіону тощо, і навіть тоді вона не завжди буде правильною.

На сьогодні відомі різні онлайн-інструменти, які можна використовувати для пошуку потрібної інформації за IP-адресою.

Наприклад, за допомогою протоколу whois* можна отримати попередню інформацію про вебсайт у випадку, якщо ця інформація не була спеціально прихована. Протокол whois надає дані про власників, реєстраторів та інші реєстраційні деталі, що можуть бути корисними для досудового розслідування.

Інформація, що надається сервісом whois, може бути обмеженою або прихованою залежно від налаштувань конфіденційності, вибраних власником домену. Є причини, через які багато реєстраторів не вносять реальні дані про власника домену у whois або замінюють контактну інформацію на власну (проксі-контакт) – це пов'язано з політикою конфіденційності та захисту персональних даних клієнтів. Щоб отримати повну інформацію про реєстрацію домену або IP-адреси, може знадобитися контакт із реєстратором або власником.

Отримати дані протоколу whois можна за допомогою таких сайтів:

- 2ip.ua;
- Who.is;
- www.whois.com;
- whois.domaintools.com;
- www.ukrnames.com/ukr/whois.

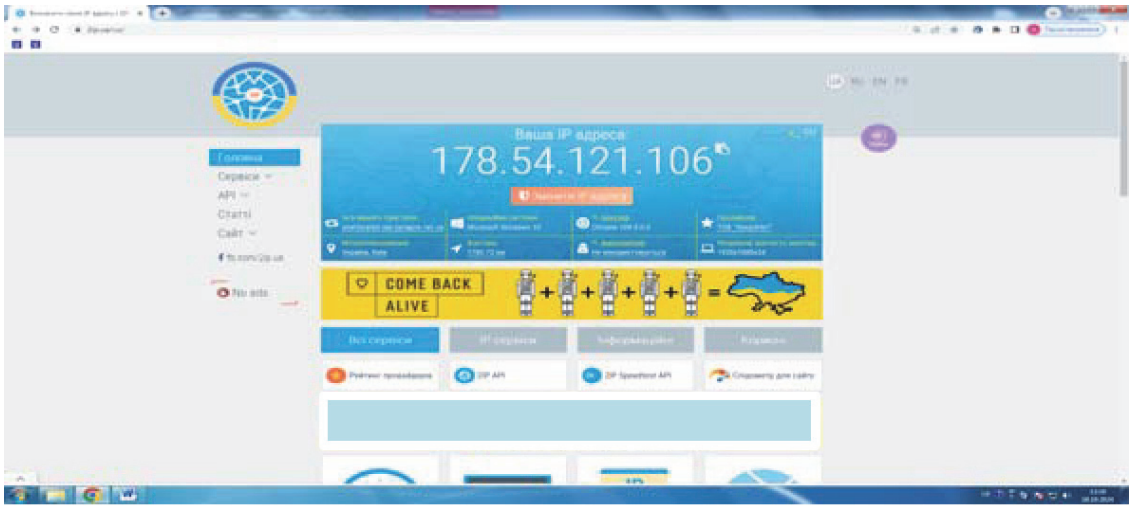
Для прикладу розглянемо більш детально інструменти 2ip та Who.is.

Назва сайту	Зміст сайту	Електронна адреса	QR-код
2ip	• надає інформацію про IP-адресу або домен; • надає інформацію про сайт, його місцезнаходження; • перевіряє наявність IP-адреси у спам-базах; • виконує інші функції	https://2ip.ua/ua/	

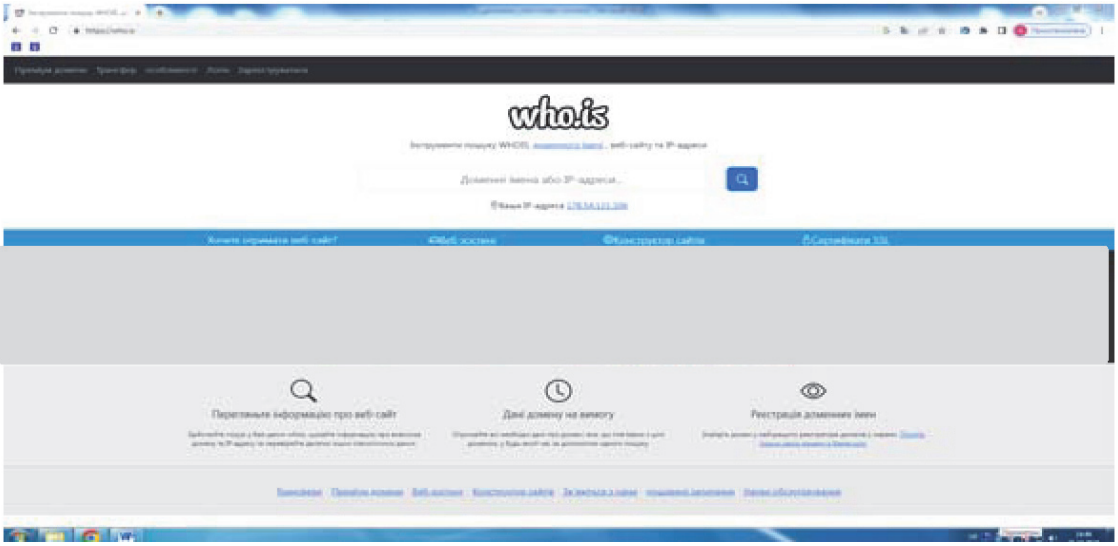
* *Whois* – це протокол, що дає змогу отримувати інформацію про домени та IP-адреси.

Who.is	• шукає інформацію про будь-яке доменне ім'я чи вебсайт; • є ґрунтовною базою даних доменних імен, серверів імен, IP-адрес, а також інструментів для пошуку й моніторингу доменних імен	https://who.is/	

За допомогою сайтів 2ip або Who.is можна знайти інформацію про провайдера, який надав послугу хостингу.



2ip (головна сторінка)



Who.is (головна сторінка)

Щоб встановити належність сайту, звертаються із запитом про такі дані:

– реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостингу для сайту;

– адреси, телефонні номери та інші реквізити власника сайту;

– IP-адреси, використані для створення сайту;

– IP-адреси, використані для поповнення сайту;

– інформація про зміст сайту;

– інформація про користування сайтом.

З метою *визначення належності електронної пошти* можна за допомогою сайтів 2ip або Who.is визначити провайдера, який надає послуги використання вже відомої електронної пошти, після чого звернутися до нього із запитом.

Довідково. Під час розслідування кіберзлочинів слідчі мають розуміти, що означають складові елементи електронної пошти. Для прикладу проаналізуємо таку адресу електронної пошти: **ghjhnts@rfrfal.kyz.com**[89]**.**

ghjhnts – це ім'я користувача. Кожне ім'я користувача має бути унікальним у межах домену, але одне й те саме ім'я користувача можна використовувати у різних доменах. Після імен користувачів стоїть знак @, щоб показати, де закінчується ім'я користувача й починається ім'я домену.

rfrfal – субдомен – можна додати будь-яке ім'я субдомену у межах домену, але їх не часто використовують в адресах електронної пошти. Субдомени електронної пошти часто використовують шахраї, щоб змусити людей подумати, що електронний лист надійшов від законної організації й спонукати натиснути посилання. Наприклад, на перший погляд може видатися, що електронний лист від «ghjhnts@rfrfal.kyz.com» надійшов від «rfrfal», але насправді він надійшов із домену «kyz».

kyz – доменне ім'я. Для організацій і компаній це, зазвичай, те саме доменне ім'я, що й вебсайт. Особисті та одноразові облікові записи електронної пошти можна налаштувати через популярних постачальників послуг, таких як Gmail, які використовують ім'я постачальника як домен. Компанії та організації можуть використовувати тих самих постачальників

[89] OBTAINING CROSS-BORDER ELECTRONIC EVIDENCE SECTION 1: INVESTIGATIVE TECHNIQUES. This e-Learning course was created as part of INTERPOL's Cyber Capabilities and Capacity Development Project (C3DP), funded by the United States Department of State – Bureau of International Narcotics and Law Enforcement (INL). The e-Learning course was jointly developedwith the National White Collar Crime Center (NW3C). ©2023.

послуг для розміщення своїх служб електронної пошти, але домен буде їхнім власним зареєстрованим іменем. Знову ж таки, доменні імена мають бути унікальними, а для позначення кінця кожного рівня домену після знака «@» в адресі електронної пошти використовують крапки.

com – домен верхнього рівня (TLD) – як і на вебсайтах, усі адреси електронної пошти мають домени верхнього рівня, в яких вони зареєстровані, причому «com» є найпоширенішим[90].

Для ідентифікації особи правопорушника треба встановити:

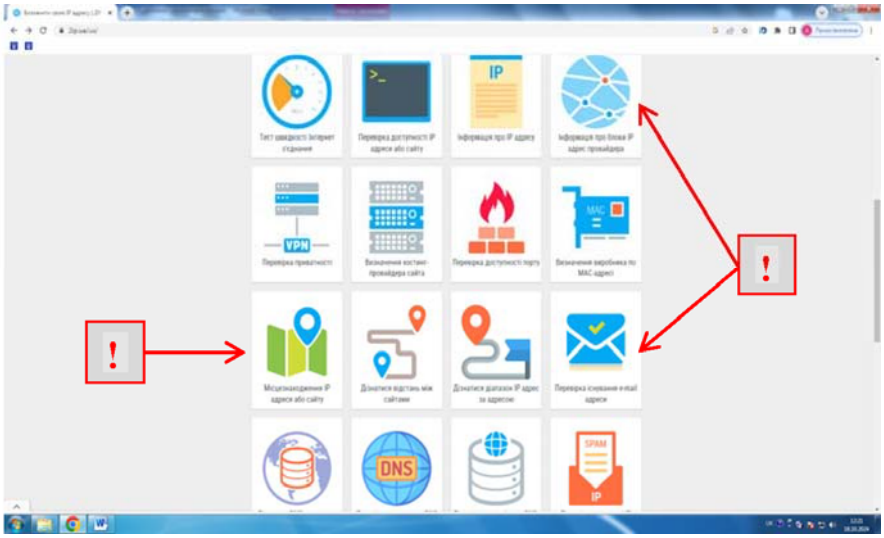
– коло осіб, які користуються певним терміналом, а також мету та межі їх користування;

– осіб, які користувалися терміналом під час вчинення протиправних дій;

– осіб, які мають доступ до мережі «Інтернет», які при цьому використовуються логіни й паролі, який провайдер надає послугу;

– з яких ще IP-адрес використовувались встановлені реквізити під час доступу до мережі тощо.

Краще надавати перевагу використанню сайту 2ip як найбільш зручному для отримання потрібної інформації, оскільки сайт пропонує за темами обрати напрям надсилання відповідного запиту, наприклад, за такими: «Інформація про блоки IP-адрес провайдера», «Місцезнаходження IP-адреси або сайту», «Перевірка існування e-mail» та ін.



2ip (меню головної сторінки)

[90] OBTAINING CROSS-BORDER ELECTRONIC EVIDENCE SECTION 1: INVESTIGATIVE TECHNIQUES. This e-Learning course was created as part of INTERPOL's Cyber Capabilities and Capacity Development Project (C3DP), funded by the United States Department of State – Bureau of International Narcotics and Law Enforcement (INL). The e-Learning course was jointly developedwith the National White Collar Crime Center (NW3C). ©2023.

Для отримання корисної інформації із заголовків електронних листів і пошуку інформації про IP-адресу джерела рекомендуємо використовувати інструмент **Trace Email**. Щоб переглянути історію оглядів, тобто як вебсайти виглядали протягом багатьох років, можна використовувати ресурс **Wayback Machine**, який архівує загальнодоступні вебсайти. За допомогою інструменту **Exonera Tor** можна з'ясувати, чи слугувала IP-адреса вузлом Tor[91] на певну дату.

Взаємодія під час розслідування кіберзлочинів

Під час вчинення злочинів у кіберпросторі треба враховувати, що утворення значної частини слідів відбувається в електронному середовищі одночасно на багатьох апаратних засобах комп'ютерної техніки, комп'ютерної мережі або електронної комунікаційної мережі, мережі електрозв'язку. Останні ж можуть перебувати на чітко визначеній географічній території під юрисдикцією певної держави та у власності конкретної особи[92], а повноваження правоохоронних органів обмежені територіальними кордонами[93].

Отже, з часом виникла необхідність створити світову загальну систему моніторингу та розробити нові юридичні обов'язкові стандарти – як результат 23 листопада 2001 р. Рада Європи прийняла Конвенцію про кіберзлочинність, яка мала на меті підвищити ефективність розслідувань кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, а також покращити можливості збирання доказів в електронній формі[94].

Відповідно до ст. 35 Конвенції про кіберзлочинність обов'язковим стало створення цілодобової мережі для надання негайної допомоги щодо розслідування або переслідування стосовно

---

[91] *Tor* – веббраузер, створений для анонімності та доступу до частин темної мережі. Мережа використовує кілька рівнів шифрування для захисту особи користувача. Його розроблено таким чином, щоб ніхто не міг зв'язати певного користувача з його мережевою діяльністю.

[92] Головкін Б. М., Денькович О. І. , Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази: навч. посіб. / за ред. канд. юрид. наук, доц. Ольги Денькович, д-ра права, проф. Габріеле Шмельцер. Львів: ЛНУ ім. Івана Франка, 2022. С. 99. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 11.04.2024).

[93] Ахтирська Н. М. Одержання доказів в електронній формі в світлі Другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. Вип. 67. 2022. С. 190, 192–193. DOI: https://doi.org/10.33994/kndise.2022.67.21

[94] Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 01.02.2024).

кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосуються кримінального правопорушення. Створені Мережі 24/7 можуть надати термінову допомогу правоохоронним органам, які шукають дані від постачальників послуг, розташованих в іноземних державах.

Закон України «Про ратифікацію Конвенції про кіберзлочинність» визначив МВС України органом, виключно на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі[95].

07 листопада 2021 р. Комітет міністрів Ради Європи прийняв Другий додатковий протокол до Конвенції про кіберзлочинність (далі – Протокол), який скерований на розширення міжнародного співробітництва та розкриття електронних доказів[96].

Протокол передбачає вищий рівень оперативності та доцільність прискореної процедури через отримання даних безпосередньо від суб'єкта, який володіє інформацією або під контролем якого вона перебуває, тобто без опосередкованого звернення до контактного центру.

У Протоколі закріплено положення щодо:

– покращення прямої співпраці з постачальниками та іншими організаціями-сторонами;

– надзвичайної взаємодопомоги;

– посилення міжнародного співробітництва між органами влади щодо розкриття збережених комп'ютерних даних;

– міжнародного співробітництва, якщо воно не застосовується за міжнародними договорами.

Цей Протокол є відкритим для підписання країнами – членами Ради Європи, які є Сторонами Конвенції або підписали її. Він підлягає ратифікації, прийняттю або схваленню.

На 2022 р. Протокол одразу підписали такі країни – члени Ради Європи: Австрія, Бельгія, Болгарія, Естонія, Фінляндія, Ісландія, Італія, Литва, Люксембург, Чорногорія, Нідерланди, Північна Македонія,

---

[95] Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 28.06.2024).

[96] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: https://rm.coe.int/1680a49dab (Last accessed: 15.05.2024).

Португалія, Румунія, Сербія, Іспанія та Швеція, а також країни, які не є країнами – членами Ради Європи: Чилі, Колумбія, Японія, Марокко та США[97]. До кінця 2022 р. до Протоколу також доєдналась Хорватія, Республіка Молдова, Словенія, Шрі-Ланка, Україна та Сполучене Королівство[98].

3.2. Особливості збирання електронних доказів під час розслідування шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки

Шахрайство, пов'язане з комп'ютерами – це дії, що призводять до втрати майна іншої особи шляхом:

– будь-якого введення, зміни, знищення чи приховування комп'ютерних даних;

– будь-якого втручання у функціонування комп'ютерної системи з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи[99].

Відповідно до ч. 4 ст. 190 КК кримінальна відповідальність передбачена за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки[100].

Досить поширеними способами вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки є:

– ***продаж товарів або надання послуг*** (наприклад, продаж неіснуючих товарів або пропозиція надання неіснуючих послуг за передплатою з використанням сайтів OLX, Shafa чи месенджерів «Telegram», «Instagram» тощо);

---

[97] Посилена співпраця та розкриття електронних доказів: 22 країни підписали новий Протокол до Конвенції про кіберзлочинність. *Офіс Ради Європи в Україні:* офіційний сайт. (12.05.2022). URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention

[98] Україна приєдналася до додаткового протоколу до Конвенції про кіберзлочинність. *Я і закон:* інформаційно-юридичний сайт. (02.12.2022). URL: https://yaizakon.com.ua/ukrayina-priyednalasya-do-dodatkovogo-protokolu-do-konventsiyi-pro-kiberzlochinnist/

[99] Конвенція про кіберзлочинність від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 01.02.2024).

[100] Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 18.02.2024).

– ***родич у біді*** (наприклад, коли телефонують людині літнього віку й повідомляють, що стався нещасний випадок, її син чи донька потрапили в лікарню і терміново потрібні кошти, щоб їм допомогти);

– ***несанкціоновані транзакції*** (наприклад, здійснення електронних платежів, коли відбувається несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах, щоб ввести в оману автоматизовану систему і видати себе за того, хто має право у ній працювати і здійснювати відповідні операції);

– ***незаконне отримання кредитів*** (наприклад, оформлення онлайн-кредитів з використанням електронно-обчислювальної техніки на ім’я осіб, анкетні дані яких отримано шляхом обману);

– ***інше***.

Із початком воєнного стану з’явилися нові способи недобросовісних дій, у тому числі й через мережу «Інтернет». Одна з найпоширеніших схем кібершахрайства, від якої постраждали тисячі українців, особливо на сході країни, – імітація допомоги в евакуації. Злодії розміщують у мережі «Інтернет» оголошення, пропонуючи усім бажаючим швидко та безпечно виїхати до безпечних регіонів України чи навіть за кордон. У процесі спілкування шахраї намагаються виманити передоплату за свої послуги, посилаючись на небезпеку, необхідність резервування місць та ін. Отримавши передоплату, шахраї зникають і перестають виходити на зв’язок.

Ще одна схема шахрайства, досить поширена після початку воєнних дій, – діяльність фейкових благодійних і волонтерських організацій. Під виглядом збору грошей на благодійність аферисти створюють фіктивні сайти, сторінки в соціальних мережах, канали в Telegram і привласнюють кошти громадян[101].

На початковому етапі розслідування шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки необхідна інформація може бути:

– отримана від заявника про відомі йому обставини вчинення кримінального правопорушення з відповідними додатками, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм);

[101] Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика: монографія. Одеса: Вид-во «Юридика», 2024. С. 49–50.

– отримана з документів (у разі наявності таких), що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби;

– установлена унаслідок отриманих даних про використані електронно-обчислювальні машини (комп'ютери), системи і комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі «Інтернет», IP-адреса, вебадреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо).

Типовими електронними джерелами доказів у кримінальних провадженнях за фактом вчиненого шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки можуть виступати:

– зміст листування між злочинцем і потерпілим;

– дані щодо одночасного листування злочинця з іншими потенційними жертвами;

– квитанції про перерахування коштів потерпілим на рахунки злочинців;

– квитанції про зняття з рахунків готівки, що потім передавалась злочинцю;

– виписки по рахунках, що належать злочинцю, про рух коштів по його банківським карткам;

– факт користування злочинцем сторінками в соціальних мережах від імені вигаданих осіб;

– факт впізнання потерпілим шахрая за ознаками голосу, якщо відбувались телефоні перемовини;

– факт належності злочинцю SIM-карти, за допомогою якої здійснювались дзвінки потерпілому;

– факт відсутності законних джерел прибутку у шахрая, за наявності в нього значних грошових коштів, джерело отримання яких він не може пояснити[102].

У провадженнях щодо шахрайства сліди можуть залишатися: у пам'яті телефону, на SIM-карті, у комп'ютері, на сервері мобільного оператора, на сервері інтернет-провайдера; на флешці, зовнішньому вінчестері; у пам'яті системи відеоспостереження (зал інтер-

[102] Заяць К. Д. Методика розслідування шахрайств: дис. ... канд. юрид. наук: 12.00.09. / Харків. нац. ун-т внутр. справ. Харків, 2020. С. 76.

нет-кафе, фойє банку, територія біля банкомата тощо), у пам'яті електронного журналу банкомата (термінала), в історії платіжних переказів через банківську систему, на квитанціях і роздруківках про електронні банківські платежі, на банківських картках; як сліди папілярних ліній на засобах комп'ютерної техніки, клавіатурі термінала тощо[103].

Типові обставини, що підлягають встановленню під час розслідування шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки, такі: джерело надходження інформації про подію шахрайства, наявність факту кримінального правопорушення; у чому саме полягали підготовчі дії, дії з безпосереднього вчинення та приховування шахрайства, яка їх тривалість, де вони відбувалися; кількість епізодів злочинної діяльності, час та місце вчинення шахрайських дій. Крім того, встановлюють такі обставини: які характеризують особу потерпілого; які характеризують особу шахраїв, їх кількість і характер участі кожного у вчиненні шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки; які доводять ознаки організованого злочинного угруповання; що підтверджують вину кожного із шахраїв; обставини, що виключають кримінальну відповідальність; які впливають на ступінь тяжкості вчиненого кримінального правопорушення, обтяжують чи пом'якшують покарання кожного співучасника; що підтверджують вид і розмір завданої шкоди, а також місце перебування шахрая, якщо його не було затримано відразу після вчинення кримінального правопорушення.

З-поміж приватних даних, які слід встановити, є такі: приналежність і характеристика сайту; визначення провайдера, який надавав послугу хостингу; визначення банку, через який проводилися транзакції; абонентська інформація про особу та її ідентифікація; встановлення IP-адреси, з якої здійснювався доступ, потрібний для укладання угоди через мережу «Інтернет» тощо[104].

---

[103] Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика: монографія. Одеса: Вид-во «Юридика», 2024. С. 55–56.

[104] Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика: монографія. Одеса: Вид-во «Юридика», 2024. С. 61–62, 73, 88–89.

3.3. Особливості збирання та дослідження електронних доказів у кримінальних провадженнях щодо воєнних злочинів

З початку повномасштабного військового вторгнення рф на територію України військовослужбовці рф вчинили численні порушення міжнародного гуманітарного права, які були кваліфіковані як воєнні злочини. Розслідування таких злочинів супроводжується труднощами, які є нетиповими для слідчих, що мають досвід розслідування загальнокримінальних правопорушень.

Основними викликами під час розслідування воєнних злочинів є:

– відсутність доступу до окупованих територій, а отже, і до місця злочину;

– недостатньо інформації про військовослужбовців рф у наявних базах даних правоохоронних органів;

– висока латентність;

– втрата доказів з часом тощо.

Названі фактори істотно впливають на ефективність розслідування, створюють дефіцит можливостей для отримання традиційних доказів.

Під час розслідування воєнних злочинів доцільно використовувати такі види електронних доказів:

– відеозаписи з БПЛА;

– матеріали радіоперехоплення;

– супутникові знімки;

– інформацію з відкритих джерел мережі «Інтернет» тощо.

Безпілотні літальні апарати широко використовують у воєнних конфліктах для спостереження, збирання інформації та проведення розвідувальних операцій. Відеозаписи з БПЛА є ефективним електронним доказом під час розслідування воєнних злочинів, оскільки вони забезпечують:

– *точну візуалізацію місця події* – дозволяють фіксувати докази з повітря в реальному часі, що може підтвердити факт вчинення злочину, рух військової техніки чи розташування підрозділів;

– *хронологічний запис* – відеозаписи з БПЛА можуть фіксувати події у різні моменти часу, що дозволяє простежити за динамікою розвитку ситуацій та документувати переміщення військових підрозділів або їх техніки, обладнання;

– *фіксацію слідів руйнувань* – завдяки відеозаписам можна зафіксувати масштаби руйнувань, спричинених воєнними діями, та їх зв'язок із діями конкретних військових частин;

– *дистанційний доступ до зон бойових дій* – у ситуаціях, коли доступ до території є небезпечним або неможливим через активні бойові дії, БПЛА можуть збирати відеодокази з висоти, що робить можливим здійснити огляд місць злочину;

– *тривале спостереження* – БПЛА можуть залишатися в повітрі тривалий час, забезпечуючи безперервний контроль і запис важливих подій.

Відеозаписи з БПЛА надають можливість створити повну картину подій навіть коли доступ до території обмежений або неможливий.

Радіоперехоплення – це процес запису та аналізу радіокомунікацій між військовими підрозділами або окремими особами. Цей спосіб збирання електронних доказів є досить важливим у розслідуванні воєнних злочинів, оскільки дозволяє:

– *встановити зміст наказів та інструкцій* – перехоплені радіопередачі можуть містити накази, що підтверджують вчинення воєнних злочинів (наприклад, накази щодо обстрілу цивільних об'єктів або інших порушень міжнародного гуманітарного права);

– *визначити причетність конкретних осіб* – радіоперехоплення дозволяє ідентифікувати осіб, які брали участь у передаванні команд, що може сприяти встановленню відповідальності за злочини;

– *реконструювати події* – за допомогою перехоплених розмов можна відтворити перебіг воєнних операцій і виявити зв'язок між наказами та наслідками їх виконання.

Це джерело інформації часто є єдиним способом отримати докази безпосередньо від учасників подій, коли інші способи збирання інформації є недоступними.

Системи радіоперехоплення фіксують усі частоти радіомовлення в автоматичному режимі. У процесі радіоперехоплення неможливо ідентифікувати пристрій, використовуваний для радіозв'язку, можна виявити лише частоту, на якій відбувається радіозв'язок, – тому в межах НСРД отримати таку інформацію майже неможливо, слідчі мають звернутися до тримачів інформації в порядку, визначеному ст. 93 КПК.

Супутникові знімки є ефективним інструментом для моніторингу великих територій у контексті воєнних конфліктів. У розслідуванні воєнних злочинів їх використовують для:

– *візуального підтвердження подій* – супутникові зображення можуть надавати докази руйнувань, переміщення військових підрозділів, розташування військової техніки або змін у ландшафті, що свідчить про воєнні операції;

– *моніторингу динаміки конфлікту* – супутникові знімки дозволяють спостерігати за подіями у реальному часі або за допомогою знімків, зроблених у різні моменти, що дозволяє відстежувати розвиток конфлікту;

– *виявлення масових поховань або укриттів* – супутникові знімки допомагають ідентифікувати місця масових поховань або інших структур, пов'язаних з воєнними злочинами, навіть у важкодоступних місцях або на окупованих територіях.

Застосування супутникових знімків надає можливість встановити точні координати території (місця) (з точністю від 1 до 3 метрів); точний час, коли відбувалося діяння (з точністю від 1 до 7 днів); тривалість діянь (період від 1–7 днів); площу (масштаб), на якій відбувався факт порушення (період від 1–7 днів до декількох років); кількість задіяних транспортних засобів, військової техніки; маршрути (дороги), які використовували транспорті засоби, військову техніку; точні координати транспортних засобів, військової техніки (від 1 до 3 метрів), які були задіяні під час порушення законів та звичаїв війни тощо[105].

Супутникові знімки є важливим інструментом для документування злочинів і можуть бути використані як візуальні докази у міжнародних судових процесах.

Відкриті джерела цифрової інформації. Інформацію з відкритих джерел можна використовувати для ідентифікації воєнних злочинців, розпізнавання їх облич, встановлення фактів і наслідків воєнних злочинів тощо, особливо в умовах, коли доступ до фізичних доказів обмежений або ускладнений.

Відповідно до передбачених у нормах КПК вимог до доказів слідчому у процесі їх збирання треба забезпечити їх належність і допустимість. Отже, *під час прийняття рішення щодо доцільності збирання цифрових матеріалів з відкритих джерел мережі «Інтернет» слідчий має з'ясувати:*

---

[105] Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: методичні рек. / С. С. Чернявський, В. І. Присяжний, О. М. Стрільців та ін.; за заг. ред. М. С. Цуцкіридзе. Київ: Нац. акад. внутр. справ, 2023. С. 55–56.

1. Чи є цифровий елемент придатним для конкретного розслідування?

2. Чи є інформація щодо цифрового контенту достовірною? Це може включати перевірку метаданих і спробу виявити першоджерела матеріалу пов'язаної інформації та джерела.

3. Чи є ймовірність видалення цифрового елемента з Інтернету чи загального доступу? Якщо так, слід зібрати найбільш надійну відому версію.

4. Чи безпечно збирати цифровий елемент, чи можна і потрібно вжити додаткові заходи безпеки[106]?

Під час роботи з цифровою інформацією з відкритих джерел слідчий має використовувати відкритий код, відкрите програмне забезпечення для пошуку, збирання та збереження цифрової інформації у відкритому доступі[107].

Окрім цього, щоб інформація з відкритих джерел стала доказом у кримінальному провадженні, вона має бути отримана у передбаченому КПК порядку й має містити фактичні дані, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню. З метою правильного збирання та збереження отриманих даних і недопущення видалення інформації з мережі «Інтернет» слідчий має провести огляд вебсторінки, на якій розміщено потрібну для кримінального провадження інформацію, *скориставшись такими рекомендаціями*:

1. Через пошуковий сервіс/додаток (наприклад, «Google», «Telegram Desktop» та ін.), увівши у пошукову стрічку запит, здійснити пошук потрібної інформації. Також для пошуку потрібної інформації у мережі «Інтернет» можна скористатися рекомендаціями щодо використання пошукових систем у мережі «Інтернет» для збирання інформації, яка має значення для кримінального провадження (див. дод. 1).

---

[106] Протокол Берклі. … .

[107] 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. С. 19.

2. Здійснити огляд знайденої вебсторінки. Огляду та опису підлягають лише ті цифрові матеріали, які мають значення для кримінального провадження.

3. У процесі огляду зробити скрін кожної оглянутої сторінки, який треба послідовно розмістити у протоколі огляду після її опису.

4. Здійснити повне збереження оглянутої вебсторінки за допомогою будь-якого браузера («Google Chrome», «Firefox», «Opera» та ін.). У результаті цього створюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.

5. Здійснити архівацію потрібної сторінки за допомогою Інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та ін.).

6. За допомогою програмних засобів, які використовуються для вивчення різних метаданих і є у відкритому доступі у мережі «Інтернет», провести аналіз потрібних файлів.

7. Зазначити у протоколі, за яким посиланням розміщено «Звіт аналізу метаданих».

8. Перейти за цим посиланням і зробити знімок екрана, на якому відображено звіт аналізу, й розмістити його за змістом в описову частину протоколу.

9. За допомогою програми «RapidCRC Unicode 0.3.37.0» провести хешування отриманого файлу з метою отримання хеш-коду (алгоритм sha).

10. Зробити знімок екрана з отриманим хеш-кодом й розмістити його за змістом в описову частину протоколу/оформити додатком до протоколу.

11. 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 загалом*).

12. Цифровий носій інформації, на який було скопійовано оглянуту інформацію, має бути належним чином упакований, оформлений як додаток до протоколу огляду.

13. 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.

14. Здійснити фіксування СРД-огляду цифрових матеріалів у протоколі огляду[108; 109].

Практичний досвід розслідування воєнних злочинів засвідчує ефективність комплексного підходу до збирання доказів і методів їх аналізу.

На початковому етапі розслідування воєнних злочинів, окрім допиту потерпілих, свідків, проведення інших першочергових СРД та НСРД, одним з основних завдань слідчих є *встановлення підрозділів збройних сил рф, які перебували на місці вчинення кримінального правопорушення, у визначений період.* Це стає можливим унаслідок проведення комплексу заходів, зокрема:

– дослідження деокупованих територій з метою пошуку та вилучення документів, мобільних пристроїв, залишених окупантами;

– робота з полоненими;

– аналіз мобільного трафіку російських військовослужбовців;

– отримання інформації від розвідувальних органів.

На цьому етапі розслідування особливу увагу слід приділити дослідженню деокупованої території. З метою виявлення та фіксації доказів вчинення злочину слідчий має провести детальний огляд місця події. Одним із завдань слідчого під час проведення СРД-огляду є виявлення та вилучення наявних носіїв інформації в електронній (цифровій) формі, на яких можуть бути зафіксовані злочини, які вчиняли військовослужбовці рф на території України, інформація, яка може стати інструментом для ідентифікації та зіставлення військової техніки, встановлення типу військової техніки та озброєння, ідентифікації зафіксованих військовослужбовців рф, встановлення їх анкетних даних, місця проживання, паспортних даних, встановлення їх сторінки у соціальних мережах, актуальних фото, які можна буде використати під час пред'явлення особи для впізнання за фотознімком, можливі номери мобільних телефонів російських військовослужбовців/їх близьких родичів, друзів та іншу інформацію, яка може бути важлива для

[108] 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.pd (дата звернення: 28.06.2024).

[109] 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.

проведення повного, швидкого та неупередженого досудового розслідування, встановлення всіх обставин кримінальних правопорушень і винних осіб.

Така інформація може бути зафіксована камерами відеоспостереження, які встановлені на будівлях, вулицях населених пунктів деокупованих територій, у засобах фото- та відеозапису на БПЛА, у виявлених на місці події ноутбуках, мобільних пристроях, якими могли користуватися військовослужбовці рф тощо. У разі виявлення таких носіїв інформації в електронній (цифровій) формі слідчі мають вжити заходи щодо належного їх вилучення і збереження інформації, яку там розміщено. Надалі така інформація підлягає детальному аналізу з метою встановлення обставин, які мають значення у кримінальному провадженні.

Наступний етап – визначення організаційної структури військового підрозділу, встановлення особового складу, ідентифікація і встановлення анкетних даних військовослужбовців.

На цьому етапі одним із найбільш складних і важливих завдань слідчого є *ідентифікація військовослужбовців* рф, у зв'язку з чим необхідно з'ясувати їх анкетні дані, що є досить складно у зв'язку з відсутністю відповідних документів. Отримати таку інформацію можна у разі виявлення абонентських номерів мобільних телефонів військовослужбовців рф та проведення їх аналізу. Для цього треба вжити ряд заходів і провести такі процесуальні дії:

1) здійснити тимчасовий доступ до речей і документів, які перебувають у розпорядженні мобільних операторів, з метою виявлення інформації щодо фіксування у мережі мобільного зв'язку операторів України, на певній деокупованій території мобільних терміналів із SIM-картами рф;

2) виявлені абонентські номери телефонів військовослужбовців рф перевірити за допомогою баз даних, які наявні у розпорядженні органів досудового розслідування, результат перевірки відобразити у довідці;

3) керуючись ст. 2, 40, 91–93 КПК підготувити запит або ж відповідно до ст. 39, 40, 41 КПК підготувити доручення до Департаменту кримінального аналізу Національної поліції України або до Департаменту кіберполіції Національної поліції України щодо проведення детального аналізу виявлених абонентських номерів, встановлення повних анкетних даних їх власників, адреси проживання, приналежність до збройних сил рф (посада, звання, взвод, рота, батальйон, полк, дивізія), фотознімки належної якості з можливістю їх використання для пред'явлення для впізнання, контактні телефони та іншу

важливу інформацію, яка могла б бути важлива для ідентифікації вказаних осіб.

Можна доручити провести огляд інформації з відкритих джерел, а саме соціальних мереж «ВКонтакте», «Однокласники», «Facebook», відеохостигу «YouTube» тощо з метою встановлення акаунтів, користувачів виявлених абонентських номерів.

До доручення/звернення слід додати довідку з результатами попередньої перевірки абонентських номерів мобільних телефонів військовослужбовців рф.

За абонентськими номерами мобільних телефонів можна встановити й відстежити маршрут переміщення військовослужбовців рф, місце їх фактичного перебування, переміщення взводу, роти, батальйону, полку, дивізії. Така інформація у сукупності з іншими доказами, виявленими слідчими безпосередньо на місці події, дає можливість довести причетність військовослужбовців рф до вчинення злочину на тій чи іншій території.

Якщо треба терміново ідентифікувати військовослужбовця рф, слідчий, за наявності відповідних навиків, самостійно може здійснити пошук інформації про нього (допоміжної інформації, що його стосується) з використанням відкритих джерел мережі «Інтернет» за фото або відеозображенням із ним.

Робота з фото

Пошук за фото в мережі «Інтернет» можна здійснювати двома способами з використанням будь-якої пошукової системи.

Перший спосіб полягає у здійсненні пошуку за коротким текстовим описом зображення:

«у поле пошуку вводять текстовий опис зображення (або фото) $\Rightarrow$ у результатах пошуку отримують зображення $\Rightarrow$ натиснувши на зображення, можна збільшити його розмір у вікні браузера й отримати доступ до відображення посилання на ресурс (сайт), на якому воно розміщене».

Другим способом пошук здійснюють за зображенням. Пошук активується натисканням відповідної іконки в полі пошуку, що дасть можливість розмістити фото, за яким потрібно зробити пошук:

1) завантаживши його, якщо фото розміщене на комп’ютері;

2) посилання на фото, якщо воно розміщене в мережі «Інтернет».

Під час аналізу зображень (фото) як джерела інформації треба:

– застосовувати зворотний пошук за зображенням, де воно є джерелом інформації. Окрім очевидних речей, що зображені на фото, потрібно аналізувати метадані, аналогічні зображенням, і можливі збіги з іншими фото за змістом (або частковим змістом);

– 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.

У розпізнаванні обличчя треба використовувати актуальні інструменти. **У практичній діяльності можуть бути використані наведені у таблиці інструменти, які є у відкритому доступі мережі «Інтернет».**

Назва програми	Стислий зміст
Neuroidentigraf	Система розпізнавання обличчя, створена на основі нейромережі.
https://identigraf.center	
Search4faces	Ресурс для пошуку людей у 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 у соціальній мережі.
https://search4faces.com/search.html	
Facecheck	Ресурс для пошуку людей у мережі «Інтернет» за фото.
https://facecheck.id	

Працюючи з контекстним меню файлу, яке відкривається після натискання на праву кнопку миші, через вкладку «Властивості» можна переглянути запис допоміжних метаданих зображення (тип, вид і параметри налаштування камери пристрою, на який було зроблено фото, дату, час, координати зйомки тощо). Слід зважати на те, що такі дані можуть бути цілеспрямовано відредаговані, а також автоматично втрачаються за умови редагування фото та/або його публікації у соціальних мережах чи під час передачі його через месенджери.

Для вивчення більшої кількості різних метаданих рекомендовано використовувати зазначені у таблиці програмні засоби, які є у відкритому доступі у мережі «Інтернет»[110].

Назва програми	Стислий зміст
FotoForensics	Дозволяє переглядати метадані з фотозображень. Також дозволяє дізнатися дуже багато про фотографію, а найголовніше – з її допомогою можна визначити, які області на фотографії були змінені – наприклад, домальовані або поверх яких 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*	
Forensically	Також дозволяє переглядати метадані із фотозображень.
https*://29a.ch/photo-forensics/#forensic-magnifier*	
ImageForensic	Автоматизований криміналістичний аналіз зображень, який дозволяє переглядати метадані з фотозображень.
https*://www.imageforensic.org/#home*	
InVID-WeVerify	Розширення для браузерів Chrome та Firefox для перевірки зображень і відео. За допомогою цього розширення можна отримувати контекстну інформацію про відео із 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*	

[110] 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.

Робота з відео

У роботі з відео доцільно:

– використовувати можливості пошукових систем і шукати відео за ключовими словами, іменами, назвами тощо, а також використовувати сортування за різними критеріями;

– здійснювати пошук за ключовими словами у різних соціальних мережах (зокрема з використанням пошукових операторів, див. додаток 1).

Для пошуку інформації за зображеннями у відкритих джерелах, таких як соціальні мережі, доцільно використовувати спеціалізовані програмні засоби, зокрема «Clearview AI» та «Artellence». Іншими джерелами інформації є онлайн-боти, які отримують дані з різних реєстрів і відомчих баз даних.

Під час аналізу відео важливо враховувати деталі, які можуть свідчити про його недостовірність (невідповідність аудіо, розмитість кадрів, зміна їх розмірів тощо).

Якщо у результаті ідентифікації військовослужбовця з використанням фото, відеозображень слідчий виявить інформацію з відкритих джерел мережі «Інтернет», яка має важливе значення для кримінального провадження, таку інформацію слід зафіксувати у процесуальному документі (протоколі огляду). Огляду та опису підлягають лише ті цифрові матеріали, які мають значення для кримінального провадження.

Детальній фіксації у протоколі огляду вебсторінки підлягають:

– послідовність дій під час пошуку інформації;

– назва пошукового сервісу/додатка, через який здійснювався пошук потрібної інформації;

– результат здійсненого пошуку;

– отримані у результаті пошуку відомості, короткий текстовий опис публікації, фото, відео, які підлягають огляду, відомості про метадані тощо;

– до тексту додають скрінфото оглянутих сторінок, відомості про метадані тощо.

Треба здійснити повне збереження вебсторінки за допомогою будь-якого веббраузера, архівацію потрібної сторінки, скопіювати необхідні для кримінального провадження фото- та відеоматеріали тощо на носій інформації. Результати і послідовність цих дій також зазначають у протоколі огляду. Носії інформації оформлюють належним чином як додатки до протоколу.

Для отримання більш деталізованої інформації, яка ідентифікує військовослужбовця, можна надати запит у порядку, визначеному

ст. 93 КПК, до підрозділу (працівнику) кримінального аналізу Національної поліції України або кіберполіції, які мають досвід у пошуку інформації, використанні Open Source Intelligence (OSINT) та інших методів збирання інформації.

Після ідентифікації особи з використанням різних джерел у тому числі мережі «Інтернет», працівники підрозділу кримінального аналізу Національної поліції України надають аналітичну довідку, яка містить персональні дані особи, актуальні фотографії, мобільні телефони, акаунти у соціальних мережах, а також інформацію про близьких родичів.

Така аналітична довідка не є процесуальним джерелом доказу, але інформація, яка у ній зазначена, може допомогти слідчому у встановленні важливих фактів, які можуть спрямувати перебіг розслідування. Наприклад, провести огляд сторінок у соціальних мережах, де, можливо, буде виявлена інформація, що містить фактичні дані про обставини вчинення злочину, що мають значення у кримінальному провадженні, й підлягає доказуванню.

Інформація про близьких родичів військовослужбовців також важлива для розслідування. Її можна використовувати для встановлення особи, що відібрала мобільний телефон у цивільного населення, а згодом здійснювала дзвінки з телефону родичам, тобто встановити номер особи, яка приймає дзвінок (т.з. «абонент Б»).

Резюмуємо.

Поєднання нових видів електронних доказів (відеозаписів з безпілотних літальних апаратів, радіоперехоплень і супутникових знімків) із традиційними доказами (відеозаписами зі стаціонарних камер, аналізом мобільного трафіку, свідченнями потерпілих, речовими доказами) є важливим інструментом для розслідування воєнних злочинів й дозволяє:

– відновити хронологію подій – наприклад, відеозаписи із БПЛА можуть фіксувати переміщення військових підрозділів у реальному часі, тоді як стаціонарні камери спостереження можуть підтверджувати присутність цих підрозділів на конкретному місці;

– зібрати докази на різних рівнях – супутникові знімки можуть показати широкі масштаби руйнувань, радіоперехоплення можуть зафіксувати накази на проведення операцій чи атак, а свідчення потерпілих підтвердять подію злочину, яку вони могли спостерігати особисто;

– зменшити прогалини у свідченнях – традиційні свідчення свідків або потерпілих можуть бути суб’єктивними чи неповними, але новітні технології, такі як супутникові знімки чи аналіз мобільного трафіку, допомагають верифікувати й уточнити інформацію.

РОЗДІЛ 4. ПРИЗНАЧЕННЯ І ПРОВЕДЕННЯ СУДОВИХ ЕКСПЕРТИЗ ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЇ В ЕЛЕКТРОННІЙ (ЦИФРОВІЙ) ФОРМІ

4.1. Підстави і процесуальний порядок призначення судових експертиз електронних носіїв інформації та інформації в електронній (цифровій) формі

Одним із методів дослідження електронних доказів та їх носіїв є судова експертиза. Особливістю цього методу є те, що такі докази досліджують судові експерти у разі залучення їх стороною кримінального провадження або слідчим суддею за клопотанням сторони захисту у випадках та порядку, передбачених ст. 244 КПК, якщо для з'ясування обставин, що мають значення для кримінального провадження, потрібні спеціальні знання (ст. 242 КПК).

Судова експертиза може бути використана для аналізу складних цифрових доказів, таких як дані з комп'ютерних систем, аудіо-, відеозаписи тощо. Крім експертних досліджень цифрової інформації, може виникнути необхідність дослідити її носії, зокрема комп'ютерно-технічні засоби, відео-, фотокамери тощо.

Судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду (ст. 1 Закону України «Про судову експертизу» від 25 лютого1994 р., № 4038-XII).

Згідно з ч. 2 ст. 84 КПК **висновок експерта є одним із процесуальних джерел доказів**. Відповідно, отримані результати проведених судових експертиз відіграють важливу роль у розслідуванні. Результати проведеного експертом дослідження (висновок експерта) слідчий, прокурор, слідчий суддя і суд можуть використовувати з метою встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню. Зазначені суб'єкти можуть використовувати висновок експерта і як окреме джерело доказу (у деяких кримінальних провадженнях саме він відіграє ключову роль під час з'ясування всіх обставин справи), і в сукупності з іншими доказами.

Судово-експертну діяльність здійснюють державні спеціалізовані установи, їх територіальні філії, експертні установи комунальної форми власності, а також судові експерти, які не є працівниками зазначених установ, та інші фахівці (експерти) з відповідних галузей знань у порядку та на умовах, визначених Законом України «Про судову експертизу» від 25 лютого 1994 р., № 4038-XII.

До державних спеціалізованих установ, які здійснюють судово-експертну діяльність, належать:

- 1) науково-дослідні установи судових експертиз Міністерства юстиції України;
- 2) науково-дослідні установи судових експертиз, судово-медичні та судово-психіатричні установи Міністерства охорони здоров'я України;
- 3) експертні служби Міністерства внутрішніх справ України, Міністерства оборони України, Служби безпеки України та Державної прикордонної служби України.

Виключно державні спеціалізовані установи здійснюють судово-експертну діяльність, пов'язану із проведенням криміналістичних експертиз (ст. 7 Закону України «Про судову експертизу»).

Призначення судових експертиз судовим експертам державних спеціалізованих науково-дослідних установ судових експертиз Міністерства юстиції України (далі – експертні установи) та атестованим судовим експертам, які не є працівниками державних спеціалізованих установ (далі – експерти), їх обов'язки, права та відповідальність, організація проведення експертиз та оформлення їх результатів здійснюються у порядку, визначеному КПК, Законом України «Про судову експертизу», іншими нормативно-правовими актами з питань судово-експертної діяльності та Інструкцією про призначення і проведення судових експертиз та експертних досліджень, затвердженою наказом Міністерства юстиції України від 08 жовтня 1998 р., № 53/5 (у редакції наказу Міністерства юстиції України від 26 грудня 2012 р., № 1950/5).

У випадку необхідності застосування спеціальних знань, для з'ясування обставин, що мають значення для кримінального провадження, слідчий, керуючись ст. 110, 242, 243 КПК, повинен:

1. Скласти постанову про призначення експертизи, у якій зазначають такі дані:

- місце й дата винесення постанови;
- посада, звання та прізвище особи, що призначила експертизу;
- номер кримінального провадження;
- обставини провадження, які мають значення для проведення експертизи;
- підстави для призначення експертизи;
- прізвище експерта або назва експертної установи, експертам якої доручається проведення експертизи;
- питання, які виносяться на вирішення експертові;
- перелік об'єктів, що підлягають дослідженню із зазначенням точного найменування, кількості, інші відмінні індивідуальні ознаки (у тому числі порівняльних зразків та інших матеріалів, направлених експертові, або посилання на такі переліки, що містяться в матеріалах кримінального провадження);
- якщо під час проведення експертизи об'єкт (об'єкти) дослідження може(уть) бути пошкоджений(і) або знищений(і), у постанові про призначення експертизи має міститися дозвіл на його пошкодження або знищення;
- інші дані, які мають значення для проведення експертизи.

2. Надати до експертної установи постанову про призначення експертизи.

3. Разом із постановою надати до експертної установи (експерту) для порівняльного дослідження:

- об'єкти, зразки, отримані в порядку ст. 245 КПК;
- матеріали провадження (протоколи оглядів з додатками, протоколи вилучення речових доказів тощо), а також показання технічних приладів і технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису (за клопотанням експерта).

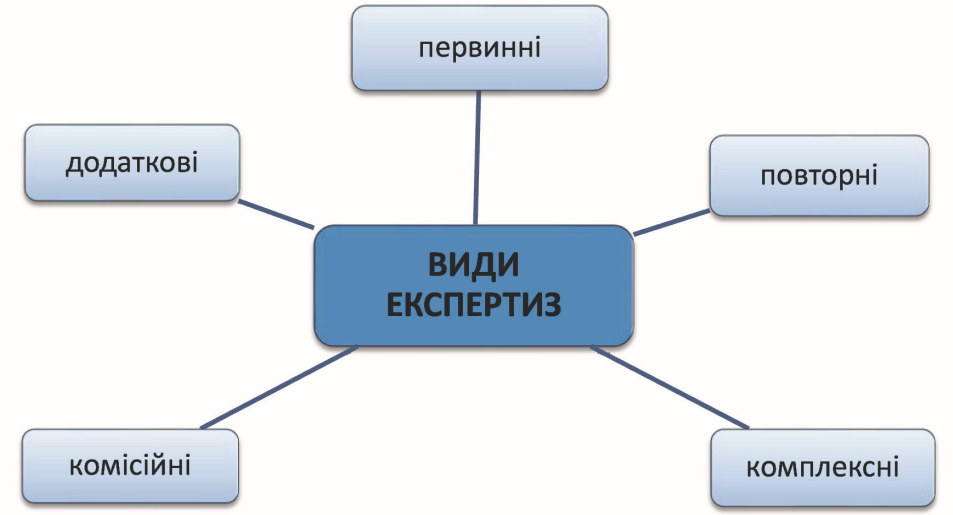
Довідково.

- Вилучення об'єктів, що підлягають дослідженню, та відібрання зразків оформлюють протоколом згідно з вимогами КПК. У них, крім загальних реквізитів такого роду документів, зазначають, які саме зразки були вилучені або відібрані, їх кількість, умови відбору або вилучення, а також інші обставини, що мають значення для вирішення поставлених питань. Протокол підписують усі особи, які брали участь у вилученні об'єктів, відбиранні зразків.
- Об'єкти дослідження надсилають в експертну установу (експертові) в упаковці, яка забезпечує їх збереження, та засвідчуються особою у передбаченому законодавством порядку. Речові докази і порівняльні зразки упаковують окремо.

4.2. Види експертиз та орієнтовний перелік питань, що можуть бути поставлені під час проведення відповідного виду експертизи

Сучасний науково-технічний прогрес створює сприятливі умови для застосування новітніх досягнень науки і техніки у боротьбі зі злочинністю, а це відкриває нові додаткові можливості реалізації спеціальних знань у судових експертизах.

Призначення і проведення судових експертиз – це найважливіша процесуальна форма застосування спеціальних знань[111].



Первинною є експертиза, коли об'єкт досліджують уперше.

Додатковою є експертиза, якщо для вирішення питань щодо об'єкта, який досліджувався під час проведення первинної експертизи, треба провести додаткові дослідження або дослідити додаткові матеріали (зразки для порівняльного дослідження, вихідні дані тощо), які не були надані експертові під час проведення первинної експертизи.

Повторною є експертиза, під час проведення якої досліджують ті самі об'єкти і вирішують ті самі питання, що й під час проведення первинної (попередніх) експертизи (експертиз).

Комісійною є експертиза, яку проводять два чи більша кількість експертів, що мають кваліфікацію судового експерта за однією експертною спеціалізацією (фахівцями в одній галузі знань). Комісію експертів

[111] Волков О. О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Дніпро: Дніпропетров. держ. ун-т внутр. справ, 2023. с. 197.

може утворювати орган (особа), який (яка) призначив(ла) експертизу (залучив(ла) експерта), або керівник експертної установи.

Комплексною є експертиза, яку проводять із застосуванням спеціальних знань різних галузей науки, техніки або інших спеціальних знань (різних напрямів у межах однієї галузі знань) для вирішення одного спільного (інтеграційного) завдання (питання). До проведення таких експертиз у разі потреби залучають як експертів експертних установ, так і фахівців установ і служб (підрозділів) інших центральних органів виконавчої влади або інших фахівців, які не працюють у державних спеціалізованих експертних установах.

З метою більш повного задоволення потреб слідчої та судової практики щодо вирішення питань, які потребують застосування наукових, технічних або інших спеціальних знань, експертні установи організовують проведення інших видів експертиз (крім судово-медичної та судово-психіатричної), зокрема й тих, що перебувають у стадії наукової розробки (пп. 1.2, 1.2.12 Інструкції про призначення та проведення судових експертиз та експертних досліджень).

Питання, які виносять на вирішення експертові, зазначають у документі про призначення експертизи (залучення експерта) серед інших обов'язкових даних.

Орієнтовний перелік питань, що можуть бути поставлені під час проведення відповідного виду експертизи, наведено у Науково-методичних рекомендаціях з питань підготовки і призначення судових експертиз та експертних досліджень.

Якщо в одному документі про призначення експертизи (залучення експерта) є питання, що стосуються різних видів експертиз, не пов'язаних між собою, керівник установи визначає, які питання підлягають вирішенню у відповідному підрозділі та послідовність їх виконання (пп. 1.2, 1.2.12, 3.3, 4.2 Інструкції про призначення та проведення судових експертиз та експертних досліджень)[112, 113].

---

[112] Інструкція про призначення та проведення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 11.04.2024).

[113] Науково-методичні рекомендації з питань підготовки і призначення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.04.2024).

Лінгвістична експертиза усного мовлення

Під час проведення ідентифікаційних і діагностичних досліджень усного мовлення особи вирішуються питання, що стосуються ототожнення особи за лінгвістичними ознаками усного мовлення.

Орієнтований перелік питань, що вирішуються під час проведення лінгвістичної експертизи усного мовлення

• Чи брала участь особа у досліджуваній розмові, зафіксованій на аудіо-, відеозаписі? Якщо так, то які слова та висловлювання промовляла саме вона?

• Чи одна й та сама особа брала участь у досліджуваних розмовах?

• Скільки осіб брали участь у розмові, зафіксованій на аудіо-, відеозаписі?

• Чи є мовлення досліджуваної особи спонтанним підготовленим (завченим) чи спонтанним непідготовленим? Чи є в мовленні досліджуваної особи ознаки читання тексту?

• Чи є в мовленні досліджуваної особи ознаки імітації мовленнєвих навичок іншої людини або спотворення своїх?

• Чи є в мовленні особи ознаки іншої мови?

• Чи є в мовленні особи лінгвістичні ознаки, що характеризують соціально-біографічні риси її особистості?

Для ототожнення досліджуваної особи з конкретною особою за ознаками мовлення надають:

• Аудіо-, відеозапис досліджуваної розмови, в якій могла брати участь певна особа.

• Аудіо-, відеозапис зразків усного мовлення особи, яку перевіряють, у формі спонтанного діалогу або монологу.

Щоб встановити ознаки читання тексту в мовленні досліджуваної особи, надають зразки читання нею тексту, зазвичай аналогічної тематики.

Експерту також обов'язково надають протокол огляду та можливість організувати прослуховування аудіо-, відеозаписів досліджуваних розмов з їх надрукованим текстом.

Фототехнічна експертиза

Фототехнічна експертиза[114] пов'язана з дослідженням фотозображень і технічних засобів їх виготовлення.

Предметом фототехнічної експертизи є фактичні дані, що мають значення для досудового розслідування або суду і стосуються дослідження фотознімків, інформації, яка в них зафіксована, техніки і технології виготовлення фотозображень.

Об'єктами дослідження фототехнічної експертизи є:

1) *фотозображення,* якими можуть бути фотокартки, діапозитиви, негативи, мікрофільми, мікрофіші, кінофільми, відеозаписи тощо. До фотознімків належать також і фотозображення, отримані без використання мокрого фотопроцесу шляхом друку на сучасних електронних засобах, але формування самого зображення при цьому обов'язково включає оптичний канал;

2) *технічні засоби виготовлення фотозображень*, до яких відносять відео-, фотознімальну апаратуру (фотоапарати, кінокамери, відеокамери, насадки на об'єктиви тощо) та лабораторне устатку-

[114] Фототехнічна експертиза. URL: https://kndise.gov.ua/fototehnichna/ (дата звернення: 28.06.2024).

вання (фотозбільшувачі, копіювальні фотостанки, кадрувальні та копіювальні рамки тощо).

Під час проведення фототехнічної експертизи вирішують *ідентифікаційні*, *класифікаційні* та *діагностичні завдання*.

Ідентифікаційні завдання пов'язані з *ототожненням предметів*, що зафіксовані у фотозображеннях, *і технічних засобів*, що використовуються для отримання фотозображень.

До предметів у цьому разі відносять: 1) предмети одягу; 2) вироби; 3) приміщення; 4) окремі ділянки місцевості, що зображені на фотознімку.

До технічних засобів, які використовують для отримання фотозображень, відносять фотокамери, відеореєстратори, системи відеоконтролю тощо.

Класифікаційні задачі пов'язані із встановленням характеристик (властивостей) невідомого чи відомого об'єкта для віднесення його до загальноприйнятого класу.

Найчастіше такі завдання виникають на початкових стадіях розслідування злочину, вони мають пошуковий характер – установити природу об'єкта, його призначення, сфери застосування тощо. Це завдання встановити клас фотоапаратури, за допомогою якої міг бути виконаний фотознімок, тип чи модель автомобіля за його зображеннями тощо.

Діагностичні завдання встановлюють стан об'єктів і події, що спричиняють його зміни.

Найбільш типовими прикладами завдань цього підкласу є:

1) встановлення обставин виготовлення фотознімків (ретуш зображення, монтаж, диференціація репродукцій і фотознімків, отриманих з натури, визначення точки зйомки тощо);

2) визначення розмірів предметів, зафіксованих на фотознімках;

3) відновлення первинного зображення на фотознімку, втраченого у результаті дії агресивних для фотоемульсії факторів;

4) реконструкція обстановки та місця події за фотознімком тощо.

Слід зазначити, що на теперішній час для проведення фототехнічної експертизи фотознімки переважно надають у цифровому вигляді, під час дослідження яких використовують інші методичні підходи, ніж ті, що застосовувались під час дослідження аналогових фотознімків.

Під час фототехнічної експертизи цифрових фото-, відеозаписів вирішують такі завдання:

– встановлення автентичності цифрових фотознімків;

– встановлення ознак монтажу цифрових фотознімків;

– встановлення технологічних і технічних характеристик виготовлення цифрових фотознімків;

– визначення розмірів зафіксованих на цифрових фотознімках предметів (об’єктів), відстані між ними;

– ідентифікація предметів (об’єктів), приміщень і ділянок місцевості, відображених на цифрових фотознімках;

– ідентифікація технічного засобу, за допомогою якого було створено цифровий фотознімок.

Орієнтований перелік питань, що вирішуються під час проведення фототехнічної експертизи

- Чи виготовлені графічні файли за допомогою наданого технічного засобу (телефону, фотоапарату, відеокамери, сканера тощо)?
- Чи виготовлені графічні файли за допомогою одного й того самого технічного засобу?
- Апарат якої моделі було застосовано для виготовлення певного фотознімка?
- Чи виготовлявся певний фотознімок за допомогою наданих технічних засобів?
- Чи застосовувалось додаткове програмне забезпечення (графічні редактори) під час виготовлення наданих фотознімків?
- Чи виготовлені (походять) надані зображення (фотознімки) з одного і того самого первинного зображення?
- Той самий чи інший об’єкт (предмет, приміщення, ділянка місцевості тощо) зафіксований на графічних файлах, зображеннях (фотознімках, негативах) та відеофайлах (відеозаписах), що надані для проведення експертизи?
- Чи виготовлено певний знімок із застосуванням фотомонтажу?
- Чи не є зображення (фотознімок) фоторепродукцією з іншого видання?
- З якої відстані знято зафіксований на фотознімку об’єкт?
- Де міститься точка зйомки наданого на експертизу фотознімка?
- За якого освітлення (природного чи штучного) проводилась зйомка?
- Чи використовувались під час виготовлення фотознімка ті чи інші технічні прийоми (глянсування, ретушування, тонування тощо)?

- Які дата і час виготовлення (редагування) фотознімка?
- Які розміри об’єктів, зафіксованих на фотознімку?
- На якій відстані один від одного були два (декілька) зображених на знімку об’єкти, яке їх взаємне розташування?
- Який зріст особи, зафіксованої на графічних зображеннях або відеофайлах[115]?

Особливості призначення фототехнічних експертиз

Залежно від питань, що поставлені на вирішення фототехнічної експертизи, експерту надають фото- та кіноапаратуру, фотознімки, кінофільми, фото- та кіноматеріали й інші відомості, що стосуються предмета дослідження.

Щоб встановити автентичність цифрових фотозображень, на експертизу надають:

– фотозображення на носіях інформації (microSD-карти тощо), на яких зазначені фотознімки фіксувалися вперше;

– технічні засоби (у повному складі), за допомогою яких було створено ці фотознімки;

– відомості про спосіб виготовлення фотозображень, що надаються на дослідження.

Щоб встановити розміри предметів, що зафіксовані на досліджуваних фотозображеннях, окрім самих фотозображень надають відомості про відомі або відповідним чином встановлені розміри інших предметів, включаючи нерухомі споруди, предмети інтер’єру тощо, які зафіксовані на досліджуваних фотознімках.

Портретна експертиза

Основним завданням портретної експертизи є ідентифікація особи за фотознімком (фотокарткою) та відеозаписом.

Орієнтований перелік питань, що вирішуються під час проведення портретної експертизи

- Чи зображена на аналізованому фотознімку особа (прізвище, ім’я, по батькові), фотокартки якої надано як зразки?

[115] Особливості призначення та можливості судової фототехнічної експертизи: інформаційний лист. Київ. наук.-досл. експертно-криміналіст. центр. Київ, 2023. URL: https://ndekc.kiev.ua (дата звернення: 19.04.2024).

• Одна чи різні особи зображені на аналізованих фотознімках?

Порівняльними матеріалами для ідентифікації особи за фотознімком можуть бути достовірні фотографії та відеозапис цієї особи (любительські, професійні, а також експериментальні). Доцільно, щоб серед порівняльних зразків були знімки, близькі до досліджуваного за часом зйомки і ракурсом зображення. Експериментальні порівняльні зразки не слід ретушувати.

Експертиза з технічного дослідження матеріалів та засобів відео-, звукозапису

Об'єктами експертизи з технічного дослідження матеріалів і засобів відео-, звукозапису[116] є:

1) звукозаписи, відеозаписи;

2) технічні засоби і пристрої, за допомогою яких здійснюють фіксацію відео- та звукозаписів, включаючи усі складові з приймання, передавання та фіксації відеозображень і звукозаписів.

Основним завданням експертизи у межах технічного дослідження матеріалів і засобів відео-, звукозапису є встановлення автентичності відео- та звукозаписів, які мають бути запропоновані як докази або використовуються іншим чином у кримінальному провадженні.

Орієнтований перелік питань, що вирішуються при проведенні експертизи з технічного дослідження матеріалів та засобів відео-, звукозапису

• Чи є наданий на дослідження звукозапис (відеозапис або відеозвукозапис) автентичним?

• Чи за допомогою досліджуваного технічного пристрою зафіксований відео-, звукозапис і його фрагменти?

• За допомогою одного чи декількох технічних пристроїв зафіксовано конкретні фрагменти відео-, звукозапису?

• Чи є наданий відео-, звукозапис оригіналом чи копією?

• Чи проводився відео-, звукозапис безперервно?

• Чи зазнавав змін наданий відео-, звукозапис?

---

[116] Експертиза відео-, звукозапису. URL: https://kndise.gov.ua/video-zvukozapysu (дата звернення: 05.03.2024).

• Чи одночасно проводився запис відеозображення і звуку у відео-, звукозаписі та чи відповідає зміст відеозображення запису звуку?

• За допомогою одного чи декількох технічних пристроїв зафіксовано конкретні фрагменти відео-, звукозапису?

• Які відео-, звукозаписи містять область видаленої інформації технічного пристрою (цифрового диктофона, змінного носія інформації, іншого пристрою відео-, звукозапису тощо)?

• Чи можна відновити у повному обсязі або частково відео-, звукозапис зі змінного носія інформації?

• Чи брали перелічені особи участь у зафіксованій на звукозаписі розмові та які конкретно слова і фрази вони промовляли?

• Скільки осіб брало участь у зафіксованій на звукозаписі розмові?

Встановлення текстового змісту розмов, що зафіксовані у відео-, звукозаписі, не є окремим експертним завданням, оскільки не потребує застосування спеціальних знань.

Особливості призначення експертизи з технічного дослідження матеріалів і засобів відео-, звукозапису

Для встановлення автентичності, технічних умов та технології отримання звукозапису (відеозапису або відеозвукозапису) на дослідження надають:

– оригінальний звукозапис (відеозапис або відеозвукозапис);

– оригінальний пристрій, яким запис (фонограма, відеограма, відеофонограма) зафіксований (зафіксована);

– додаткове обладнання, яке використовувалось для фіксації запису, у повному складі: мікрофон, джерело живлення, прилади передавання сигналу, керування тощо;

– за потреби повні відомості про внесення конструктивних змін у пристрій запису і додаткове обладнання із зазначенням хронології таких змін та опис тракту запису від передавача (мікрофона, відеокамери) до приймача (технічного засобу фіксації) із зазначенням кількості каналів та інших технічних супутніх засобів.

Слід мати на увазі, що під оригіналом з технічної точки зору розуміють запис, який утворено одночасно (у період) з фіксацією тих подій, які в ньому зафіксовані і який міститься саме на тому носії (касеті, цифровому носії інформації тощо), що при цьому використовувався.

За копіями записів без наявності їх оригіналів встановити автентичність записів експертними методами найчастіше неможливо.

Комп’ютерно-технічна експертиза

Комп’ютерно-технічну експертизу[117] проводять з метою визначення статусу об’єкта як комп’ютерного засобу, виявлення і вивчення його ролі у розслідуваному злочині, а також отримання доступу до інформації на електронних носіях з наступним всебічним її дослідженням.

Предметом комп’ютерно-технічної експертизи є факти (обставини), що мають значення для органів досудового розслідування та встановлюються на основі дослідження закономірностей розробки й експлуатації комп’ютерних засобів і систем, що забезпечують реалізацію інформаційних процесів.

Об’єктами дослідження цього виду експертизи є комп’ютерна техніка та/або комп’ютерні носії інформації, а саме:

– персональні комп’ютери (системні блоки), портативні комп’ютери (ноутбуки, нетбуки);

– будь-які машинні носії інформації, периферійні пристрої, інтегровані системи та будь-які комплектуючі всіх зазначених компонентів (апаратні блоки, плати розширення та ін.);

– програмно-апаратні комплекси, де потрібний комплексний підхід до розгляду функцій апаратури і програмного забезпечення;

– мережеве обладнання (сервери, робочі станції, файлові сховища та ін.);

– офісна периферія (принтери, сканери, багатофункціональні пристрої, модеми, роутери, точки доступу, відеоспостереження та ін.);

– програми і програмні засоби, їх компоненти (підсистеми) та супроводжувальні аналітичні матеріали й технічні документи (технічні завдання, вимоги, специфікації, моделі та ін.), алгоритми, окремі програмні модулі, вихідні тексти програм, текстові та графічні документи (в електронній формі), дані у форматах мультимедіа, виготовлені з використанням комп’ютерних засобів;

– інформація у форматах баз даних, журнали (протоколи) роботи спеціалізованих програм, інших додатків прикладного характеру, інформаційні дані;

– інформація, розміщена на сайтах у мережі «Інтернет».

---

[117] Комп’ютерно-технічна експертиза. URL: https://kndise.gov.ua/kompyuterno-tehnichna/ (дата звернення: 11.04.2024).

Інформація може міститися на різних типах носіїв, які можна класифікувати за такими видами:

– накопичувачі на жорстких магнітних дисках – пристрої для зберігання інформації, робота яких здійснюється за принципом магнітного запису;

– твердотілі накопичувачі (англ. SSD, solid-state drive) – комп'ютерні запам'ятовувальні пристрої на основі мікросхем пам'яті та контролера керування ними, що не містять рухомих механічних частин, які можуть бути виконані як окремими, так і вбудованими в інше обладнання;

– USB флеш-накопичувачі – носії інформації, що використовують флеш-пам'ять для збереження даних та підключаються до комп'ютера чи іншого пристрою через USB-порт;

– карти пам'яті – носії інформації, що також використовують флеш-пам'ять для збереження даних і підключаються до комп'ютера чи іншого пристрою за допомогою різних спеціалізованих адаптерів.

До основних завдань експертизи комп'ютерної техніки і програмних продуктів належать:

– установлення робочого стану комп'ютерно-технічних засобів;

– установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Орієнтований перелік питань, що вирішуються при проведенні комп'ютерно-технічної експертизи

- Чи міститься на досліджуваному носії потрібна інформація (зазначити, яка інформація цікавить) та у якому вигляді?
- Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?
- Чи містяться на наданих на дослідження об'єктах серед наявних і видалених файлів інформація щодо ключових слів (вказати, які саме ключові слова)? Якщо так, то скопіювати зазначену інформацію на окремий носій.
- Чи містяться на наданих на дослідження об'єктах серед наявних і видалених файлів документи формату «doc», «docx» та елек-

тронні таблиці формату «xls», «xlsx»? Якщо так, то скопіювати зазначену інформацію на окремий носій.

- Чи містяться на наданих на дослідження об’єктах файли форматів (вказати, які саме формати)? Якщо так, то скопіювати зазначену інформацію на окремий носій.
- Чи містяться на наданих на дослідження об’єктах листи електронної пошти? Якщо так, то скопіювати зазначену інформацію.
- На які вебадреси мережі «Інтернет» та коли здійснювався вихід із наданих на дослідження об’єктів?
- Чи містяться на наданих на дослідження об’єктах облікові дані користувача (логіни та паролі) для доступу до Інтернет-ресурсів? Якщо так, то надати інформацію які саме дані.
- Чи встановлені на наданих на дослідження об’єктах програми обміну повідомлення у мережі «Інтернет», а саме «Viber», «Skype», «Telegram», «Signal», «Instagram», «Facebook Messenger»? Якщо так, то чи містять вони інформацію щодо історії повідомлень і дзвінків? Скопіювати таку інформацію.
- Чи міститься на наданих на дослідження об’єктах програмне забезпечення, призначене для віддаленого керування комп’ютером: «TeamViewer», «Ammyy Admin», «Radmin», «UltraVNC»? Якщо так, то скопіювати лог-файли використання виявлених програм на окремий носій.
- Чи наявні на наданих на дослідження об’єктах програми (клієнти) дистанційного банківського обслуговування «Клієнт-банк», «Інтернетбанкінг»?
- Чи міститься на наданих дослідження об’єктах встановлене програмне забезпечення (вказати назви видів програмного забезпечення)? Якщо так, то вказати дату і час їх інсталяції.
- Чи міститься на наданих на дослідження об’єктах (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення (у сенсі грального бізнесу): «iConnect», «iChampion», «G-slot», «Gaminator», «Superomatic», «iGaming Casino», «Megasuperomatic»?
- Чи містяться на наданих на дослідження об’єктах файли, які ідентифікуються антивірусним програмним забезпеченням як шкідливе програмне забезпечення? Якщо так, то вказати які.
- Чи міститься на наданих на дослідження об’єктах інформація щодо USB-пристроїв, які використовувались у системі. Якщо так, то зазначити їх VID, PID, серійні номери, дату та час їх підключень.

- Чи містяться на наданому на дослідження відеореєстраторі відеозаписи (вказати дату, за яку потрібні відеозаписи)»? Якщо так, то виявлені відеозаписи скопіювати на окремий носій.
- Чи містяться у пам'яті наданих на дослідження об'єктів інформація щодо вмісту телефонної книги, вхідних, вихідних та неприйнятих дзвінків, текстових повідомлень, вебісторії, повідомлень у мережі «Інтернет» з додатків «Viber», «Skype», «Telegram», «Signal», «Instagram», «Facebook Messenger», а також файли користувача? За наявності зазначеної інформації скопіювати їх на окремий носій інформації[118].
- Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?
- Чи могла бути створена зазначена інформація на досліджуваному комп'ютері чи вона перенесена з іншого носія?
- Яким чином інформація (зазначити, яка саме) перенесена на досліджуваний комп'ютер (носій)?
- Які технологія та хронологія створення електронного документа (зазначити електронний документ і певний зміст)?
- Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)?
- Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме у разі встановлення) програмне забезпечення?
- Чи можна виконати певні дії за допомогою досліджуваного програмного продукту?
- Чи можливе вирішення певного завдання за допомогою досліджуваного програмного продукту?
- Чи реалізовані у досліджуваному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Для дослідження інформації, що міститься на комп'ютерних носіях, експерту надають сам комп'ютерний носій, а за потреби – комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій).

[118] Особливості призначення та можливості судової компю'терно-технічної експертизи: інформац. лист. Київ. наук.-досл. експертно-криміналіст. центр. URL: https://ndekc.kiev.ua (дата звернення: 19.04.2024).

Щоб зберегти надані на дослідження носії інформації у робочому стані, їх надають в окремих пакуваннях. Системні блоки персональних комп'ютерів надають у пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення.

Для встановлення відповідності програмних продуктів певним параметрам експерту надають носій із копією досліджуваного програмного продукту або програмного коду.

Щоб дослідити робочий стан комп'ютерно-технічних засобів, експерту надають ці комп'ютерно-технічні засоби, а також технічну документацію до них.

З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) у галузі комп'ютерної техніки.

Експертиза електронних комунікацій

Основними завданнями експертизи електронних комунікацій[119] *є*:

– визначення характеристик і параметрів мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів і випромінювальних пристроїв;

– встановлення фактів і способів передавання (отримання) інформації з використанням мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв;

– встановлення фактів і способів доступу до мереж, ресурсів та інформації у сфері електронних комунікацій;

– визначення технічних чинників якості надання електронних комунікаційних послуг на рівні їх споживання;

– встановлення конфігурації та робочого стану мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв;

[119] Науково-методичні рекомендації з питань підготовки і призначення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.04.2024).

– встановлення типу, марки, моделі та інших класифікаційних категорій мереж електронних комунікацій та їх складових, радіообладнання, радіоелектронних засобів, випромінювальних пристроїв;

– дослідження алгоритмів обробки інформації та її захисту в мережах електронних комунікацій та їх складових, у радіообладнанні, радіоелектронних засобах, випромінювальних пристроях.

Орієнтований перелік питань, що вирішуються при проведенні експертизи електронних комунікацій

- Які тип, марка, модель мережі електронних комунікацій та її складових (радіообладнання, радіоелектронного засобу, випромінювального пристрою)?
- Чи перебуває мережа електронних комунікацій та її складові (радіообладнання, радіоелектронний засіб, випромінювальний пристрій) у робочому стані?
- Які характеристики підключень до мережі має елемент мережі електронних комунікацій (радіообладнання, радіоелектронний засіб, випромінювальний пристрій)?
- Чи змінював користувач налаштування мережі електронних комунікацій та її складових (радіообладнання, радіоелектронного засобу, випромінювального пристрою)? У який час? Яке значення мають такі зміни?
- Які параметри підключень мають складові мережі електронних комунікацій (радіообладнання, радіоелектронного засобу, випромінювального пристрою)?
- За допомогою яких програмних засобів здійснювалось підключення до мережі електронних комунікацій?
- Яка топологія технічних пристроїв, об’єднаних у мережу електронних комунікацій?
- Чи відповідає функціонування мережі електронних комунікацій та її складових (радіообладнання, радіоелектронного засобу, випромінювального пристрою) технічній документації?
- Які технічні характеристики (параметри) має мережа електронних комунікацій та її складові (радіообладнання, радіоелектронний засіб, випромінювальний пристрій)?
- Чи підтверджується факт доступу до мережі електронних комунікацій та в який спосіб?

- Чи підтверджується використання ресурсів та інформації в мережі електронних комунікацій і в який спосіб?
- Чи підтверджується факт передавання (отримання) інформації в мережі електронних комунікацій та її складових?
- Чи підтверджується факт передавання (отримання) інформації з використанням радіообладнання (радіоелектронного засобу, випромінювального пристрою) та в який спосіб?
- Чи є ознаки втручання в роботу мережі електронних комунікацій?
- Які шляхи маршрутизації даних у мережі електронних комунікацій?
- Чи можливе використання мережі електронних комунікацій та її складових для вказаних цілей?
- Чи можливе використання радіообладнання (радіоелектронного засобу, випромінювального пристрою) для вказаних цілей?

Вказані рекомендовані переліки питань, що вирішуються експертами, не є вичерпними.

Під час проведення експертизи можуть вирішуватися й інші питання, що стосуються її предмета.

Експерт може відмовитися від проведення експертизи, якщо наданих йому матеріалів недостатньо для виконання покладених на нього обов'язків, а витребувані додаткові матеріали не надані, або якщо поставлені питання виходять за межі його спеціальних знань[120].

[120] Науково-методичні рекомендації з питань підготовки і призначення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.04.2024).

ВИСНОВКИ

В умовах стрімкого розвитку ІТ-індустрії фактичні дані та обставини різних видів кримінальних правопорушень, що мають значення для доказування, дедалі частіше фіксують та зберігають в електронній (цифровій) формі.

У роботі поєднано теоретичне осмислення проблеми із практичними рекомендаціями щодо збирання та дослідження електронних доказів у кримінальному провадженні. Більшість положень методичних рекомендацій містять низку важливих рекомендацій практичного спрямування. Частину матеріалу візуалізовано у таблицях і схемах. Також методичні рекомендації містять ряд QR-кодів та Інтернет-посилань на програмні засоби мережі «Інтернет», які доцільно використовувати під час пошуку, збирання та дослідження інформації в електронній (цифровій) формі.

Методичні рекомендації є адекватною відповіддю на сучасні потреби слідчої практики зі збирання та дослідження інформації в електронній (цифровій) формі у кримінальному провадженні.

ДОДАТОК 1. РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ПОШУКОВИХ СИСТЕМ У МЕРЕЖІ «ІНТЕРНЕТ» ДЛЯ ЗБИРАННЯ ІНФОРМАЦІЇ, ЯКА МАЄ ЗНАЧЕННЯ ДЛЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Пошук

– це діяльність, орієнтована на завдання, спрямована на виявлення нової інформації, що стосується визначеної мети або питання, яке становить інтерес, в тому числі під час досудового розслідування.

Під час використання пошукових систем Інтернету рекомендуємо використовувати такі алгоритми пошуку: простий пошук, розширений пошук та контекстний пошук.

Простий пошук

Під час цього пошуку в поле запиту вводять одне або декілька слів, які можуть характеризувати зміст документа. Під час введення одного слова пошукова система видає зазвичай велику кількість посилань, з яких обрати потрібну інформацію буває доволі складно. Простий пошук використовують для знаходження нескладних, однозначних питань чи теоретичних положень.

Розширений пошук

Такий пошук завжди містить запит із групи слів. Під час розширеного пошуку рекомендують зв’язувати ключові слова логічними операторами «and» (і), «or» (або), «–» (мінус) тощо. Зазвичай записи ключових слів і логічних операторів у різних пошукових системах або однакові, або доволі схожі, тому, засвоївши один раз прийоми розширеного пошуку, можна ними користуватися де завгодно, переключивши пошукову систему в потрібний режим розширеного пошуку.

Контекстний пошук

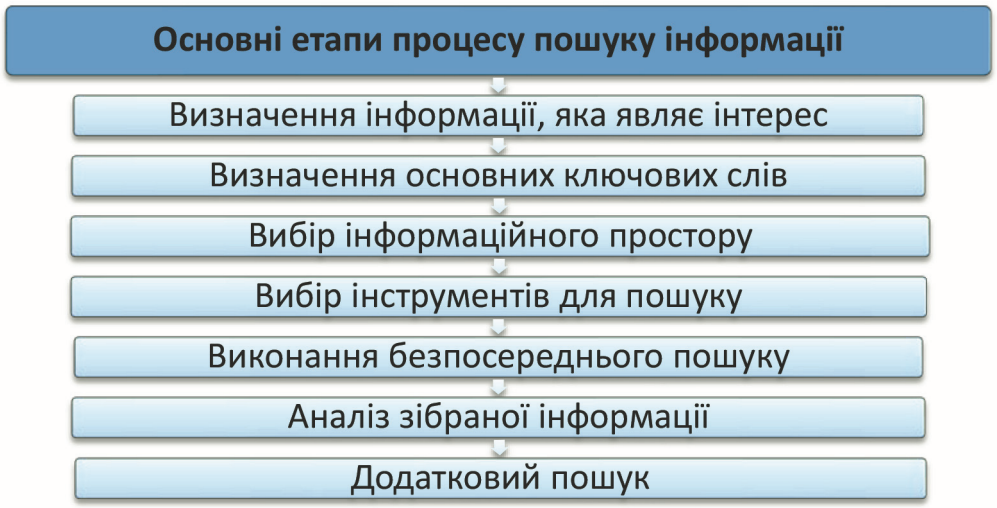
Пошукові системи, що підтримують цей вид пошуку, видають посилання на інформацію, яка точно відповідає ключовим словам у пошуковому вікні. Для цього у більшості випадків ключову фразу потрібно взяти в лапки[121].

[121] Пошук інформації в базах даних: посіб. / упор. Г. Горбенко. Київ, 2022. С. 9.

Відтак, пошук інформації в мережі «Інтернет» може бути виконаний декількома методами, які будуть різними як за ефективністю результатів пошуку, так і за типом отриманої інформації.

Пошуки в мережі «Інтернет» мають бути структурованими і систематичними, включаючи чітке досліджуване питання та параметри пошуку, а також ключові слова. Різні пошукові системи, інструменти пошуку і пошукові терміни можуть надати різні результати, тому в мережі «Інтернет» слід обирати різні шляхи для пошуку відповідної інформації.

Результативність пошуку безпосередньо залежить від чіткого усвідомлення послідовності дій, а саме чіткого планування процедури пошуку в мережі «Інтернет». Щодо цього розглянемо, з яких етапів складається процес пошуку інформації.



Визначення інформації, яка являє інтерес, передбачає виокремлення відомостей, які можуть бути використаними під час досудового розслідування. Такі відомості можуть стосуватись як обставин, що підлягають доказуванню, так і іншої інформації, що може бути корисною під час досудового розслідування. Наприклад, інформацію про підозрюваного можна використовувати для створення його психологічного портрета, що, безумовно, впливає на вибір тактики проведення слідчої (розшукової) дії за його участі.

Під час вибору ключових слів слід знати, що знайдені документи розміщуються залежно від місця ключових слів (у заголовку, на початку тексту, у перших параграфах) і частоти їх появи у тексті. Застосу-

вання різних комбінацій ключових слів дає різні результати пошуку інформації. Поєднувати ключові слова можна також за допомогою знаків і допоміжних слів.

Пошукові запити за допомогою ключових слів треба формувати так, щоб область пошуку була максимально конкретизована і звужена. Перевага надається використанню декількох вузьких запитів порівняно з одним розширеним.

Вибір інформаційного простору включає визначення регіонів пошуку. Оскільки результати пошуку залежать від географічного розташування джерела інформаційного ресурсу, слід враховувати зазначену особливість під час вибору ключових слів, які у деяких випадках слід використовувати оригінальною мовою цього регіону або мовою, яка використовується для міжнародного спілкування у цьому регіоні.

Вибір інструментів для пошуку залежить від характеру потрібної інформації. Пошук інформації відбувається переважно з використанням таких інструментів:

- інформаційно-пошукові системи («Google», «Yandex» та ін.);
- соціальні мережі;
- телеграм-боти;
- тематичні ресурси, зокрема сайти, чати і канали у месенджерах.

Інформаційно-пошукові системи

На кожному пошуковому сервері застосована своя система правил (синтаксис команд), що визначає пошук фраз із декількох слів, застосування логічних операцій і т. д. Отже, конкретні правила, що діють на тому чи іншому сервері, можуть бути різними.

Найпопулярнішим пошуковим сервісом в Україні є «Google». Пошук «Google» відбувається поетапно: через сканування, індексацію та обслуговування результатів пошуку, однак не всі вебсторінки проходять кожний етап.

1. Сканування (визначає, які сторінки існують у мережі, завантажує текст, зображення та відео зі сторінок, знайдених в Інтернеті).

2. Індексація («Google» аналізує текст, зображення та відеофайли на сторінці і зберігає інформацію в індексі «Google», який, по суті, є великою базою даних).

3. Обслуговування результатів пошуку (коли користувач шукає в «Google», «Google» повертає інформацію, яка відповідає запиту користувача).

Соціальні мережі

Сьогодні майже не залишилося осіб, які не зареєстровані в соціальних мережах, а якщо навіть особа не має акаунту в соціальній мережі, інформація про неї може бути на сторінках її родичів, знайомих тощо. Якість пошуку інформації у зазначеному сегменті Інтернету залежить від конкретної соціальної мережі та передбачає необхідність знань механізмів пошуку певної інформації. Якщо є первинні дані для пошуку, наявна електронна пошта або телефонний номер, то потрібно передусім зрозуміти, чи є в соціальних мережах облікові записи, прив'язані до цих ідентифікаторів.

Соціальні мережі в одних країнах досліджувати набагато зручніше, ніж в інших, – це певною мірою залежить від культури, доступності Інтернету й особливостей регіону. Потрібно оцінити, які соціальні мережі популярні в середовищі та країні аналізованого фігуранта. Обов'язково треба ознайомитися із законодавством про захист даних і конфіденційність та з культурою у цільовій країні. Слід зазначити, що навіть найбільш обережний і найбільш вправний користувач цифрових технологій мимоволі залишає за собою слід, не усвідомлюючи цього[122].

Телеграм-боти

Телеграм-боти передбачають право безкоштовного користування на умовах платної передплати або з оплатою кожного пошукового запиту.

Джерелом інформації можуть бути тематичні телеграм-боти, а також мобільні додатки, за допомогою яких громадяни можуть передавати інформацію, наприклад такі, як телеграм-бот «єВорог» (@evorog_bot), мобільний додаток «BACHU» та ін.

Телеграм-боти здебільшого однакові, у роботі з ними пошук інформації слід здійснювати за такими ідентифікаторами:

- пошук за прізвищем, іменем, по-батькові;
- пошук за обліковим номером платника податків;
- пошук за інформацією про автотранспорт;
- пошук за соціальними мережами;
- пошук за номером телефону;
- пошук за email;
- пошук за телеграм-акаунтом;

[122] Пошук інформації в базах даних: посіб. / упор. Г. Горбенко. Київ, 2022. С. 177.

- пошук пошти, логіну чи номера телефону за паролем;
- пошук за адресою проживання,
- пошук за кадастровим номером;
- пошук за інформацією про юридичних осіб;
- пошук за інформацією про IP чи домен;
- пошук за інформацією щодо Bitcoin-адреси;
- пошук за фотокарткою людини на сайтах «Facebook», «Вконтакте» та ін.;
- пошук за фотокарткою номера автотранспорту;
- пошук за геолокацією.

Виконання безпосереднього пошуку об'єднує рішення, прийняті на попередніх етапах, та дозволяє отримати результат пошуку за обраними параметрами.

Здебільшого первинними даними для пошуку є:

- ідентифікатори облікових записів (месенджери, соціальні мережі, особисті кабінети на сайтах, email, пароль, логін тощо);
- ідентифікатори предметів (IP-адреса, доменне ім'я, IMEI, номер телефону, назва точки доступу, номер банківської платіжної картки, номери автотранспорту, відомості про нерухоме майно, опис предмета тощо);
- ідентифікатори фізичної особи (прізвище, ім'я, по батькові, дата народження, місце народження, дані документів, прикмети тощо);
- ідентифікатори юридичної особи (назва, ЄДРПОУ, розрахунковий рахунок, контрагенти тощо);
- мультимедійні дані та інші електронні відомості (аудіо-, відеоконтент, зображення, офісні документи, віртуальні образи, банки даних тощо);
- ідентифікатори події (час, місце, тривалість).

У більшості випадків пошук починається саме із введення пошукового запиту в один із доступних пошукових сервісів.

Задля уточнення пошуку за допомогою інформаційно-пошукової системи «Google» рекомендуємо використовувати наведені в таблиці оператори, тобто комбінації слів чи знаків.

Найбільш використовувані комбінації слів чи знаків (оператори мови запитів) під час пошуку у пошуковій системі «Google»	
Оператор	Призначення
AND	Пошук 1, 2 та *n*-го слова (логічне «і» також використовують за замовчуванням під час проставляння пробілів між словами)
OR	Пошук 1 або 2-го слова (логічне «або»)
« »	Пошук точної фрази, укладеної в лапки
+	Виділення головних ключових слів у запиті
–	Виключення небажаних слів у результатах пошукової видачі
~	Включення у видачу синонімів виділеного слова
intitle	Забезпечує пошук за словом, яке міститься у заголовку, наприклад, вводимо у пошукову стрічку intitle: доказування
related	За допомогою цього оператора можна шукати сайти, які пов’язані з конкретним заданим у запиті сайтом, наприклад related:mvs.go.ua
*	За потреби цей знак замінює слово у фразі, наприклад найкращий * у розслідуваннях
filetype	Здійснює пошук за конкретним типом файлу, наприклад під час введення у рядок filetype:pdf доказування будуть відображені лише результати з pdf-файлами
site	Може обмежити пошук межами конкретного сайту, наприклад під час набирання site:rada.gov.ua будуть відображені лише сторінки сайту Верховної Ради України
define	Шукає визначення невідомого слова або поняття, наприклад вводимо у пошукову стрічку define: ДНК

ДОДАТОК 2. БЛАНКИ ПРОЦЕСУАЛЬНИХ ДОКУМЕНТІВ

Слідчому судді

_____

(назва місцевого суду)

_____

КЛОПОТАННЯ
про тимчасовий доступ до речей і документів

ВСТАНОВИВ:

_____

(короткий виклад обставин кримінального правопорушення, у зв'язку з яким подається клопотання; правова

_____

кваліфікація кримінального правопорушення за законом України про кримінальну відповідальність;

_____

перелік речей і документів, тимчасовий доступ до яких планується отримати; підстави вважати, що речі й

_____

документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;

_____

значення речей і документів для встановлення обставин у кримінальному провадженні; можливість

_____

використання як доказів відомостей, що містяться у речах і документах, та неможливість іншими способами

_____

встановити обставини, які передбачається довести за допомогою цих речей і документів, у випадку подання

_____

клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю;

_____

обґрунтування необхідності вилучення речей і документів, якщо відповідне питання порушується сторонами

_____

кримінального провадження)

Беручи до уваги вищевикладене та враховуючи, що в матеріалах кримінального провадження вбачається наявність достатніх підстав вважати, що вказані речі й документи мають суттєве значення для встановлення важливих обставин у кримінальному провадженні, потрібно отримати

_____,

(тимчасовий доступ до речей і документів та (за потреби) можливість їх вилучити)

які перебувають (або можуть перебувати) у володінні

_____,

(прізвище, ім'я, по батькові, дата народження фізичної особи; реквізити юридичної особи)

керуючись ст. 40, 131, 132, 159–164 КПК України,

ПРОШУ:

Надати _____
(тимчасовий доступ до речей і документів та (за потреби) можливість їх вилучення)

_____,
(перелік речей і документів)

що перебувають (або можуть перебувати) у володінні _____

_____
(прізвище, ім'я, по батькові, дата народження фізичної особи; реквізити юридичної особи)

Додатки:

1. _____ на __арк.
(копії матеріалів, якими обґрунтовуються доводи клопотання)

2. Витяг з Єдиного реєстру досудових розслідувань №_____ від «___» _____ 20 __ року.

Слідчий_____
(найменування органу, підпис, прізвище, ініціали)

«ПОГОДЖЕНО»
Прокурор_____
(найменування органу, підпис, прізвище, ініціали)

«___»_____20 ___ року

ПРОТОКОЛ
тимчасового доступу до речей і документів

_____ _____
(місце складання) (дата складання)

Слідчий _____,
(найменування органу, звання, прізвище, ім'я, по батькові)
у період часу з «__» години «__» хвилин до «__» години «__» хвилин у приміщенні _____,
розташованому за адресою: _____,
керуючись ст. 103–107, ст. 165 КПК України, у присутності _____
(особа,

_____
яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей

_____
або документів, із зазначенням її прізвища, імені, по батькові, дати народження та місця мешкання)
за участю понятих, яким роз'яснені вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії: _____
(їх прізвище, імена, по батькові, дати народження та місце проживання, підписи)

_____
_____,

заздалегідь повідомивши учасникам цієї процесуальної дії про застосування технічних засобів фіксації, умови й порядок їх використання:

_____
(характеристики технічних засобів фіксації та носіїв інформації, які застосовуються

_____
під час проведення цієї процесуальної дії, підписи осіб)

_____,
на підставі ухвали слідчого судді _____
(назва місцевого суду, прізвище, ініціали слідчого судді)
від «__» _____ 20__ року про тимчасовий доступ до речей і документів ознайомився із _____
(перелік речей та документів, до яких їх володільцем

_____
фактично надано тимчасовий доступ)

_____

_____

_____

Перед початком цієї процесуальної дії _____

(особа, яка зазначена в ухвалі слідчого

_____

судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів)

пред'явлено оригінал вищезазначеної ухвали суду, вручено її копію та роз'яснено, що відповідно до ст. 166 КПК України у разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями КПК України з метою відшукання та вилучення зазначених речей і документів.

Під час ознайомлення зі змістом документів встановлено _____

_____

(опис речей та документів)

_____

(зазначення про вилучення речей та документів,

_____

якщо на це надано дозвіл в ухвалі суду,

_____

про спосіб їх упакування для надійного збереження із засвідченням

_____

підписами понятих)

Володільцю залишено опис вилучених речей і документів, його копія додається до цього протоколу.

З протоколом ознайомлені: _____

_____

(спосіб ознайомлення учасників зі змістом протоколу,

_____

зауваження і доповнення з боку учасників процесуальної дії;

_____

прізвище,

_____.

ініціали, підпис)

У зв'язку з тим, що особа, яка брала участь у проведенні процесуальної дії _____, відмовилася під-

писати протокол, їй надано право дати письмові пояснення щодо причин відмови від підписання: _____
(пояснення, підпис)

_____

Факт надання (або відмови від надання) письмових пояснень особи щодо причин відмови підписати протокол засвідчується підписом її захисника (законного представника), а у разі його відсутності – понятих: _____
(прізвище, ініціали, підпис)

У зв'язку з тим, що особа через фізичні вади або з інших причин не може особисто підписати протокол, ознайомлення такої особи з протоколом здійснюється у присутності її захисника (законного представника), який своїм підписом засвідчує зміст протоколу та факт неможливості його підписання особою

_____
(прізвище, ініціали, підпис)

Володілець документів: _____
(прізвище, ініціали, підпис)

Поняті: _____
(прізвище, ініціали, підпис)

_____
(прізвище, ініціали, підпис)

Протокол склав:

Слідчий _____
(найменування органу, підпис, прізвище, ініціали)

ПРОТОКОЛ
тимчасового вилучення майна

_____ _____
(місце складання) (дата складання)

Слідчий _____,
(найменування органу, звання, прізвище, ім'я, по батькові)
у період часу з «___» год. «___» хв. до «___» год. «___» хв., у приміщенні (на території) _____
_____,
(місце тимчасового вилучення майна або його передачі)
керуючись ст. 103–107, 167–168 КПК України у присутності осіб, яким роз'яснені вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії: _____
_____
_____
_____,
(їх прізвище, ім'я, по батькові, дата народження та місце проживання, підпис)
яким заздалегідь повідомлено про застосування технічних засобів фіксації, умови та порядок їх використання: _____
(характеристики технічних
_____
засобів фіксації та носіїв інформації, які застосовуються під час проведення цієї процесуальної дії,
_____
підписи осіб)
_____
_____,
тимчасово вилучив майно:
_____
(особа, у якої вилучається або яка передає вилучене майно, послідовність дій, отримані у результаті
_____
процесуальної дії відомості, виявлені та/або надані речі та документи і спосіб їх ідентифікації)
_____
_____.

З протоколом ознайомлені: _____
_____
(спосіб ознайомлення, зауваження і доповнення учасників процесуальної дії; прізвище, ініціали, підпис)
_____
_____

У зв'язку з тим, що особа, яка брала участь у проведенні процесуальної дії _____, відмовилася під-

писати протокол, їй надано право дати письмові пояснення щодо причин відмови від підписання: _____
(пояснення, підпис)
_____.

Факт надання (або відмови від надання) письмових пояснень особи щодо причин відмови підписати протокол засвідчується підписом її захисника (законного представника), а у разі його відсутності – понятих:

_____
(прізвище, ініціали, підпис)

У зв'язку з тим, що особа через фізичні вади або з інших причин не може особисто підписати протокол, ознайомлення такої особи з протоколом здійснюється у присутності її захисника (законного представника), який своїм підписом засвідчує зміст протоколу та факт неможливості його підписання особою: _____
(прізвище, ініціали, підпис)

Особа, у якої
тимчасово вилучено майно: _____
(прізвище, ініціали, підпис)

Поняті: _____
(прізвище, ініціали, підпис)

_____
(прізвище, ініціали, підпис)

Протокол склав:

Слідчий _____
(найменування органу, підпис, прізвище, ініціали)

Додаток до протоколу тимчасового доступу до речей і документів
від «___» _____ ____ року

ОПИС
речей і документів, які були вилучені на підставі ухвали слідчого судді, суду

_____ _____
(місце складання) (дата складання)

Слідчий _____,
(найменування органу, звання, прізвище, ім'я, по батькові)
у приміщенні
_____
за адресою: _____
_____,
на виконання ухвали слідчого судді _____,
провів вилучення таких документів: _____
(опис речей та документів)
_____
_____
_____
_____
_____
_____

Опис склав:

Слідчий_____
(найменування органу, підпис, прізвище, ініціали)

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 джерел 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 підтверджують 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 під час усіх дій, 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 й порядок їх використання: _____.

(підписи осіб)

Здійснюють поетапний опис послідовності дій під час огляду інформації з вебсторінки, з чітким описом інформації, що оглядається, та графічним копіюванням оглянутих вебсторінок. Зазначають також: 1) інформацію про утворений файл з назвою збереженої сторінки із розширенням «HTML» (у разі його створення або відмітка про його відсутність) і папку з назвою, часом її створення і розміром електронних файлів на визначеному носії та відомості про нього, в якій містяться автоматично створені файли цієї сторінки; 2) інформацію про здійснення архівування потрібної сторінки у 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 хешкоду, зазначають 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)

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Академіка Богомольця, 10,
м. Київ, 01601,
тел. 256-12-82, gsu@police.gov.ua
Ідентифікаційний код 40108578

_____ № _____
На № _____ від _____

Голові правління

АТ «А-БАНК»

nbu@bank.gov.ua

Про надання інформації

Управлінням проводяться слідчі (розшукові) дії по матеріалах кримінального провадження № 1202410004000_____ від __.__.2024 відкритого за ознаками кримінального правопорушення, передбаченого ч. _ ст. 190 КК України, за фактом заволодіння грошовими коштами шахрайським шляхом.

Під час проведення слідчих (розшукових) дій встановлено, що до скоєння злочину у цьому провадженні причетні: гр. Іванов Іван Іванович, __.__.____ року народження РНОКПП _____, які (короткий виклад обставин справи) _____.

Під час заходів з'ясовано, що вказаний громадянин є клієнтом Вашого банку, враховуючи викладене, керуючись п. 6 ст. 23, п. 2 ч. 2 ст. 25 Закону України «Про Національну поліцію», ч. 5 ст. 40, ч. 2 ст. 93 КПК України та положенням ст. 62 Закону України «Про банки і банківську діяльність» просимо Вас надати інформацію щодо номера банківського(их) рахунку(ів) **_____,** повідомити, кому належить(ать) зазначений(і) вище банківський(і) рахунок(ки), повідомити, чи проводились транзакції по його рахунку(ах) або картках «А-Банк», у тому числі зняття готівкових коштів, з 01.03.2024 по теперішній час (зазначити дату, час, вид транзакції, суму та місце), а також зазначити номер(и) мобільного(их) телефону(ів), який(і) використовувався(лися) для ідентифікації під час здійснення транзакцій, і місце перебування користувача картки (рахунків).

Відповідь прошу надати у найкоротший термін працівнику поліції, який надав запит.

Начальник **_____**

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Академіка Богомольця, 10,
м. Київ, 01601,
тел. 256-12-82, gsu@police.gov.ua
Ідентифікаційний код 40108578

_____ № _____
На № _____ від _____

Начальникові
Департаменту кіберполіції
Національної поліції України
(звання)_____
(ПІБ)_____

ДОРУЧЕННЯ
оперативному підрозділу
(у порядку статті 40 КПК України)

місто Київ «__»._____. року

Головним слідчим управлінням Національної поліції України здійснюється досудове розслідування у кримінальному провадженні № 8738748349, відомості про яке внесені до Єдиного реєстру досудових розслідувань __.__._____, за ознаками кримінальних правопорушень, передбачених ч. 1, 2 ст. 438 КК України.

Вказане кримінальне провадження зареєстроване за численними фактами порушення законів та звичаїв війни військовослужбовцями збройних сил та інших військових формувань російської федерації _____ у період з __.__.____ по __.__.____.

Під час проведення слідчих дій на території _____ за адресою _____ вилучено ноутбук, на якому виявлено інформацію про підрозділи збройних сил російської федерації, а саме: _____ _____.

Враховуючи викладене, з метою забезпечення проведення повного, всебічного та об'єктивного досудового розслідування, керуючись ст. 39, 40, 41 КПК України,

ПРОШУ:

Доручити підлеглим Вам співробітникам Департаменту кіберполіції Національної поліції України провести аналіз штатного розпису особового складу вказаного полку та встановити:

– повні анкетні дані зазначених військовослужбовців зс рф;

– місця їх проживання;

– паспортні дані;

– сторінки у в соціальних мережах;

– актуальне фото, яке можна використати під час пред'явлення особи для впізнання за фотознімком;

– мобільні номери їх телефонів і близьких родичів;

– іншу інформацію, яка може бути важлива для їх ідентифікації.

Матеріали, отримані у результаті виконання цього доручення, сформувати у вигляді досьє (інформаційної картки на особу) й надіслати до Головного слідчого управління Національної поліції із приміткою для _____.

Додаток:

1. Флеш-носій з електронними файлами штатного розпису.

Старший слідчий в ОВС
ГСУ НП України
(звання) **(ПІБ)**

0XX-XX-XX-XXX

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ГОЛОВНЕ СЛІДЧЕ УПРАВЛІННЯ

вул. Академіка Богомольця, 10,
м. Київ, 01601,
тел. 256-12-82, gsu@police.gov.ua
Ідентифікаційний код 40108578

_____ № _____
На № _____ від _____

Начальникові Департаменту кримінального аналізу Національної поліції України підполковнику поліції (прізвище, ім'я)

01601, м. Київ,
вул. Академіка Богомольця, 10

Про проведення кримінального аналізу

Головним слідчим управлінням Національної поліції здійснюється досудове розслідування у кримінальному провадженні № ХХХХХХХХХ, відомості про яке внесені до Єдиного реєстру досудових розслідувань __.__.____, за ознаками кримінальних правопорушень, передбачених ч. 1 ст. 438, ч. 2 ст. 438 КК України.

Вказане кримінальне провадження зареєстроване за численними фактами порушення законів та звичаїв війни військовослужбовцями збройних сил та інших військових формувань рф на території Бучанської міської територіальної громади Бучанського району Київської області у період з __.__.20__ по __.__.20__.

Під час досудового розслідування було отримано ряд тимчасових доступів до речей і документів, які перебувають у розпорядженні мобільних операторів, та отримано інформацію про фіксування у мережі мобільного зв'язку операторів України на території Київської області мобільних терміналів із SIM-картами рф, а саме: 793ХХХХХХХХ, 795ХХХХХХХХ, 799ХХХХХХХ, 792ХХХХХХХХ, 790ХХХХХХХХ, 798ХХХХХХХХ, 791ХХХХХХХХ, 796ХХХХХХХХ, … .

Вказані абонентські номери попередньо перевірені за допомогою баз даних, які наявні у розпорядженні слідства, результат перевірки відображено у довідці на ___ аркушах, яка додається до вказаного запиту.

Відповідно до наказу Національної поліції України від 29.12.2019 № 1354 «Про затвердження Положення про департамент кримінального аналізу Національної поліції України» одним з основних завдань Департаменту кримінального аналізу є організація та здійснення інформаційно-аналітичної діяльності для реалізації повноважень поліції.

Враховуючи вищевикладене, керуючись ст. 2, 40, 91–93 Кримінального процесуального Кодексу України, для всебічного, повного і неупередженого дослідження обставин кримінального провадження прошу Вас проаналізувати вказані абонентські номери, встановити повні анкетні дані їх власників, адреси проживання, приналежність до збройних сил рф (посада, звання, взвод, рота, батальйон, полк, дивізія), фотознімки належної якості, з можливістю їх використання для пред'явлення для впізнання, контактні телефони та іншу важливу інформацію, яка могла б бути важлива для ідентифікації вказаних осіб.

Також прошу провести огляд відкритих джерел інформації, а саме соціальних мереж «ВКонтакте», «Одноклассники», «Facebook», меседжерів «Viber», «Telegram», «WhatsApp», застосунків «Getcontact», відеохостигу «YouTube» з метою встановлення акаунтів, користувачів вищевказаних абонентських номерів.

Вказана інформація має важливе значення для проведення повного, швидкого та неупередженого досудового розслідування, встановлення всіх обставин вчинення кримінальних правопорушень та винних осіб.

Додаток:

1. Копія довідки про результат перевірки абонентських номерів на __ аркушах.

Слідчий _____

(0XX)-XXX-XX-XX

ПОСТАНОВА

про призначення експертизи

_____ _____
(місце складання) (дата складання)

Слідчий слідчого відділення _____ відділу поліції ГУНП в _____ області _____,
(звання, прізвище, ім'я, по батькові)
розглянувши матеріали кримінального провадження № _____,
за ознаками _____,
(правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) КК України)

ВСТАНОВИВ:

_____
(зміст обставин, які є підставами для прийняття постанови;

_____
мотиви прийняття постанови, їх обґрунтування)

_____

Враховуючи, що для з'ясування обставин, що мають значення для кримінального провадження, потрібні спеціальні знання, керуючись ст. 110, 242, 243 КПК України,

ПОСТАНОВИВ:

1. Призначити _____ експертизу,
(найменування експертизи)
до проведення якої залучити _____.
2. На вирішення експерта поставити такі питання:_____.
_____.
3. Для дослідження експерту надати: _____.
_____.
4. Для ознайомлення експерту надати:_____.
_____.
5. Копію постанови направити _____.

Слідчий_____.
(найменування органу, підпис, прізвище, ініціали)

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахтирська Н. М. Одержання доказів в електронній формі в світлі Другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 188–200. DOI: https://doi.org/10.33994/kndise.2022.67.21.

2. 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. *Науковий вісник університету Короля Данила*. 2024. Вип. 17 (29). С. 227–243.

3. Брендель О. І. Засоби прихованого відеоспостереження та особливості їх використання в процесі розслідування злочинів і експертного дослідження. *Теорія і практика судової експертизи і криміналістики*. 2016. Вип. 16. С. 240.

4. 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.

5. Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рек. / М. В. Гуцалюк та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.

6. Волков О. О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: дис. … канд. юрид. наук: 12.00.09. Дніпро: Дніпропетров. держ. ун-т внутр. справ. 2023. С. 197.

7. Головкін Б. М., Денькович О. І. , Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази: навч. посіб. / за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле 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 (дата звернення: 11.04.2024).

8. Господарський процесуальний кодекс України: Закон України від 06.11.1991 р. № 1798-XII. *Відомості Верховної Ради України.* 1992. № 6. Ст. 56. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (дата звернення: 05.03.2024).

9. Експертиза відео-, звукозапису. URL: https://kndise.gov.ua/video-zvukozapysu (дата звернення: 05.03.2024).

10. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: моногр. 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. С. 433.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 09.03.2024).

12. Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: методичні рек. / С. С. Чернявський, В. І. Присяжний, О. М. Стрільців та ін.; за заг. ред. М. С. Цуцкіридзе. Київ: Нац. акад. внутр. справ, 2023. 92 с.

13. Заяць К. Д. Методика розслідування шахрайств: дис. ... канд. юрид. наук: 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. С. 76.

14. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: затв. наказом МВС України від 07.07.2017 р. № 575. URL: https://zakon.rada. gov.ua/laws/show/z0937-17#Text (дата звернення: 09.03.2024).

15. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 11.04.2024).

16. Інформаційні системи та технології: підруч. / за заг. ред. д-ра техн. наук, проф. В. Б. Вишні. Дніпро: Дніпропетр. держ. ун-т внутр. справ, 2021. С. 242–243.

17. Кобець М. В. Установлення місцезнаходження радіообладнання (радіоелектронного засобу) як метод слідчої (розшукової) дії та оперативно-розшукового заходу з розшуку осіб. *Актуальні питання та перспективи розшукової роботи в діяльності підрозділів кримінальної поліції*: матеріали міжвідомч. наук.-практ. круглого столу (Київ, 28 берез. 2024 р.). С. 74–78. URL: https://elar.naiau.kiev.ua/items/4ae4967b-a13d-48b3-89c7-a2472369592b (дата звернення: 11.05.2024).

18. Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. DOI : 10.21564/2414- 990X.161.278117.

19. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України*. 2017. № 1 (88). С. 182–191.

20. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 р. № 2747-IV. *Відомості Верховної Ради України*. 2005. № 35–36, 37. Ст. 446. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 01.02.2024).

21. Комп'ютерно-технічна експертиза. URL: https://kndise.gov.ua/kompyuterno-tehnichna/ (дата звернення: 11.04.2024).

22. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 01.02.2024).

23. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 01.02.2024).

24. Копія та дублікат службового документа: ВС розбирався, чи є між ними різниця. URL: https://sud.ua/ru/news/sudebnaya-praktika/208995-kopiya-ta-dublikat-sluzhbovogo-dokumenta-vs-rozbiravsya-chi-ye-mizh-nimi-riznitsya (дата звернення: 21.05.2024).

25. Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. *Інформаційні технології та захист інформації*: зб. наук. пр. Запоріжжя, 1998. С. 70–79.

26. Криміналістика: криміналістична техніка: навч. посіб. / Р. Л. Степанюк та ін.; МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2023. С. 124.

27. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 18.02.2024).

28. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.04.2024).

29. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: кол. моногр. / А. В. Гутник, А. Я. Хитра. Львів: ЛьвДУВС, 2022. 204 с.

30. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф. Харків, 2020. С. 44. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content (дата звернення: 19.04.2024).

31. Лісовий В. В. Огляд місця події при розслідуванні «комп'ютерних» злочинів. *Право України*. 2001. № 1. С. 52–54.

32. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал*. 2014. № 4. С. 202–205. URL: http://www.lsej.org.ua/4_2014/53.pdf (дата звернення: 11.04.2024).

33. Малій М. І. Особа комп'ютерного злочинця як об'єкт криміналогічного дослідження: дис. … д-ра філос.: 081 / Хмельницьк. ун-т управління та права ім. Леоніда Юзькова. Хмельницький, 2022. С. 120.

34. Надія Стефанів. Суддя Верховного Суду. Судова практика ККС Верховного Суду щодо допустимості електронних доказів. С. 12. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf (дата звернення: 19.05.2024).

35. Науково-методичні рекомендації з питань підготовки і призначення судових експертиз та експертних досліджень: затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5, зареєстр. у М-ві юстиції України 03.11.1998 р. за № 705/3145 (у редакції наказу М-ва юстиції України від 26.12.2012 р. № 1950/5). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.04.2024).

36. Особливості призначення та можливості судової комп'ютерно-технічної експертизи: інформац. лист. Київ. наук.-досл. експертно-криміналіст. центр. URL: https://ndekc.kiev.ua (дата звернення: 19.04.2024).

37. Особливості призначення та можливості судової фототехнічної експертизи: інформаційний лист / Київський науково-дослідний експертно-криміналістичний центр. Київ, 2023. URL: https://ndekc.kiev.ua (дата звернення: 19.04.2024).

38. Оцінювання цифрових зображень з відкритих джерел: Посібник для суддів та дослідників фактів (2024), опублікований онлайн на сайті, 2024. С. 16.URL: https://www. trueproject.co.uk/osguide

39. Посилена співпраця та розкриття електронних доказів: 22 країни підписали новий Протокол до Конвенції про кіберзлочинність. *Офіс Ради Європи в Україні*: офіційний сайт (12 трав. 2022 р.). URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-

disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention (дата звернення: 16.05.2024).

40. Постанова Верховного Суду від 03.11.2020 р. у справі № 419/2016/19 (провадження № 51-2950км20). URL: https://reyestr.court.gov.ua/Review/92765503 (дата звернення: 22.04.2024).

41. Постанова Верховного Суду від 07.10.2020 р. у справі № 725/1199/19 (провадження № 51-5720км19). URL: https://reyestr.court.gov.ua/Review/92173671 (дата звернення: 19.04.2024).

42. Постанова Верховного Суду від 10.09.2019 р. у справі № 761/8589/15-к (провадження № 51-4571км18). URL: https://reyestr.court.gov.ua/Review/84229858 (дата звернення: 06.07.2024).

43. Пошук інформації в базах даних: посібник / упоряд. Г. Горбенко. Київ, 2022. С. 177.

44. Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 28.06.2024).

45. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 15.02.2024).

46. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 28.06.2024).

47. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII (станом на 01.01.2024 р.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 29.04.2024).

48. Про захист прав споживачів: Закон України від 12.05.1991 р. № 1023-XII. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text (дата звернення: 28.06.2024).

49. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-15. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 28.06.2024).

50. 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-ProtocolUkrainian.pdf (дата звернення: 28.06.2024).

51. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навч.-метод. посіб. Одеса, 2020. С. 11.

52. 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.pd (дата звернення: 28.06.2024).

53. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (дата звернення: 28.06.2024).

54. Тетерятник Г. К., Виходець Ю. О. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з Інтернет-джерел. *Юридичний науковий електронний журнал*. 2022. № 10. С. 773.

55. ТОП-7 хмарних сховищ. URL: https://gigacloud.ua/blog/navchannja/top-7-hmarnih-shovisch (дата звернення: 25.06.2024).

56. Україна приєдналася до додаткового протоколу до Конвенції про кіберзлочинність. *Я і закон*: інформаційно-юридичний сайт (02 груд. 2022 р.). URL: https://yaizakon.com.ua/ukrayina-priyednalasya-do-dodatkovogo-protokolu-do-konventsiyi-pro-kiberzlochinnist/ (дата звернення: 28.05.2024).

57. Фототехнічна експертиза. URL: https://kndise.gov.ua/fototehnichna/ (дата звернення: 28.06.2024).

58. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони*. 2017. № 4 (58). С. 83. (Серія «Право»).

59. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40–41, 42. Ст. 492. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 11.01.2024).

60. Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Методика розслідування шахрайства в інтернет-комерції: теорія та практика: монографія. Одеса: Вид-во «Юридика», 2024. С. 55–56.

61. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп’ютерних злочинів: посібник / МВС України; Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2010. 12 с.

62. Юзишина Т. В. Проблематика проведення судово-почеркознавчої експертизи при ідентифікаційному дослідженні почерку та підписів в електронних документах. *Експерт: парадигми юридичних наук і державного управління*. 2023. № 1 (25). С. 56–61. URL: https://doi.org/10.32689/2617-9660-2023-1(25)-56-61 (дата звернення: 28.06.2024).

63. Icove D., Seger K., Von Sorsh W. Computer Crime: A Crime fighter's Handbook / O'Reylli &Associates, Ins., 1995. 437 p.

64. GPS: що це, і який принцип роботи. URL: https://gpsuaservice.com.ua/gps-shcho-tse-i-yakyi-pryntsyp-roboty/ (дата звернення: 04.08.2024).

65. OBTAINING CROSS-BORDER ELECTRONIC EVIDENCE SECTION 1: INVESTIGATIVE TECHNIQUES. This e-Learning course was created as part of INTERPOL's Cyber Capabilities and Capacity Development Project (C3DP), funded by the United States Department of State – Bureau of International Narcotics and Law Enforcement (INL). The e-Learning course was jointly developedwith the National White Collar Crime Center (NW3C). ©2023.

66. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: https://rm.coe.int/1680a49dab (Last accessed: 15.05.2024).

67. SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition Version: 1.2 (September 17, 2020).

Авторський колектив

Шевчишен А. В. – заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, доктор юридичних наук, професор, заслужений юрист України.

Гаврилюк Л. В. – провідний науковий співробітник науково-дослідної лабораторії проблем правового та організаційного забезпечення діяльності Міністерства ДНДІ МВС України, кандидат юридичних наук, старший дослідник.

Ангеленюк А.-М. Ю. – старший науковий співробітник науково-дослідної лабораторії проблем правового та організаційного забезпечення діяльності Міністерства ДНДІ МВС України, кандидат юридичних наук, старший дослідник.

Дрозд В. Г. – начальник консультативно-контрольного відділу Департаменту забезпечення діяльності Голови Національної поліції України, доктор юридичних наук, професор, заслужений юрист України.

Бурлака В. В. – начальник 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, кандидат юридичних наук.

Подиряко Х. В. – начальник управління організації розслідування злочинів, учинених в умовах збройного конфлікту Головного слідчого управління Національної поліції України, полковник поліції.

Пелехатий В. Т. – старший слідчий в ОВС 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України.

Віткалова А. Є. – старший слідчий в ОВС 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України.

Калантай І. М. – начальник 2-го відділу (організації розслідування злочинів, учинених на тимчасово окупованих територіях) управління організації розслідування злочинів, учинених в умовах збройного конфлікту Головного слідчого управління Національної поліції України.

Дулкай І. І. – старший слідчий в ОВС 1-го відділу (розслідування злочинів, учинених в умовах збройного конфлікту) управління організації розслідування злочинів, учинених в умовах збройного конфлікту Головного слідчого управління Національної поліції України.

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Навчальне видання

Шевчишен Артем Вікторович
Гаврилюк Людмила Володимирівна
Ангеленюк Анна-Марія Юріївна
Дрозд Валентина Георгіївна
Бурлака Владислав Васильович
Подиряко Христина Віталіївна
Пелехатий Віталій Тадейович
Віткалова Аліна Євгенівна
Калантай Ігор Миколайович
Дулкай Іван Іванович

ЗБИРАННЯ ТА ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Методичні рекомендації

Коректура *Наталії Мурашової*
Комп'ютерне верстання *Марини Марченко*

В оформленні обкладинки використовуються ілюстрації:
ідентифікатор стокового матеріалу 2485793717
(URL https://www.shutterstock.com/image-vector/abstract-cloud-technology-circuit-board-large-2485793717),
ідентифікатор стокового матеріалу 2318895125
(URL https://www.shutterstock.com/image-vector/isometric-smart-technology-circuit-connected-cloud-2318895125).

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 25.04.2025. Формат $60\times84^{1}/_{16}$. Папір офс. Гарнітура Arial.
Спосіб друку – електрографічний. Ум. друк. арк. 9,69. Обл.-вид. арк. 7,79.
Поз. 25-2-3-001. Наклад 57 пр. Зам. № 25-032.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
03056, м. Київ
тел. (044) 204-81-78