Посольство Великої Британії в Україні

Міністерство внутрішніх справ України

ОБСЄ Організація з безпеки та співробітництва в Європі
**Координатор проектів в Україні**

Global Affairs Canada
Affaires mondiales Canada

НАВЧАЛЬНИЙ КУРС

# З ВИЯВЛЕННЯ, ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНИЙ КУРС

# З ВИЯВЛЕННЯ, ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**ISBN**

**Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. – 148 с.**

Навчальний курс з виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій, підготовлений до апробації з метою його подальшого використання у навчальному процесі під час підготовки курсантів вищих навчальних закладів МВС України та підвищення кваліфікації діючих працівників ОВС щодо протидії торгівлі людьми та кіберзлочинності.

Навчальний курс та матеріали методичного посібника будуть також корисними для підвищення кваліфікації прокурорів та суддів.

Global Affairs Canada Affaires mondiales Canada

ОБСЄ Організація з безпеки та співробітництва в Європі
**Координатор проектів в Україні**

Опубліковано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», який впроваджується за фінансової підтримки Уряду Канади, наданої через Департамент закордонних справ, торгівлі і розвитку.

*Україна, 01030, Київ*
*вул. Стрілецька, 16*
*www.osce.org/ukraine*

# ЗМІСТ

# ВСТУП

Даний навчальний курс містить основні відомості, необхідні для виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (ІТ). Курс призначено для працівників правоохоронних органів.

У даній роботі основну увагу приділено підвищенню рівня загального розуміння зв'язків між торгівлею людьми, інформаційними технологіями та кіберзлочинністю і визначенню шляхів взаємодії у виявленні, попередженні та розслідуванні таких злочинів.

Курс поділено на модул, у кожному з яких розглядаються окремі аспекти застосування тих чи інших технологій під час здійснення злочинної діяльності, наводяться приклади, а також способи документування протиправних дій і встановлення особи злочинця. Наприкінці курсу наведено комплексну вправу для відпрацювання засвоєного матеріалу.

Для ефективного засвоєння курсу слухач повинен мати базові знання у сфері комп'ютерних технологій та розуміти сучасні форми і методи торгівлі людьми.

**МОДУЛЬ 1**

# ЗАГАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ТОРГІВЛІ ЛЮДЬМИ

## 1. ТОРГІВЛЯ ЛЮДЬМИ ТА ГОЛОВНІ ТЕНДЕНЦІЇ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЦІЙ СФЕРІ

Торгівля людьми – це сучасна форма рабства. Вона розглядає людей як товар, який можна продавати і купувати. Жертви торгівлі людьми експлуатуються для виконання примусової праці, особливо у секс-індустрії, за мізерну зарплатню або й взагалі безоплатно. Торгівля людьми підриває основоположні цінності, такі як права людини, гідність, демократія та верховенство права.

У цій сфері існує кілька міжнародних угод і документів, присвячених захисту жертв торгівлі людьми та їхніх прав. Ретроспективний аналіз їх імплементації в українське законодавство дозволяє виділити такі основні віхи:

- 1991 – Ратифікація Конвенції ООН про права дитини від 20 листопада 1989 року.
- 2004 – Ратифікація Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності від 15 листопада 2000 року.
- 2010 – Ратифікація Конвенції РЄ про заходи щодо протидії торгівлі людьми від 16 травня 2005 року.
- 2012 – Ратифікація Конвенції Ради Європи про захист дітей від сексуальної експлуатації і сексуального насильства (Лансаротська Конвенція) від 25 жовтня 2007 року.

Згідно зі ст. 4 Конвенції Ради Європи «Про заходи щодо протидії торгівлі людьми» від 16 травня 2005 р. [1] *«торгівля людьми»* означає найм, перевезення, передачу, приховування або одержання осіб шляхом погрози або застосування сили чи інших форм примусу, насильницького викрадення, шахрайства, обману, зловживання владою або безпорадним станом або наданням чи отриманням плати чи вигоди для досягнення згоди особи, яка має владу над іншою особою, для експлуатації. Експлуатація включає в себе, принаймні, експлуатацію проституції інших осіб чи інші форми сексуальної експлуатації, примусову працю чи послуги, рабство чи подібну до рабства практику, поневолення або вилучення органів.

Використання інформаційних технологій у торгівлі людьми спричинило включення до даної конвенції визначення, згідно з яким поняття вербування не залежить від засобів, яким його здійснено (через Інтернет, засоби масової інформації або усно).

Ще однією міжнародною конвенцією, яка стосується питань протидії торгівлі людьми є Конвенція «Про кіберзлочинність» [2]. Україна залишила за собою право не застосовувати повністю підпункти статті 9 цієї Конвенції, які стосуються встановлення кримінальної відповідальності за здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи, а також за володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

+

Окремі норми Конвенції «Про кіберзлочинність» спрямовані на здійснення заходів, які б забезпечували збереження файлів протоколів провайдерів та операторів телекомунікаційних послуг (ст. 16) та встановлення повноважень компетентних органів щодо отримання такої інформації (ст. 18), а також здійснення окремих слідчих (розшукових) дій (обшук і арешт комп'ютерних даних, які зберігаються) та оперативно-розшукових або негласних слідчих (розшукових) дій (збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації).

Важливою нормою Конвенції «Про кіберзлочинність» (ч. 1-2 ст. 31) є право її учасників «на здійснення без дозволу іншої сторони доступу до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи».

На сьогодні в нашій державі діє Закон України «Про протидію торгівлі людьми» від 20.09.2011, яким визначено організаційно-правові засади протидії торгівлі людьми, повноваження органів державної влади та місцевого самоврядування, а також правовий статус осіб, які постраждали від зазначеного кримінального правопорушення.

Постановою Кабінету Міністрів України від 22.08.2012 № 783, із змінами, внесеними згідно з Постановою Кабінету Міністрів України від 13.07.2016 № 437, затверджено «Порядок взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми». Цей Порядок визначає механізм взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми, процедуру здійснення ними заходів щодо надання допомоги та захисту осіб, які постраждали від торгівлі людьми.

Окрім того, з метою запобігання торгівлі людьми, підвищення ефективності переслідування осіб, які вчиняють пов'язані з нею злочини або сприяють їх вчиненню, а також захисту прав осіб, що постраждали від торгівлі людьми, постановою Кабінету Міністрів України від 24.02.2016 № 111 затверджено Державну цільову соціальну програму протидії торгівлі людьми на період до 2020 року.

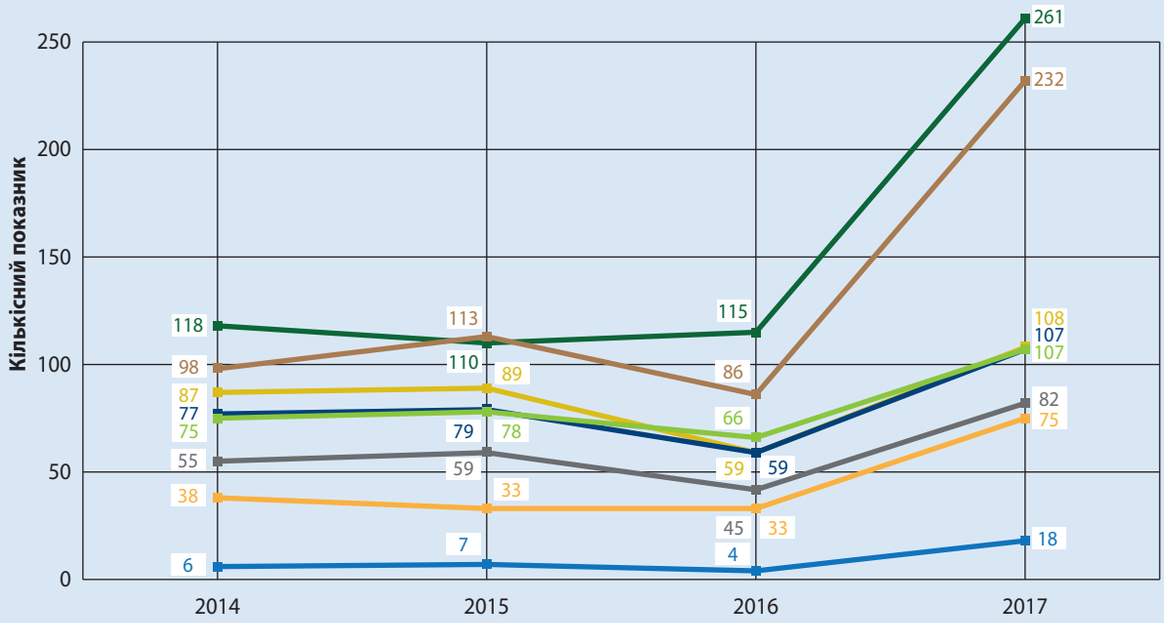
У Кримінальному кодексі (КК) України [3] передбачено *відповідальність* за торгівлю людьми згідно зі ст. 149 «Торгівля людьми або інша незаконна угода щодо людини». Останні зміни до описаної норми КК було внесено у 2006 році. Це було зроблено з метою приведення національного законодавства України у відповідність до міжнародних стандартів у сфері протидії торгівлі людьми.

ЗА 9 МІСЯЦІВ 2017 РОКУ КІЛЬКІСТЬ ОБЛІКОВАНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЗА СТ. 149 КК УКРАЇНИ (ТОРГІВЛЯ ЛЮДЬМИ) ЗРОСЛА ДО 261-ГО, У ТОЙ ЧАС КОЛИ В 2016 РОЦІ ЦЕЙ ПОКАЗНИК ДОРІВНЮВАВ 115-ТИ. ОТЖЕ, КІЛЬКІСТЬ ВИЯВЛЕНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ, ПОРІВНЯНО З МИНУЛИМ РОКОМ ЗБІЛЬШИЛАСЬ НА 127 % (146).

ПРИ ЦЬОМУ, ОБВИНУВАЛЬНІ АКТИ В 108-МИ ПРОВАДЖЕННЯХ НАПРАВЛЕНІ ДО СУДУ, ЩО НА 1,8 РАЗИ ПЕРЕВИЩУЄ РІВЕНЬ 2016 РОКУ ПО ДАНОМУ КРИТЕРІЮ. У 107-МИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ ОСОБАМ ВРУЧЕНО ПОВІДОМЛЕННЯ ПРО ПІДОЗРУ ПРОТЯГОМ СІЧНЯ-ВЕРЕСНЯ 2017 РОКУ (А В 2016 РОЦІ ВІДПОВІДНО – 59, 2015 – 79). НАЙБІЛЬШ УРАЗЛИВИМИ ВІД ДАНОЇ КАТЕГОРІЇ ПРАВОПОРУШЕНЬ В 2017 РОЦІ ВИЯВИЛИСЬ ЖІНКИ З ПОКАЗНИКОМ – 107-М ЖЕРТВ, ТА ДІТИ – 18-ТЬ, ПРИ ЗАГАЛЬНІЙ КІЛЬКОСТІ ПОТЕРПІЛИХ В 232-ВІ ОСОБИ, ПРОТИ 86-ТИ В 2016 РОЦІ.

ДИНАМІКИ ЗРОСТАННЯ ПОКАЗНИКІВ СТАНУ РЕЄСТРАЦІЇ ТА РОЗСЛІДУВАННЯ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЗА ФАКТАМИ ТОРГІВЛІ ЛЮДЬМИ В 2017 РОЦІ ПОРІВНЯНО З 2016, 2015, 2014 ПРОІЛЮСТРОВАНА В ГРАФІКУ №1.

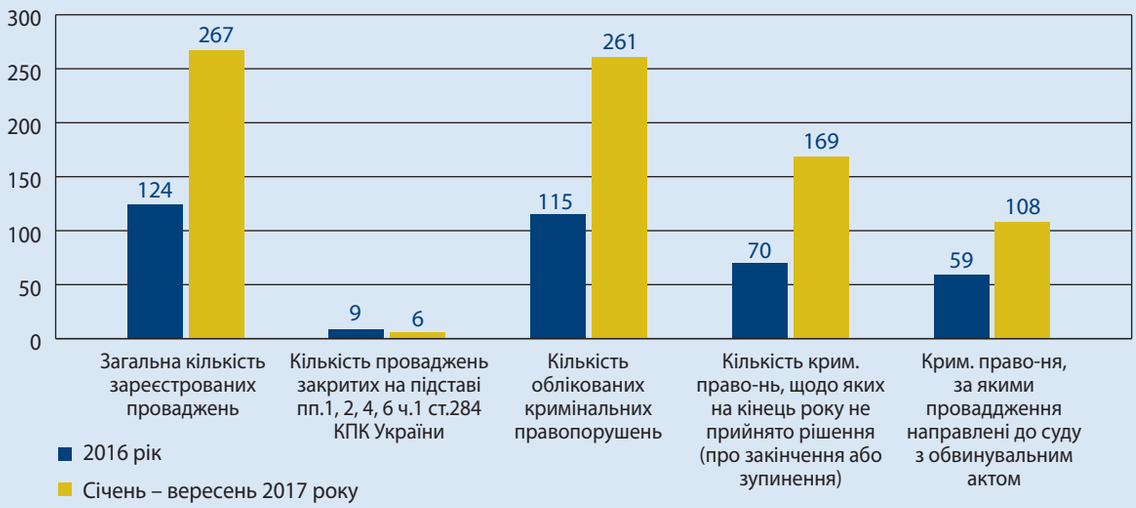
***ГРАФІК № 1.***




- Кількість облікованих кримінальних правопорушень.
- Кількість правопорушень, з числа облікованих протягом звітного періоду, в яких обвинувальні акти направлені до суду.
- Кількість правопорушень, у яких особам вручено повідомлення про підозру.
- Кількість потерпілих осіб.
- Кількість потерпілих жінок.
- Кількість потерпілих дітей.
- Кількість правопорушень, у яких обвинувальні акти направлені до суду (з урахуванням проваджень минулих років).
- За закінченими розслідуваннями, з урахуванням минулих років, виявлено осіб, які вчинили злочини.

ДОСУДОВЕ РОЗСЛІДУВАННЯ ЗАКІНЧЕНО ЗА 108-МИ КРИМІНАЛЬНИМИ ПРОВАДЖЕННЯМИ ЦІЄЇ КАТЕГОРІЇ (ПРОТИ 59-ТИ У 2016 РОЦІ), МАТЕРІАЛИ ЯКИХ НАПРАВЛЕНІ ДО СУДУ З ОБВИНУВАЛЬНИМ АКТОМ, ХОЧА ПРИ ЦЬОМУ В 169-ТИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ НА КІНЕЦЬ ЗВІТНОГО ПЕРІОДУ НЕ ПРИЙНЯТО РІШЕННЯ ПРО ЗАКІНЧЕННЯ АБО ЗУПИНЕННЯ ПРОВАДЖЕННЯ, У 2016 РОЦІ ЦЯ ЦИФРА ДОРІВНЮВАЛА 70-ТИ.

***ГРАФІК № 2.*** *ДАНІ ЩОДО КІЛЬКОСТІ ЗАРЕЄСТРОВАНИХ ТА РОЗСЛІДУВАНИХ УПРОДОВЖ 2016 РОКУ ТА СІЧНЯ-ВЕРЕСНЯ 2017 РОКУ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ (ПРОВАДЖЕНЬ) ЗА СТ. 149 КК УКРАЇНИ*



ЩОДО РЕЗУЛЬТАТИВНОСТІ ДОСУДОВОГО СЛІДСТВА ТА СУДОВОГО РОЗГЛЯДУ ПО СПРАВАХ ЩОДО ТОРГІВЛІ ЛЮДЬМИ, ТО ЗА 9 МІСЯЦІВ 2017 РОКУ 62-ВІ ОСОБИ ПРИТЯГНУТО ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ, А 8-М ОСІБ ЗАСУДЖЕНО ДО ПОЗБАВЛЕННЯ ВОЛІ НА ПЕВНИЙ СТРОК. НА ПІДСТАВІ ПП. 1, 2 СТ. 284 КПК УКРАЇНИ ЗАКРИТО 26 КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ, ПРОТИ 17-ТИ В 2016 РОЦІ.

***ГРАФІК №3.*** *ДАНІ ЩОДО РЕЗУЛЬТАТІВ ДОСУДОВОГО СЛІДСТВА ОРГАНАМИ ПОЛІЦІЇ ТА СУДОВОГО РОЗГЛЯДУ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ, ПЕРЕДБАЧЕНИХ СТ. 149 КК УКРАЇНИ УПРОДОВЖ 2016-2017 РОКІВ.*


ЯК ВИСНОВОК, НАЙБІЛЬШ ВРАЖЕНІ РЕГІОНИ УКРАЇНИ ВІД ТОРГІВЛІ ЛЮДЬМИ: ВІННИЦЬКА, ДОНЕЦЬКА, ЖИТОМИРСЬКА, ЗАКАРПАТСЬКА, ІВАНО-ФРАНКІВСЬКА, ЛУГАНСЬКА, МИКОЛАЇВСЬКА, СУМСЬКА, ТЕРНОПІЛЬСЬКА, ЧЕРНІВЕЦЬКА, ЧЕРНІГІВСЬКА ОБЛАСТІ.

ОСНОВНИМИ КРАЇНАМИ ПРИЗНАЧЕННЯ «ЖИВОГО ТОВАРУ» Є: РОСІЙСЬКА ФЕДЕРАЦІЯ, ПОЛЬЩА, ТУРЕЧЧИНА, УКРАЇНА, НІМЕЧЧИНА, ІЗРАЇЛЬ, ГРЕЦІЯ, ОБ'ЄДНАНІ АРАБСЬКІ ЕМІРАТИ.

У коментарі до Кримінального кодексу України [4, с. 342-349] відзначається, що ст. 149 КК України визначає кримінально караною торгівлю людьми або здійснення іншої незаконної угоди, об’єктом якої є людина, а так само вербування, переміщення, переховування, передача або одержання людини, вчинені з метою експлуатації, з використанням обману, шантажу чи уразливого стану особи.

Крім того, приміткою до ст. 149 КК України встановлено, що відповідальність за вербування, переміщення, переховування, передачу або одержання малолітнього чи неповнолітнього за цією статтею має наставати незалежно від того, чи вчинені такі дії з використанням обману, шантажу чи уразливого стану зазначених осіб або із застосуванням чи погрозою застосування насильства, використання службового становища, або особою, від якої потерпілий був у матеріальній чи іншій залежності.

Основним безпосереднім об’єктом цього злочину є честь і гідність особи, а також – крім випадків, коли угода, об’єктом якої є людина, укладається за згодою цієї ж людини, – воля особи. Його додатковим факультативним об’єктом можуть виступати життя та здоров’я особи, встановлений порядок здійснення службовими особами своїх повноважень.

Об’єктивна сторона цього злочину виражається у таких формах, як:

1) торгівля людьми;

2) здійснення іншої незаконної угоди, об’єктом якої є людина;

3) вербування людини;

4) переміщення людини;

5) переховування людини;

6) передача людини;

7) одержання людини.

**1.** Поняття **торгівля людьми** у Протоколі про запобігання та припинення торгівлі людьми, особливо жінками і дітьми, та покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності, а так само і в інших актах міжнародного законодавства, які є чинними і для України, означає **«здійснювані з метою експлуатації вербування, перевезення, передачу, приховування або одержання людей»**, які вчинюються певними способами.

Той факт, що український законодавець, на відміну від міжнародних актів, торгівлю людьми виділив як окрему форму злочину, відмінну від таких його форм, як вербування, перевезення (переміщення), передача, переховування або одержання людини, означає, що у ст. 149 КК України під торгівлею людьми слід розуміти власне торгівлю, тобто вчинення актів купівлі-продажу людей.

НА ПОЧАТКУ СЕРПНЯ 2012 РОКУ ОБВИНУВАЧЕНИЙ УМИСНО ВСТУПИВ В ЗЛОЧИННУ ЗМОВУ ЗІ СВОЄЮ СПІВМЕШКАНКОЮ ПРО ПРОДАЖ ЇЇ МАЛОЛІТНЬОГО СИНА. РЕАЛІЗУЮЧИ СВІЙ ЗЛОЧИННИЙ НАМІР ПО ПРОДАЖУ ДИТИНИ, ЗЛОЧИНЦІ ПЕРЕСЛІДУЮЧИ КОРИСНИЙ МОТИВ ТА МЕТУ ОСОБИСТОГО ЗБАГАЧЕННЯ, УМИСНО, ЗА ГРОШОВУ ВИНАГОРОДУ В СУМІ 30 000 ГРИВЕНЬ ПРОДАЛИ СТОРОННІЙ ЇМ ОСОБІ МАЛОЛІТНЬОГО 13.01.2007 РОКУ НАРОДЖЕННЯ.

РОЗГЛЯДАЮЧИ СПРАВУ ПО СУТІ СУД, ДІЙШОВ ВИСНОВКУ, ЩО ДІЇ ОБВИНУВАЧЕНИХ СЛІД КВАЛІФІКУВАТИ ЗА Ч. 3 СТ. 149 КК УКРАЇНИ, ЯК ТОРГІВЛЯ ЛЮДЬМИ, КВАЛІФІКУЮЧИМИ ОЗНАКАМИ ЯКОЇ Є: ТОРГІВЛЯ ЛЮДЬМИ ВЧИНЕНА ЗА ПОПЕРЕДНЬОЮ ЗМОВОЮ ГРУПОЮ ОСІБ ТА ВЧИНЕНА ЩОДО МАЛОЛІТНЬОГО [5].

### 2. Здійснення іншої незаконної угоди, об'єктом якої є людина

ПРИКЛАДОМ ЦІЄЇ ФОРМИ ОБ'ЄКТИВНОЇ СТОРОНИ ТОРГІВЛІ ЛЮДЬМИ Є ЗЛОЧИННІ ДІЇ ГРОМАДЯНКИ С., ЯКА У 2002 РОЦІ УМИСНО, З КОРИСЛИВИХ СПОНУКАНЬ, ПІД ПРИВОДОМ ПРАЦЕВЛАШТУВАННЯ НА РИНКАХ М. МОСКВИ, ПІДШУКУВАЛА В УКРАЇНІ ЖІНОК ДЛЯ ЗАЙНЯТТЯ ПРОСТИТУЦІЄЮ. З ЦІЄЮ МЕТОЮ ВОНА ПЕРЕВЕЗЛА ЧОТИРЬОХ ЖІНОК ДО М. МОСКВИ ТА ПЕРЕДАЛА ЇХ НЕВСТАНОВЛЕНІЙ ОСОБІ В РАХУНОК ПОГАШЕННЯ ЇЇ БОРГУ [6].

### 3. Вербування людини

З ВИРОКУ БОРИСПІЛЬСЬКОГО МІСЬКРАЙОННОГО СУДУ КИЇВСЬКОЇ ОБЛАСТІ ВІД 17.02.2014: «КОЛИ НА ЗАЗНАЧЕНИЙ У ОГОЛОШЕННІ АБОНЕНТСЬКИЙ НОМЕР МОБІЛЬНОГО ТЕЛЕФОНУ НАДХОДИВ ДЗВІНОК, ПІДОЗРЮВАНА ПОЧИНАЛА ПРОВОДИТИ ВЕРБУВАННЯ ОСОБИ, ЯКА ТЕЛЕФОНУЄ. СПЕРШУ СПІЛКУВАННЯ ВЕЛОСЯ ТІЛЬКИ ПО ТЕЛЕФОНУ. ПІСЛЯ ТОГО, ЯК ПІДОЗРЮВАНА ПЕРЕКОНУВАЛАСЯ У БЕЗПЕЦІ ВЕРБУВАННЯ ПОТЕРПІЛОЇ, ВОНА ПРИЗНАЧАЛА ЗУСТРІЧ НА ЯКУ ПРИХОДИЛА З СПІВУЧАСНИКОМ. НА ЗУСТРІЧ ВОНИ ВІДПРАЦЬОВАНІЙ МІЖ НИМИ СХЕМІ, ДОПОВНЮЮЧИ ОДИН ОДНОГО ПОЧИНАЛИ ПОСТУПОВО ЗДІЙСНЮВАТИ ПСИХОЛОГІЧНИЙ ТИСК НА ПОТЕРПІЛУ, З МЕТОЮ СХИЛИТИ ЇЇ ПОЇХАТИ НА ЇХ УМОВАХ ЗА КОРДОН ДЛЯ РОБОТИ ПО НАДАННЮ СЕКСУАЛЬНИХ ПОСЛУГ ЗА ГРОШОВУ ВИНАГОРОДУ. ВИКОРИСТОВУЮЧИ, ЯК ПРАВИЛО, СКРУТНЕ МАТЕРІАЛЬНЕ СТАНОВИЩЕ ЖІНКИ, ЯКУ ВЕРБУВАЛИ, НЕМОЖЛИВІСТЮ ПОТЕРПІЛОЇ ПРАЦЕВЛАШТУВАТИСЬ, ВОНИ ОБІЦЯЛИ ЗА КОРОТКИЙ СТРОК ВЕЛИКІ ПРИБУТКИ В ІНОЗЕМНІЙ ВАЛЮТІ» [7].

З ВИРОКУ ПРИМОРСЬКОГО РАЙОННОГО СУДУ М. ОДЕСИ ВІД 06 ВЕРЕСНЯ 2016 РОКУ: «ПІДОЗРЮВАНА В ГРУДНІ 2015 РОКУ В ХОДІ ТЕЛЕФОННОЇ РОЗМОВИ З ПОТЕРПІЛОЮ, ПЕРЕСЛІДУЮЧИ ЗЛОЧИННИЙ НАМІР, НАПРАВЛЕНИЙ НА ВЕРБУВАННЯ ЛЮДИНИ З МЕТОЮ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ З ВИКОРИСТАННЯМ ЇЇ УРАЗЛИВОГО СТАНУ, ДІЮЧИ ПРОТИПРАВНО, ДОВІДАЛАСЬ, ЩО ТА ВНАСЛІДОК ЗБІГУ ТЯЖКИХ СІМЕЙНИХ ТА МАТЕРІАЛЬНИХ ОБСТАВИН, ВИКЛИКАНИХ ЇЇ СКРУТНИМ МАТЕРІАЛЬНИМ СТАНОВИЩЕМ, БОРГАМИ, ВІДСУТНІСТЮ РОБОТИ, ПОСТІЙНОГО ДЖЕРЕЛА ДОХОДІВ, НАЯВНОСТІ КРЕДИТУ, ПЕРЕКОНАВШИСЬ, ЩО ВОНА ПЕРЕБУВАЄ В УРАЗЛИВОМУ СТАНІ, УСВІДОМЛЮЮЧИ ЦЮ ОБСТАВИНУ, УМИСНО ВИКОРИСТОВУЮЧИ ЇЇ У СВОЇХ ПРОТИПРАВНИХ ЦІЛЯХ ЗАПРОПОНУВАЛА ПОТЕРПІЛІЙ РОБОТУ ПОВІЄЮ НА ТЕРИТОРІЇ ТУРЕЧЧИНИ.

ПРИ ЦЬОМУ РОЗ'ЯСНИЛА ЇЙ УМОВИ ПРОЖИВАННЯ ТА ПРАЦІ, А ТАКОЖ РОЗМІРИ ОПЛАТИ ЗА НАДАННЯ НЕЮ СЕКСУАЛЬНИХ ПОСЛУГ КЛІЄНТАМ ТА ПОЯСНИЛА, ЩО ВОНА БУДЕ ПРОЖИВАТИ В ОПЛАЧУВАНОМУ БУДИНКУ (ВІЛЛІ) З ІНШИМИ ДІВЧАТАМИ, ЯКІ ТЕЖ ПРАЦЮЮТЬ ПОВІЯМИ, ДЕ ЇХ БУДУТЬ ЗАБЕЗПЕЧУВАТИ ХАРЧУВАННЯМ, МАТИМУТЬ ПРИБЛИЗНО 3 КЛІЄНТИ НА ДЕНЬ, А ТАКОЖ 70 ДОЛАРІВ США ЗА ГОДИНУ НАДАННЯ СЕКСУАЛЬНИХ ПОСЛУГ. ТАКОЖ, ПООБІЦЯЛА ОПЛАТИТИ ВИТРАТИ НА ПЕРЕЛІТ ДО ТУРЕЧЧИНИ, ЯКІ ОСТАННЯ ПОВИННА ПОВЕРНУТИ З ПЕРШОЇ ЗАРПЛАТИ, ПОСТАВИВШИ ТИМ САМИМ ПОТЕРПІЛУ В ЗАЛЕЖНЕ ВІД НЕЇ МАТЕРІАЛЬНЕ ПОЛОЖЕННЯ.

ПРОДОВЖУЮЧИ ВЕРБУВАННЯ ПОТЕРПІЛОЇ ОБВИНУВАЧЕНА СТАЛА НЕОДНОРАЗОВО ТЕЛЕФОНУВАТИ НА ЇЇ НОМЕР МОБІЛЬНОГО ТЕЛЕФОНУ, ПИСАТИ ПОВІДОМЛЕННЯ ЗА ДОПОМОГОЮ ПРОГРАМИ МИТТЄВОГО ОБМІНУ ПОВІДОМЛЕННЯМИ «VIBER» [8].

**4. Переміщення людини**

РЕАЛІЗУЮЧИ СВІЙ ЗЛОЧИННИЙ УМИСЕЛ З ВИКОРИСТАННЯМ БЕЗПОРАДНОГО СТАНУ ЛЮДИНИ, ОБВИНУВАЧЕНА, ЗНАХОДЯЧИСЬ В М. РИМ РЕСПУБЛІКИ ІТАЛІЯ, ВИКОРИСТОВУЮЧИ МОБІЛЬНИЙ ЗВ'ЯЗОК, А ТАКОЖ КОМУНІКАЦІЙНІ РЕСУРСИ МЕРЕЖІ «ІНТЕРНЕТ», ДОРУЧИЛА ІНШИМ СПІВУЧАСНИКАМ ПІДШУКАТИ ОСІБ ЖІНОЧОЇ СТАТІ, ЯКІ ЧЕРЕЗ ТЯЖКИЙ МАТЕРІАЛЬНИЙ СТАН АБО ЧЕРЕЗ ЗБІГ ТЯЖКИХ СІМЕЙНИХ ОБСТАВИН ПОГОДЯТЬСЯ НАДАВАТИ ПОСЛУГИ СЕКСУАЛЬНОГО ХАРАКТЕРУ ЗА ГРОШОВУ ВИНАГОРОДУ НА ТЕРИТОРІЇ ІТАЛІЇ.

ТАКИМ ЧИНОМ, ВСТУПИЛА У ЗЛОЧИННУ ЗМОВУ НА ВЕРБОВКУ ТА ПЕРЕМІЩЕННЯ З МЕТОЮ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ ОСІБ ЖІНОЧОЇ СТАТІ З ВИКОРИСТАННЯМ УРАЗЛИВОГО СТАНУ ЛЮДИНИ.

СПІВУЧАСНИКИ НЕОДНОРАЗОВО ЗУСТРІЧАЛИСЬ З ПОТЕРПІЛИМИ НА ТЕРИТОРІЇ ХОРТИЦЬКОГО РАЙОНУ М. ЗАПОРІЖЖЯ ТА ЗА ДОПОМОГОЮ МОБІЛЬНОГО ЗВ'ЯЗКУ, ВИКОРИСТОВУЮЧИ ЇХ УРАЗЛИВИЙ СТАН, ОБІЦЯЮЧИ ВИСОКУ ЗАРОБІТНУ ПЛАТУ, ДОБРІ УМОВИ ПРАЦІ, ІНШІ МАТЕРІАЛЬНІ БЛАГА, ПЕРЕКОНАЛИ ЇЇ У ВИГІДНОСТІ ВИЇЗДУ ДО ІТАЛІЇ ДЛЯ НАДАННЯ ПОСЛУГ СЕКСУАЛЬНОГО ХАРАКТЕРУ ЗА ГРОШОВУ ВИНАГОРОДУ. НА ВИКОНАННЯ ЗАГАЛЬНОГО ЗЛОЧИННОГО УМИСЛУ ЗА ДОПОМОГОЮ ЗАЛІЗНИЧНОГО ТА АВТОМОБІЛЬНОГО ТРАНСПОРТУ ПОТЕРПІЛУ ПЕРЕМІСТИЛИ З ТЕРИТОРІЇ УКРАЇНИ НА ТЕРИТОРІЮ ІТАЛІЇ У М. РИМ, ДЕ ПІДДАВАЛИ СЕКСУАЛЬНІЙ ЕКСПЛУАТАЦІЇ [9].

**5.** Переховування людини передбачає **розміщення людини у певному приміщенні, у транспортному засобі, у певній місцевості тощо, надання їй підроблених документів, вчинення щодо неї пластичної операції і т. ін.**

**6, 7.** Під передачею і одержанням людини треба розуміти відповідні **фактичні дії, вчинені після вчинення стосовно неї акту купівлі-продажу, вербування, переміщення тощо, пов'язані з переходом фактичного контролю над нею від однієї особи (групи осіб) до іншої.**

У перших двох формах (*торгівля людьми, здійснення іншої незаконної угоди, об'єктом якої є людина*) злочин є закінченим з моменту продажу (іншої передачі) людини іншій особі (особам). Якщо до угод з продажу людини застосувати за аналогією правило, що діє у цивільному праві (а специфіка предмета суспільних відносин, з приводу якого ці дії вчинюються, людина, хоча й цілком перетворює юридичну сутність їх із законних на незаконні, але залишає незмінною зовнішню правову оболонку, недаремно законодавець у статті 149 використовує термін цивільного права – «угода»), то злочин треба вважати закінченим з моменту фактичної передачі особи за договором купівлі-продажу, який означає зміну власника, чи з іншого моменту, прямо передбаченого договором між сторонами.

Злочин у його третій – сьомій формах (*вербування людини, переміщення людини, переховування людини, передача людини, одержання людини*) є закінченим з того моменту, коли жертва злочину, відповідно, завербована, переміщена, перехована, передана чи одержана.

Як випливає із примітки 3 до ст. 149 КК України, обов'язковою ознакою злочину, передбаченого ч. 1 ст. 149 КК України, якщо він вчинюється у третій – сьомій формах, крім випадків вчинення його стосовно малолітнього та неповнолітнього, є **спосіб**. Він може альтернативно проявлятися у використанні:

1) обману;

2) шантажу;

3) уразливого стану особи.

Більш небезпечні способи вчинення цього злочину розглядаються як його кваліфікуючі ознаки.

**1. Обман**, як спосіб вербування, переміщення, переховування, передачі, одержання людини полягає у повідомленні потерпілому неправдивих відомостей (наприклад, відомостей про те, що він буде брати участь у конкурсі або отримає широкі можливості для працевлаштування за кордоном) або приховуванні певних відомостей, повідомлення яких мало б суттєве значення для поведінки потерпілого (наприклад, відомостей про дійсні умови праці, розміри і порядок виплати заробітку).

**2. Шантаж**, як спосіб вербування, переміщення, переховування, передачі, одержання людини полягає у погрозі розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці.

> СУД ВИЗНАВ, ЩО ОБВИНУВАЧЕНА ДІЮЧИ УМИСНО, З КОРИСЛИВИХ МОТИВІВ, З ВИКОРИСТАННЯМ УРАЗЛИВОГО СТАНУ ДВОХ ПОТЕРПІЛИХ, З МЕТОЮ ЇХ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ, ШЛЯХОМ ОБМАНУ, ЩО ПОЛЯГАВ У ПОВІДОМЛЕННІ НЕПРАВДИВИХ ВІДОМОСТЕЙ, НЕ ВЛАШТУВАВШИ ЇХ НА ЗАЗДАЛЕГІДЬ ОБІЦЯНЕ МІСЦЕ РОБОТИ, ЗАСТОСУВАЛА ДО ПОТЕРПІЛИХ ПСИХОЛОГІЧНИЙ ТИСК, ЯКИЙ ВИРАЗИВСЯ В ЗАЛЯКУВАННІ ТА ПОГРОЗАХ ЗАСТОСУВАННЯ ФІЗИЧНОГО НАСИЛЬСТВА, ШАНТАЖУ ЩОДО ПОЗБАВЛЕННЯ ОДНІЄЇ З ПОТЕРПІЛИХ ЇЇ СИНА, З ЯКИМ ОСТАННЯ ПРИЇХАЛА НА ПРАЦЕВЛАШТУВАННЯ, А ТАКОЖ В ЗАСТОСУВАННІ НАСИЛЬСТВА, ЯКЕ ВИРАЗИЛОСЬ В НАНЕСЕННІ ТІЛЕСНИХ УШКОДЖЕНЬ ЗА ВІДМОВУ У НАДАННІ СЕКСУАЛЬНИХ ПОСЛУГ.
>
> ЗДОЛАВШИ ОПІР З БОКУ ПОТЕРПІЛИХ, ЯКІ НЕ МАЛИ ЗМОГИ ПОВЕРНУТИСЯ ДОДОМУ ЗА ВІДСУТНОСТІ КОШТІВ ТА ДОКУМЕНТІВ, ВІДРАЗУ ОБМЕЖИЛА ЇХ У ВІЛЬНОМУ ПЕРЕСУВАННІ ПО МІСЦЕВОСТІ, ШЛЯХОМ ПОСТІЙНОГО, ПИЛЬНОГО НАГЛЯДУ ЗА НИМИ ДЛЯ ЗАПОБІГАННЯ МОЖЛИВОЇ ВТЕЧІ ТА ЗМУСИЛА ЇХ ПРОТЯГОМ ТРЬОХ МІСЯЦІВ В НІЧНИЙ ТА ДЕННИЙ ЧАС НАДАВАТИ СЕКСУАЛЬНІ ПОСЛУГИ ЗА ГРОШОВУ ВИНАГОРОДУ [10].

**3.** У примітці 2 до ст. 149 КК України розкривається поняття **уразливого стану особи**, який зазначено у диспозиціях ст. ст. 149, 303 КК України під яким слід розуміти зумовлений фізичними чи психічними властивостями або зовнішніми обставинами стан особи, який позбавляє або обмежує її здатність

усвідомлювати свої дії (бездіяльність) або керувати ними, приймати за своєю волею самостійні рішення, чинити опір насильницьким чи іншим незаконним діям, збіг тяжких особистих, сімейних або інших обставин.

ТАК, НАПРИКЛАД КОТОВСЬКИЙ МІСЬКРАЙОННИЙ СУД ОДЕСЬКОЇ ОБЛАСТІ У ВИРОКУ ВІД 29.06.2017 ВКАЗАВ, ЩО ОБВИНУВАЧЕНА З КОРИСЛИВИХ МОТИВІВ, МАЮЧИ УМИСЕЛ НА ЗДІЙСНЕННЯ ВЕРБУВАННЯ ОСОБИ З МЕТОЮ ПОДАЛЬШОЇ ПЕРЕМІЩЕННЯ ЗА МЕЖІ УКРАЇНИ ДЛЯ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ ЗА ГРОШОВУ ВИНАГОРОДУ, З ВИКОРИСТАННЯМ УРАЗЛИВОГО СТАНУ ПОТЕРПІЛОЇ, ВИКЛИКАНОГО ЇЇ СКРУТНИМ МАТЕРІАЛЬНИМ СТАНОВИЩЕМ, ВІДСУТНІСТЮ РОБОТИ, ПОВ'ЯЗАНИХ З ТИМ, ЩО ЯВЛЯЄТЬСЯ ПЕРЕСЕЛЕНКОЮ З МІСЦЯ ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ, А ТАКОЖ НАЯВНОСТІ НА УТРИМАННІ МАЛОЛІТНЬОЇ ДОНЬКИ ПРОПОНУВАЛА РОБОТУ ПОВ'ЯЗАНУ З НАДАННЯМ СЕКСУАЛЬНИХ ПОСЛУГ НА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У М. МОСКВА [11 ].

**Суб'єкт злочину загальний, суб'єктивна сторона** характеризується прямим умислом і корисливим мотивом.

Крім того, для третьої і наступних його форм (вербування, переміщення, переховування, передача і одержання людини) обов'язковою ознакою є **мета** експлуатації людини.

Що ж стосується двох перших форм, то торгівля людьми та здійснення іншої незаконної угоди, об'єктом якої є людина, мають тягнути кримінальну відповідальність за ст. 149 КК України незалежно від того, чи вчинені вони із зазначеною метою. Інший підхід унеможливив би притягнення до відповідальності особи, яка здійснила продаж людини або передала її за іншою угодою, адже за допомогою існуючих процесуальних засобів практично неможливо довести, що винною особою факт подальшої – після продажу або іншої передачі – експлуатації людини усвідомлювався як неминучий (тим більше неможливо довести, що для інтелектуальної ознаки умислу особи, яка продала дитину, характерним є усвідомлення того, що в подальшому покупець усиновить дитину, маючи за мету наживу).

Вказана мета може бути доведена, як правило, лише у випадках, коли винна особа систематично поставляє певним покупцям дітей для використання їх як жебраків або жінок для сексуальної експлуатації тощо. У більшості ж випадків продавцю насправді байдуже – буде покупець використовувати продану йому особу в порнобізнесі чи одружиться з нею.

**Психічне ставлення** до тяжких наслідків характеризується **необережністю**.

Мета експлуатації розкривається у примітці 1 до ст. 149 КК України. Під експлуатацією розуміються:

1) всі форми сексуальної експлуатації;

ПІДСУДНИЙ ДІЮЧИ З КОРИСЛИВИХ МОТИВІВ І КЕРУЮЧИСЬ МЕТОЮ ЗБАГАЧЕННЯ, НА ПОЧАТКУ 2009 РОКУ СТВОРИВ СТІЙКУ ЗЛОЧИННУ ГРУПУ, ЯКА НА ПОСТІЙНІЙ ОСНОВІ ЗАЙМАЛАСЯ ВЕРБУВАННЯМ, ПЕРЕМІЩЕННЯМ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНИ, ПЕРЕДАЧЕЮ ТА ОТРИМАННЯМ МОЛОДИХ ЖІНОК ПРИВАБЛИВОЇ ЗОВНІШНОСТІ З МЕТОЮ ЇХ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ.

ЗГІДНО ЗАГАЛЬНОГО ПЛАНУ ВЧИНЕННЯ ЗЛОЧИНУ, НА ТЕРИТОРІЇ ВОЛИНСЬКОЇ ОБЛАСТІ ПІДШУКУВАЛИСЬ МОЛОДІ ЖІНКИ ВІКОМ ПРИВАБЛИВОЇ ЗОВНІШНОСТІ, ЯКІ БУЛИ МАТЕРІАЛЬНО НЕЗАБЕЗПЕЧЕНИМИ. В ПОДАЛЬШОМУ, ОБМАННИМ ШЛЯХОМ, ПОВІДОМЛЯЮЧИ НЕПРАВДИВІ ВІДОМОСТІ ПРО ВИД ДІЯЛЬНОСТІ ЯКИЙ НІБИ ТО ПОЛЯГАВ У ПРИБИРАННІ ГОТЕЛІВ, А НАСПРАВДІ У НАДАННІ СЕКСУАЛЬНИХ ПОСЛУГ, ВИКОРИСТОВУЮЧИ УРАЗЛИВИЙ СТАН ПОТЕРПІЛИХ, ЯКИЙ БУВ ВИКЛИКАНИЙ СКРУТНИМ МАТЕРІАЛЬНИМ СТАНОВИЩЕМ, ПОТЕРПІЛИХ СХИЛЯЛИ ДО ПОЇЗДКИ ЗА КОРДОН.

ОТРИМАВШИ ЗГОДУ НА ПОЇЗДКУ, З МЕТОЮ ОТРИМАННЯ КОНТРОЛЮ НАД ЗАВЕРБОВАНИМИ, ЖІНОК СХИЛЯЛИ НЕ БРАТИ В ПОЇЗДКУ ВЛАСНИХ ГРОШОВИХ КОШТІВ, ЧИМ ВВОДИЛИ ОСТАННІХ В ПОВНУ МАТЕРІАЛЬНУ ЗАЛЕЖНІСТЬ. ПІСЛЯ ЦЬОГО, ЛЕГАЛЬНО ПЕРЕПРАВЛЯЛИ ЇХ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНИ ДЕ В БОРДЕЛІ, ЯКИЙ БУВ ЗАВУАЛЬОВАНИЙ ПІД НІЧНИЙ КЛУБ ЗАЛУЧАЛИ ДО ЗАЙНЯТТЯ ПРОСТИТУЦІЄЮ, ЩО ПРИНОСИЛО ЗНАЧНІ КРИМІНАЛЬНІ ПРИБУТКИ, ЯКІ РОЗПОДІЛЯЛИСЯ МІЖ ЧЛЕНАМИ ЗЛОЧИННОГО УГРУПУВАННЯ [12].

2) використання в порнобізнесі;

НАПРИКЛАД ГРОМАДЯНИН УКРАЇНИ В ПЕРІОД 3 КВІТНЯ 2002 ПО ТРАВЕНЬ 2003 У СКЛАДІ ОРГАНІЗОВАНОЇ ЗЛОЧИННОЇ ГРУПИ ОРГАНІЗУВАВ ПОШУК ТА ВЕРБУВАННЯ В УКРАЇНІ ПОНАД 20 МОЛОДИХ ДІВЧАТ, З НЕЗАДОВІЛЬНИМ МАТЕРІАЛЬНИМ СТАНОВИЩЕМ, ЯКИМ ПРОПОНУВАЛОСЬ ПРАЦЕВЛАШТУВАННЯ В МОДЕЛЬНОМУ БІЗНЕСІ В РОСІЙСЬКІЙ ФЕДЕРАЦІЇ, ОДНАК НАСПРАВДІ ВИКОРИСТОВУВАЛИ В ПОРНОБІЗНЕСІ ШЛЯХОМ ОПЛАТНОГО ДЕМОНСТРУВАННЯ ЇХ ОГОЛЕНИХ ТІЛ НА СПЕЦІАЛЬНИХ САЙТАХ У МЕРЕЖІ «ІНТЕРНЕТ» [13].

3) примусова праця або примусове надання послуг;

ПРИКЛАДОМ Є ВИРОК ЗВЕНИГОРОДСЬКОГО РАЙОННОГО СУДУ ВІД 11.04.2013 ЗГІДНО ЯКОГО ОБВИНУВАЧЕНИЙ У 2012 РОЦІ, ШЛЯХОМ ОБМАНУ ТА ВИКОРИСТАННЯ УРАЗЛИВОМУ СТАНУ ПОТЕРПІЛОЇ, ПІД ПРИВОДОМ ВИКОНАННЯ СІЛЬСЬКОГОСПОДАРСЬКИХ РОБІТ ЗА ВИНАГОРОДУ ЗАВЕРБУВАВ ЇЇ ТА НЕ НАДАВШИ ОБІЦЯНИХ УМОВ ПРАЦІ, МАЮЧИ НА МЕТІ ПРИМУСОВО ЗМУСИТИ ЇЇ ДО ВИКОНАННЯ РОБІТ БЕЗОПЛАТНО, ЗАСТОСУВАВ ДО ПОТЕРПІЛОЇ ПСИХОЛОГІЧНИЙ ТИСК, ЯКИЙ ВИРАЗИВСЯ В ЗАЛЯКУВАНІ ТА ПОГРОЗАХ ЗАСТОСУВАННЯ ДО ОСТАННЬОЇ ФІЗИЧНОГО НАСИЛЬСТВА ТА ЗАСТОСУВАННІ НАСИЛЬСТВА, ЯКЕ НЕ Є НЕБЕЗПЕЧНИМ ДЛЯ ЖИТТЯ ТА ЗДОРОВ'Я.

ЗДОЛАВШИ ОПІР ПОТЕРПІЛОЇ, ЯКА НЕ МАЛА ЗМОГИ ПОВЕРНУТИСЯ ДОДОМУ ЗА ВІДСУТНОСТІ КОШТІВ, ОБВИНУВАЧЕНИЙ ОБМЕЖИВ ЇЇ У ВІЛЬНОМУ ПЕРЕСУВАННІ ТА ЗМУСИВ ЇЇ ПРОТЯГОМ ОДНОГО МІСЯЦЯ БЕЗОПЛАТНО ВИКОНУВАТИ СІЛЬСЬКОГОСПОДАРСЬКІ РОБОТИ У НЬОГО В ДОМОВОЛОДІННІ [14].

ЩЕ ОДИН ПРИКЛАД ЗАЛУЧЕННЯ ПОТЕРПІЛИХ ДО ПРИМУСОВОЇ ПРАЦІ ОПИСАНИЙ В УХВАЛІ АПЕЛЯЦІЙНОГО СУДУ ТЕРНОПІЛЬСЬКОЇ ОБЛАСТІ ПРО ПЕРЕГЛЯД ВИРОКУ КРЕМЕНЕЦЬКОГО РАЙОННОГО СУДУ ТЕРНОПІЛЬСЬКОЇ ОБЛАСТІ ВІД 11 ЛИСТОПАДА 2016 РОКУ.

ЗГІДНО УХВАЛИ ЗАСУДЖЕНІ, ВИКОРИСТОВУЮЧИ УРАЗЛИВИЙ СТАН ПОТЕРПІЛИХ, ЩО БУВ ВИКЛИКАНИЙ СКРУТНИМ МАТЕРІАЛЬНИМ СТАНОВИЩЕМ, ВІДСУТНІСТЮ ПОСТІЙНОГО МІСЦЯ РОБОТИ ТА ІНШИХ ДЖЕРЕЛ ОТРИМАННЯ ДОХОДІВ ДЛЯ ІСНУВАННЯ, ПРОПОНУЮЧИ ВИГІДНІ УМОВИ ПРАЦІ І ВИСОКІ ЗАРОБІТКИ, ЯКІ НЕ ВІДПОВІДАЛИ ДІЙСНОСТІ, СХИЛЯЛИ ЇХ У ТАКИЙ СПОСІБ ДО ПОЇЗДКИ В КРАСНОДАРСЬКИЙ КРАЙ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ (ЗДІЙСНЮВАЛИ ВЕРБУВАННЯ), ДЕ ПОТЕРПІЛИХ ПЕРЕДАВАЛИ ЗА ГРОШОВУ ВИНАГОРОДУ З МЕТОЮ ЗАЛУЧЕННЯ ДО ПРИМУСОВОЇ ПРАЦІ

АДВОКАТ ОБҐРУНТОВУЮЧИ СВОЮ АПЕЛЯЦІЙНУ СКАРГУ ЗВЕРТАВ УВАГУ НА ТЕ, ЩО СУД НЕ ДАВ НАЛЕЖНОЇ ОЦІНКИ ДОКУМЕНТАМ ОТРИМАНИМ НА АДВОКАТСЬКИЙ ЗАПИТ ВІД ПРАВООХОРОННИХ ОРГАНІВ РФ, ДЕ ВІДОБРАЖЕНІ ВИТЯГИ ІЗ БУХГАЛТЕРСЬКИХ ДОКУМЕНТІВ ПРО НАРАХУВАННЯ ЗАРОБІТНОЇ ПЛАТИ ПОТЕРПІЛИМ, ЯКА ПЕРЕВИЩУВАЛА НА ТОЙ ЧАС СЕРЕДНЬОМІСЯЧНИЙ ЗАРОБІТОК В ТЕРНОПІЛЬСЬКІЙ ОБЛАСТІ.

НАТОМІСТЬ КОЛЕГІЯ СУДДІВ ЗАЗНАЧИЛА, ЩО ПРО НАЯВНІСТЬ ОЗНАК ТРУДОВОЇ ЕКСПЛУАТАЦІЇ ПОТЕРПІЛИХ СВІДЧАТЬ ПОНАДУРОЧНИЙ РЕЖИМ РОБОТИ, НЕНАЛЕЖНІ УМОВИ ПРАЦІ, АНТИСАНІТАРНІ УМОВИ ПРОЖИВАННЯ, ВІДСУТНІСТЬ

ТРУДОВОГО ДОГОВОРУ З ПОТЕРПІЛИМИ ТА НАКАЗУ ПРО ПРИЙНЯТТЯ ЇХ НА РОБОТУ, ВИЛУЧЕННЯ У НИХ ПАСПОРТІВ ТА НЕМОЖЛИВІСТЬ ВІДМОВИТИСЬ ВІД РОБОТИ ПОКИ НЕ БУДУТЬ ВІДРОБЛЕНІ КОШТИ ЗА ПРОЇЗД.

КРІМ ТОГО, ДОВОДИ ЗАХИСНИКА ПРО ПРОВЕДЕННЯ ОПЛАТИ ПОТЕРПІЛИМ ЗА ВИКОНАНУ НИМИ РОБОТУ ТА ВІДСУТНОСТІ З ЇХ БОКУ СКАРГ НЕ БЕРУТЬСЯ ДО УВАГИ, ОСКІЛЬКИ ФАКТ ОПЛАТИ ПРАЦІ ПОТЕРПІЛИХ І ЇХ ЗГОДА НА РОБОТУ, НА ЗАПРОПОНОВАНИХ ОБВИНУВАЧЕНИМИ УМОВАХ, НЕ ВИКЛЮЧАЄ КАРАНОСТІ ДІЯННЯ ЗА СТ.149 КК УКРАЇНИ [15].

У КВІТНІ2017 РОКУ ДО ПОЛІЦІЇ ЗВЕРНУВСЯ ЧОЛОВІК. ВІН ПОВІДОМИВ, ЩО В ЖОВТНІ 2016 РОКУ ЙОГО ВИКРАЛИ НЕВІДОМІ ОСОБИ. З ТОГО ЧАСУ І ДО МОМЕНТУ ВТЕЧІ ПОТЕРПІЛОГО УТРИМУВАЛИ В ОДНОМУ З НАСЕЛЕНИХ ПУНКТІВ ДНІПРОПЕТРОВЩИНИ. УВЕСЬ ЦЕЙ ЧАС ЗЛОВМИСНИКИ ЗМУШУВАЛИ ЧОЛОВІКА ПРАЦЮВАТИ БЕЗОПЛАТНО НА БУДІВНИЦТВІ.

СЛІДЧІ ВНЕСЛИ ІНФОРМАЦІЮ ВІД УПРАВЛІННЯ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ, ПОВ'ЯЗАНИМИ З ТОРГІВЛЕЮ ЛЮДЬМИ ПОЛІЦІЇ ДНІПРОПЕТРОВЩИНИ ДО ЄДИНОГО РЕЄСТРУ ДОСУДОВИХ РОЗСЛІДУВАНЬ. ДІЇ ЗЛОВМИСНИКІВ КВАЛІФІКУВАЛИ ЗА ОЗНАКАМИ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО Ч. 1 СТ. 149 (ТОРГІВЛЯ ЛЮДЬМИ АБО ІНША НЕЗАКОННА УГОДА ЩОДО ЛЮДИНИ) КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ.

ПІД ЧАС РОЗСЛІДУВАННЯ ПОЛІЦЕЙСЬКІ З'ЯСУВАЛИ, ЩО ГРУПА ОСІБ НА ДНІПРОПЕТРОВЩИНІ СТВОРИЛА ТАК ЗВАНІ «РЕАБІЛІТАЦІЙНІ ЦЕНТРИ». ВОНИ ДІЯЛИ ПІД ВИГЛЯДОМ БЛАГОДІЙНИХ ОРГАНІЗАЦІЙ З ДОПОМОГИ ХВОРИМ НА НАРКОМАНІЮ ТА АЛКОГОЛІЗМ. ЛЮДЕЙ ТАМ УТРИМУВАЛИ ПРОТИ ЇХ ВОЛІ, ПРИМУШУЮЧИ БЕЗОПЛАТНО ПРАЦЮВАТИ.

ПОЛІЦІЯ ВСТАНОВИЛА І ОСОБИ ЗЛОВМИСНИКІВ. КЕРІВНИКАМИ «ЦЕНТРІВ» ВИЯВИЛИСЯ ДВОЄ МЕШКАНЦІВ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ ВІКОМ 27 І 34 РОКІВ. ВОНИ РАЗОМ З ІНШИМИ СПІВУЧАСНИКАМИ ОРГАНІЗУВАЛИ ТАК ЗВАНІ «РЕАБІЛІТАЦІЙНІ ЦЕНТРИ» У ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ.

ТУДИ ЗВЕРТАЛИСЯ РОДИЧІ ОСІБ АЛКО-, НАРКОЗАЛЕЖНИХ, ВІЛ-ІНФІКОВАНИХ, ХВОРИХ ТУБЕРКУЛЬОЗОМ, ТОЩО. ОСОБИ, ЯКІ ЗВЕРТАЛИСЬ ДО ЦИХ «ЦЕНТРІВ», ПРОСИЛИ ВИЛІКУВАТИ ЇХНІХ ХВОРИХ РОДИЧІВ. ПОТЕРПІЛИХ ВИКРАДАЛИ ІЗ ЗАСТОСУВАННЯМ НАСИЛЬСТВА І ВІДВОЗИЛИ ДО «РЕАБІЛІТАЦІЙНИХ ЦЕНТРІВ». АДРЕСИ ЦИХ ЗАКЛАДІВ НІКОМУ НЕ ПОВІДОМЛЯЛИСЯ.

ТАМ ПОТЕРПІЛИХ ПОМІЩУВАЛИ ПІД ОХОРОНУ І ЗАСТОСОВУВАЛИ НАСИЛЛЯ, ПРИГНІЧУЮЧИ ЇХ ВОЛЮ. ЛЮДЕЙ ІЗ ЗАДОВІЛЬНИМ СТАНОМ ЗДОРОВ'Я ВИКОРИСТОВУВАЛИ ЯК НАЙМАНУ РОБОЧУ СИЛУ ДЛЯ РІЗНОМАНІТНОЇ ФІЗИЧНОЇ ПРАЦІ, ЗАЗВИЧАЙ – ПІД ПИЛЬНИМ НАГЛЯДОМ ОХОРОНЦІВ. ГРОШІ ЗА ВИКОНАНУ ПРАЦЮ ОТРИМУВАЛИ КЕРІВНИКИ ЦЕНТРУ.

СЛІДЧІ ВБАЧАЮТЬ У ДІЯХ ОРГАНІЗАТОРІВ «ЦЕНТРІВ» ОЗНАКИ ЗЛОЧИНІВ, ПЕРЕДБАЧЕНИХ СТ. 146 (НЕЗАКОННЕ ПОЗБАВЛЕННЯ ВОЛІ АБО ВИКРАДЕННЯ ЛЮДИНИ), А ТАКОЖ СТ. 149 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ. ВИРІШУЄТЬСЯ ПИТАННЯ ПРО ОГОЛОШЕННЯ ЗЛОВМИСНИКАМ ПІДОЗРИ У ВЧИНЕНІ ЦИХ ЗЛОЧИНІВ.

4) рабство або звичаї, подібні до рабства;

5) підневільний стан;

6) залучення в боргову кабалу;

НА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ, ДВОЄ ОБВИНУВАЧЕНИХ, ДІЮЧИ УМИСНО, З КОРИСЛИВИХ МОТИВІВ, З МЕТОЮ ОТРИМАННЯ КОНТРОЛЮ НАД ПОТЕРПІЛОЮ В ЯКОЇ БУЛИ ВІДСУТНІ БУДЬ-ЯКІ ДОКУМЕНТИ, ЩО ПОСВІДЧУЮТЬ ЇЇ ОСОБУ, ЗАЛУЧИЛИ ЇЇ В БОРГОВУ КАБАЛУ, ПОВІДОМИВШИ ПРО НЕОБХІДНІСТЬ ВІДПРАЦЮВАННЯ КОШТІВ, ВИТРАЧЕНИХ

НА ЇЇ ПЕРЕВЕЗЕННЯ ДО РОСІЇ ТА СКОРИСТАВШИСЬ ПЕРЕБУВАННЯМ ПОТЕРПІЛОЇ У ПІДНЕВІЛЬНОМУ СТАНІ ЧЕРЕЗ НЕЛЕГАЛЬНЕ ПЕРЕБУВАННЯ НА ТЕРИТОРІЇ ІНШОЇ ДЕРЖАВИ, БЕЗ ВІДПОВІДНОЇ РЕЄСТРАЦІЇ, СПОНУКАЛИ ПОТЕРПІЛУ ДО ЗАНЯТТЯ ЖЕБРАЦТВОМ ПІД ЇХ КОНТРОЛЕМ НА ПРОТЯЗІ ОДНОГО ТИЖНЯ У М. МОСКВА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ [16].

7) вилучення органів;

ОБВИНУВАЧЕНИЙ, МАЮЧИ НА МЕТІ ЗДІЙСНЕННЯ ТОРГІВЛІ ЛЮДЬМИ ТА НЕЗАКОННОЇ УГОДИ ЩОДО ПЕРЕДАЧІ ЛЮДИНИ, В ЦІЛЯХ ЇЇ ПОДАЛЬШОЇ ЕКСПЛУАТАЦІЇ, БУДУЧИ ЗНАЙОМИМ ІЗ ПОТЕРПІЛИМ ТА УСВІДОМЛЮЮЧИ, ЩО ОСТАННІЙ ВНАСЛІДОК ЗБІГУ ТЯЖКИХ СІМЕЙНИХ ТА МАТЕРІАЛЬНИХ ОБСТАВИН ПЕРЕБУВАЄ В УРАЗЛИВОМУ СТАНІ, ПЕРЕКОНАВ ЙОГО НАДАТИ ЗГОДУ НА ВИЛУЧЕННЯ НИРКИ ДЛЯ ТРАНСПЛАНТАЦІЇ, ЗА ЩО ОБІЦЯВ ЗАПЛАТИТИ ГРОШОВУ ВИНАГОРОДУ В РОЗМІРІ 10 000 (ДЕСЯТЬ ТИСЯЧ) ДОЛАРІВ США.

ПІСЛЯ ПРОВЕДЕННЯ ВЕРБУВАННЯ ПІДСУДНИЙ ОРГАНІЗУВАВ ВИЇЗД ПОТЕРПІЛОГО В М. КИЇВ, ДЕ В ІНСТИТУТІ ХІРУРГІЇ ТА ТРАНСПЛАНТОЛОГІЇ ІМЕНІ О. О. ШАЛІМОВА, ХІРУРГІЧНИМ ШЛЯХОМ ВИЛУЧИЛИ ВІД ОСТАННЬОГО НИРКУ ДЛЯ ПОДАЛЬШОЇ ТРАНСПЛАНТАЦІЇ РЕЦИПІЄНТУ [17].

8) проведення дослідів над людиною без її згоди;

9) усиновлення (удочеріння) з метою наживи;

10) примусова вагітність;

11) втягнення у злочинну діяльність;

12) використання у збройних конфліктах.

**Кваліфікуючими ознаками** розглядуваного злочину (ч. 2 ст. 149 КК України) є вчинення його:

1) щодо неповнолітнього;

2) щодо кількох осіб;

3) повторно;

4) за попередньою змовою групою осіб;

5) службовою особою з використанням службового становища;

6) особою, від якої потерпілий був у матеріальній чи іншій залежності;

7) у поєднанні з насильством, яке не є небезпечним для життя чи здоров'я потерпілого чи його близьких, або особою, від якої потерпілий був у матеріальній або іншій залежності;

8) з погрозою застосування такого насильства (ч. 2 ст. 149 КК України).

**Особливо кваліфікуючими ознаками** злочину (ч. 3 ст. 149 КК України) є вчинення тих самих дій:

1) щодо малолітнього;

2) організованою групою;

3) у поєднанні з насильством, яке є небезпечним для життя чи здоров'я потерпілого чи його близьких;

4) з погрозою застосування такого насильства;

5) якщо вони спричинили тяжкі наслідки.

ПРИКЛАД СПРИЧИНЕННЯ ТЯЖКИХ НАСЛІДКІВ ОПИСАНИЙ У ВИРОКУ КОНОТОПСЬКОГО МІСЬКРАЙОННОГО СУДУ СУМСЬКОЇ ОБЛАСТІ ВІД 30.06.2011 РОКУ. ТАК ОБВИНУВАЧЕНА ВИКОРИСТОВУЮЧИ ОБМАН, СВОЇ ВІДНОСИНИ З ПОТЕРПІЛОЮ, ЯКА НЕ ВИЇЗДИЛА НІКУДИ ЗА МЕЖІ СЕЛА, ЇЇ МАТЕРІАЛЬНИЙ СТАН, ВІК, ПЕРЕКОНАЛА ОСТАННЮ ВИЇХАТИ ДО МОСКОВСЬКОЇ ОБЛАСТІ РФ, ДЛЯ ПРАЦЕВЛАШТУВАННЯ ЇЇ ПРИБИРАЛЬНИЦЕЮ.

ОДНАК, ПРИБУВШИ НА МІСЦЕ ПРАЦЕВЛАШТУВАННЯ ПОТЕРПІЛУ ЗҐВАЛТУВАЛИ ТА ПРИМУСИЛИ НАДАВАТИ СЕКСУАЛЬНІ ПОСЛУГИ.

ПІСЛЯ ПОВЕРНЕННЯ В УКРАЇНУ ПОТЕРПІЛА В ЗВ'ЯЗКУ З ОТРИМАНИМИ В СЕКСУАЛЬНОМУ РАБСТВІ ДУШЕВНИМИ ТА ФІЗИЧНИМИ ТРАВМАМИ, ПЕРЕЖИВАЮЧИ СТРАЖДАННЯ ТА ЖАХЛИВІ СПОГАДИ ВІДНОСНО ВЧИНЕНИХ ЩОДО НЕЇ ЗЛОЧИННИХ ДІЙ В СЕКСУАЛЬНОМУ РАБСТВІ, НАМАГАЛАСЯ ПОКІНЧИТИ ЖИТТЯ САМОГУБСТВОМ ЧЕРЕЗ ПОВІШАННЯ, ЩО ВИЗНАНО СУДОМ ТЯЖКИМИ НАСЛІДКАМИ [18, С. 44].

У листопаді 2017 року Верховна Рада України в першому читанні прийняла законопроект «Про внесення змін до статті 149 Кримінального кодексу України (щодо приведення у відповідність до міжнародних стандартів)» від 27.03.2017 № 6243 [19].

Згідно з ним планується змінити диспозицію ст. 149 Кримінального кодексу України в частині визначення поняття «торгівлі людьми», під яким пропонується розуміти вербування, переміщення, переховування, передачу або одержання людини, вчинені з метою експлуатації, з використанням обману, **шахрайства**, шантажу, уразливого стану особи, **примусу, або шляхом підкупу третьої особи для отримання згоди на експлуатацію людини**.

Немаловажним аспектом запропонованих змін є те, що тепер під експлуатацією пропонується окрім попередніх форм також розуміти **примусове переривання вагітності, примусове одруження, примусове втягнення у заняття жебрацтвом**. Також відповідальність за вербування, переміщення, переховування, передачу або одержання людини за ст. 149 буде наставати **незалежно від наявності згоди цієї людини на експлуатацію, якщо до неї був застосований будь-який із заходів впливу**, передбачений ст. 149 Кримінального кодексу України.

Торгівля людьми межує зі складами злочинів, передбаченими статтями:

*143 «Порушення встановленого законом порядку трансплантації органів або тканин людини»;*

*146 «Незаконне позбавлення волі або викрадення людини»;*

*147 «Захоплення заручників»;*

*148 «Підміна дитини»;*

*150 «Експлуатація дітей»;*

*150-1 «Використання малолітньої дитини для заняття жебрацтвом»;*

*169 «Незаконні дії щодо усиновлення (удочеріння)»;*

*301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів»;*

*303 «Сутенерство або втягнення особи в заняття проституцією»;*

*304 «Втягнення неповнолітніх у злочинну діяльність»;*

*447 «Найманство».*

При розмежуванні необхідно враховувати, що особливістю торгівлі людьми є здійснення незаконної угоди стосовно людини, що відображається на особливостях складу цього злочину [20, с. 17]. Надалі, говорячи про торгівлю людьми будемо мати на увазі усі перераховані вище склади злочинів [21].

Найчастіше на практиці зустрічаються випадки, пов'язані із торгівлею органами або тканинами людини, експлуатацією дітей, незаконною передачею дитини, злочинами у сфері суспільної моралі, контрабанди мігрантів тощо).

Відмінність між торгівлею людьми та незаконною торгівлею органами полягає у предметі злочину. У першому випадку предметом оплатної передачі є людина, у другому – лише її орган або тканини (наприклад, якщо батьки відвели свою дитину до медичного закладу, де отримали оплату за незаконне вилучення у неї нирки).

Експлуатація дітей (склад злочину, передбачений ст. 150 Кримінального кодексу України) має місце у випадку використання добровільної праці дитини, яка не досягла віку, з якого законодавством дозволяється працевлаштування, з метою отримання прибутку. У той же час випадки вербування дитини для використання її примусової праці чи примусового надання послуг або з іншою передбаченою у примітці 1 до ст. 149 метою, повинні розглядатися як торгівля людьми. Також як торгівля дітьми кваліфікуватимуться й інші випадки купівлі-продажу, іншої незаконної угоди щодо дитини, переміщення, переховування, передача або одержання дитини, вчинені з метою її експлуатації.

Незаконна передача дитини (ст. 169) може здійснюватися для усиновлення (удочеріння) дитини, передачі її під опіку (піклування) чи на виховання в сім'ю громадян. На відміну від цього, статтею 149 охоплюються лише випадки усиновлення (удочеріння) з метою наживи. При цьому мета наживи може поєднуватися з іншими цілями, передбаченими статтею 149 КК України: втягненням у злочинну діяльність, примусову працю, жебрацтво тощо.

Розмежовуючи торгівлю людьми із злочинами у сфері суспільної моралі, слід пам'ятати, що дії сутенера, який за грошову винагороду зводить жінку з клієнтом, за відсутності інших обов'язкових для торгівлі людьми ознак, не можна вважати торгівлею людьми, навіть, якщо жінку «замовляють» на тривалий час. Такі дії необхідно розглядати як звідництво для розпусти (ст. 302 КК України) або як сутенерство чи втягнення особи в зайняття проституцією (ст. 303 КК України).

Різниця між проституцією і торгівлею людьми дуже значна. Особа, яка займається проституцією, робить це добровільно, контролює сексуальну практику і кількість клієнтів, сама розпоряджається прибутками, отриманими від надання своїх послуг. Плутанина між торгівлею людьми та проституцією найчастіше виникає в ситуації, коли відомо, що жертва знала, що вона буде надавати сексуальні послуги. Однак, якщо ситуація відповідає всім об'єктивним і суб'єктивним ознакам, що характеризують торгівлю людьми (наприклад, мали місце обман, експлуатація, позбавлення права прийняття власного рішення, контроль), особа, яка дала свою згоду на надання сексуальних послуг, буде вважатися потерпілою від цього злочину.

Для розмежування торгівлі людьми або іншої незаконної угоди щодо людини від грубого порушення угоди про роботу українського громадянина в Україні або за її межами (ст. 173 КК України) необхідно враховувати, чи мала вона примусовий характер. Торгівля людьми відрізняється від цього злочину тим, що торговець використовує обман, шантаж, уразливий стан, насильство або інші передбачені засоби впливу вже під час вербування, усвідомлюючи при цьому подальшу мету експлуатації людини.

Дії, які полягають у використанні трудової міграції для незаконного збагачення, наприклад, обманного заволодіння грошима під приводом надання послуг із працевлаштування за кордоном, можуть кваліфікуватися як шахрайство (ст. 190 КК України).

Щоб відмежувати торгівлю людьми від незаконного ввезення мігрантів, необхідно проаналізувати, за яких обставин ці злочини було вчинено. Хоча у них є і деякі спільні риси, зокрема переміщення людей, але при цьому існує принципова різниця щодо використаних засобів і цілей. У випадку торгівлі людьми жертв змушують виїхати за допомогою обману або інших злочинних засобів впливу з метою їх подальшої експлуатації.

При незаконному ввезенні мігрантів, хоча воно нерідко здійснюється в принижуючих людську гідність або небезпечних умовах, має місце добровільна згода на таке переміщення. А основним джерелом прибутків злочинців є плата, яку вони отримують за його організацію. Після прибуття до місця призначення стосунки між нелегальним мігрантом і перевізником припиняються (оскільки відбувся перетин кордону і розрахунок за це), а зв'язок постраждалих з торгівцями людьми лише посилюється, оскільки після перевезення починається етап експлуатації. Інша відмінність полягає в тому, що незаконне ввезення мігрантів завжди носить транснаціональний характер, а торгівля людьми може здійснюватися і в межах однієї країни. Хоча торгівля людьми і незаконне ввезення мігрантів – це два різних злочини, однак вони не виключають один одного. Мігрант, який доїхав до країни призначення, в будь-який момент може стати жертвою торгівлі людьми.

Особливу небезпеку становлять організовані злочинні угруповання, які здійснюють торгівлю людьми. Дуже часто можна побачити модель злочинного угруповання, яке налічує небагато учасників, але вони вузько спеціалізуються на вчиненні певних видів злочинів. Ці групи співпрацюють, часто на міжнародному рівні, надаючи одна одній послуги.

Незалежно від структури організованих злочинних угруповань, функції їх учасників схожі:

- вербування жертв;
- нагляд за жертвами торгівлі та транспортування;
- виготовлення фальшивих документів;
- налагодження корумпованих зв'язків з державними органами;
- збирання грошей від торгівлі людьми;
- утримання нерухомості, де жертви піддаються експлуатації, зокрема барів, нічних клубів, борделів, фабрик, готелів, будівельних майданчиків, ферм.
- посередництво;
- зберігання та розподіл доходів;
- відмивання коштів та управління активами.

ВІДПОВІДНО ДО ЗВІТУ ДЕРЖАВНОГО ДЕПАРТАМЕНТУ США 2017 РОКУ ЩОДО СТАНУ ТОРГІВЛІ ЛЮДЬМИ У СВІТІ, УРЯД УКРАЇНИ ПРОДЕМОНСТРУВАВ АКТИВІЗАЦІЮ ЗУСИЛЬ У БОРОТЬБІ З ТОРГІВЛЕЮ ЛЮДЬМИ ПОРІВНЯНО З ПОПЕРЕДНІМ ЗВІТНИМ ПЕРІОДОМ. У ЗВ'ЯЗКУ ІЗ ЦИМ УКРАЇНУ ПІДВИЩИЛИ ДО 2-ГО РІВНЯ. СУТТЄВУ ЧАСТИНУ ЗВІТУ ПРИСВЯЧЕНО ЗАГОСТРЕННЮ СИТУАЦІЇ З ТОРГІВЛЕЮ ЛЮДЬМИ НА ТЕРИТОРІЇ ДОНЕЦЬКОЇ ТА ЛУГАНСЬКОЇ ОБЛАСТЕЙ, ТИМЧАСОВО НЕПІДКОНТРОЛЬНІЙ УКРАЇНІ. ЗОКРЕМА НАГОЛОШУЄТЬСЯ НА ВИПАДКАХ ВИКРАДЕННЯ ЖІНОК ТА ДІВЧАТ НА ЦИХ ТЕРИТОРІЯХ З МЕТОЮ СЕКСУАЛЬНОЇ ТА ТРУДОВОЇ ЕКСПЛУАТАЦІЇ, ЗАЛУЧЕННІ НЕПОВНОЛІТНІХ ДО ВІЙСЬКОВИХ ДІЙ, А ТАКОЖ ВИКОРИСТАННЯ ДІТЕЙ У ЯКОСТІ ІНФОРМАТОРІВ БОЙОВИКІВ ТА ЖИВОГО ЩИТА.

ОДНІЄЮ З РЕКОМЕНДАЦІЙ, ВИКЛАДЕНИХ У ЗВІТІ, БУЛО ЗАЗНАЧЕНО НЕОБХІДНІСТЬ У ЗБІЛЬШЕННІ ТРЕНІНГІВ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ, ПРОКУРОРІВ, ТА СУДДІВ ЩОДО РОЗСЛІДУВАННЯ ТА ПІДТРИМКИ ОБВИНУВАЧЕННЯ В СУДІ У СПРАВАХ ПРО ТОРГІВЛЮ ЛЮДЬМИ [22].

ЩО СТОСУЄТЬСЯ СТАТИСТИЧНИХ ДАНИХ ПО ЗЛОЧИНАХ ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ, ЗІБРАНИХ ВІТЧИЗНЯНИМИ ПРАВООХОРОННИМИ ОРГАНАМИ, ТО ТУТ СЛІД ВІДЗНАЧИТИ НАСТУПНЕ:

1. З ЧАСУ ВВЕДЕННЯ (З БЕРЕЗНЯ 1998 РОКУ) КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ТОРГІВЛЮ ЛЮДЬМИ ВИЯВЛЕНО БІЛЬШЕ П'ЯТИ ТИСЯЧ ТАКИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ (У 2005 РОЦІ – 415, 2006 – 376, 2007 – 359, 2008 – 322, 2009 – 279, 2010 – 257, 2011 – 197, 2012 – 155, 2013 – 130, 2014 – 109, 2015 – 111, 2016 – 115).

2. НАБУВАЮТЬ ВСЕ БІЛЬШОГО ПОШИРЕННЯ ФОРМИ ТОРГІВЛІ ЛЮДЬМИ, НЕ ПОВ'ЯЗАНІ З СЕКСУАЛЬНОЮ ЕКСПЛУАТАЦІЄЮ, ТАКІ ЯК ТРУДОВА ЕКСПЛУАТАЦІЯ (СІЛЬСЬКОГОСПОДАРСЬКІ РОБОТИ, БУДІВНИЦТВО, ПРИМУСОВЕ ЖЕБРАЦТВО), ЖЕРТВАМИ ВІД ЯКОЇ ЧАСТІШЕ СТАЮТЬ ЧОЛОВІКИ ПРАЦЕЗДАТНОГО ВІКУ АБО ОСОБИ З ЯВНИМИ ОЗНАКАМИ ІНВАЛІДНОСТІ, БЕЗ ПОСТІЙНОГО МІСЦЯ МЕШКАННЯ ТА ІНШІ МАЛОЗАБЕЗПЕЧЕНІ КАТЕГОРІЇ ГРОМАДЯН.
3. ОСНОВНИМИ ГРУПАМИ РИЗИКУ СТАТИ ЖЕРТВАМИ ТОРГІВЛІ ЛЮДЬМИ Є НЕЗАМІЖНІ ЖІНКИ, САМОТНІ МАТЕРІ, РОЗЛУЧЕНІ ОСОБИ; МОЛОДЬ, ДІТИ ВУЛИЦІ, ДІТИ-СИРОТИ, ВИХІДЦІ З НЕБЛАГОПОЛУЧНИХ СІМЕЙ; СІЛЬСЬКЕ НАСЕЛЕННЯ; ВНУТРІШНЬО ПЕРЕМІЩЕНІ ОСОБИ, ІНОЗЕМНІ ГРОМАДЯНИ – ТРУДОВІ МІГРАНТИ; ОСОБИ, ЯКІ ЗАЗНАЛИ НАСИЛЬСТВА, У ТОМУ ЧИСЛІ СЕКСУАЛЬНОГО; БІДНІ, МАЛОЗАБЕЗПЕЧЕНІ ОСОБИ; ОСОБИ З ПРОБЛЕМАМИ ПСИХІЧНОГО ЗДОРОВ'Я.
4. ЗА ВІКОВИМИ ОЗНАКАМИ ЖЕРТВАМИ ТОРГІВЛІ ЛЮДЬМИ НАЙЧАСТІШЕ СТАЮТЬ: ЖІНКИ У ВІЦІ 18-26 РОКІВ, У ПЕРШУ ЧЕРГУ НЕЗАМІЖНІ (ВРАЗЛИВІ ДО СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ); ЧОЛОВІКИ У ВІЦІ 31-60 РОКІВ, У ПЕРШУ ЧЕРГУ ОДРУЖЕНІ (ВРАЗЛИВІ ДО ТРУДОВОЇ ЕКСПЛУАТАЦІЇ); ДІТИ У ВІЦІ 13-18 РОКІВ, У ПЕРШУ ЧЕРГУ ДІВЧАТКА З НЕПОВНИХ ТА РЕСТРУКТУРОВАНИХ СІМЕЙ (КОЛИ ОДИН ІЗ БАТЬКІВ НЕРІДНИЙ).

Торгівля людьми, що вчиняється із застосуванням інформаційних технологій, по суті, поєднує два види злочинів – торгівлю людьми та кіберзлочинність. Анонімність та масовість користувачів онлайн-сервісів сприяє як розповсюдженню, так і отриманню доходів від цих сервісів, що суттєво ускладнює розслідування таких злочинів за допомогою лише традиційних підходів.

На теперішній час можна виділити такі головні тенденції застосування інформаційних технологій у торгівлі людьми:

- деякі види сексуальної експлуатації жертв торгівлі людьми здійснюються винятково в Інтернеті (в онлайновому режимі). Серед таких форм насильства над жертвами – відео шоу наживо та секс-чати;
- зловмисники шантажують жертв з використанням попередньо зібраної інформації, пов'язаної з профілями жертв в Інтернеті, зокрема приватної електронної кореспонденції, облікових записів у соціальних мережах, сімейних стосунків або місць працевлаштування;
- у злочинній діяльності торговці використовують як спеціально створені для цього веб-сайти (наприклад, ескорт-сайти), так і публічні, загальні веб-сайти з оголошеннями працевлаштування;
- онлайнові платформи дозволяють організованим злочинним угрупованням використовувати жертв торгівлі людьми у широких масштабах. Інформація про жертв сексуальної експлуатації, зайнятих у проституції, публікується у спеціально для цього створених добірках, каталогах, доступних в онлайновому режимі в Інтернеті.
- розвиток нових технологій дозволяє організованим злочинним групам віддавати накази і водночас відстежувати своїх жертв по телефону або в Інтернеті.
- співробітництво між злочинними групами на міжнародному рівні або створення злочинних груп, члени яких є громадянами різних країн.
- у контексті сексуальної експлуатації дітей, соціальні медіа дозволяють зловмисникам легко отримувати доступ до потенційних жертв і значно спрощують їх вербування. Можливості і переваги сучасного програмного забезпечення дозволяють зловмисникам практично анонімно поширювати порнографічний контент в онлайновому режимі, у тому числі такий, де показано насильство над дітьми. Зловмисники також можуть користуватися анонімними форумами та онлайновими групами, де окрім обміну зображеннями та відео з дитячою порнографією можна поділитися власним досвідом сексуальної експлуатації дітей або можливими шляхами її здійснення,

дитячого секс-туризму чи запропонувати міркування щодо відповідної поведінки та кроків, які необхідно вжити для захисту заборонених матеріалів у разі втручання правоохоронних органів, напр., під час обстеження комп'ютера (наприклад, шифрування даних);

- використання Інтернету значно полегшило здійснення торгівлі людьми та міжнародну торгівлю з метою сексуальної експлуатації, які вчиняються у змові зі спеціалістами, що експлуатують веб-сайти, та адміністраторами послуг. Очікується, що ця тенденція посилюватиметься і призведе до зростання кількості жінок, які зазнають сексуального насильства у менш видимому онлайновому середовищі.

**ЗАВДАННЯ**

**ОПИШІТЬ ВІДОМІ ВАМ ПРИКЛАДИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ЗДІЙСНЕННЯ ТОРГІВЛІ ЛЮДЬМИ.**

## 2. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА РІЗНИХ СТАДІЯХ ТОРГІВЛІ ЛЮДЬМИ

З точки зору застосування інформаційних технологій здійснення торгівлі людьми (після підшукування засобів, знарядь вчинення злочину та співучасників) можна умовно поділити на декілька *стадій*:

- вербування жертв;
- комунікація, учасниками якої можуть бути суб'єкти вчинення злочину, жертви та треті особи;
- контролювання та експлуатація жертв.

Факультативною стадією може бути одержання коштів від експлуатації жертв.

Використання технологій з метою здійснення торгівлі людьми можна умовно розділити на застосування засобів комп'ютерної техніки (апаратної частини) та використання різного штибу системних та прикладних програмних продуктів (програмної частини).

*Апаратні засоби*, які використовуються для торгівлі людьми, найчастіше включають:

- персональні комп'ютери;
- ноутбуки та нетбуки;
- планшети;
- мобільні телефони;
- смартфони;
- телевізори із функцією SMART;
- телекомунікаційну інфраструктуру;
- системи фото- та відеофіксації;

Вказані засоби, як правило, застосовуються на всіх стадіях торгівлі людьми.

Найбільш часте використання *програмних засобів* на різних стадіях торгівлі людьми наведено у таблиці 1.

*Таблиця 1. Співвідношення стадій та технологій*

| № з/п | Стадія торгівлі людьми | Назва технологій | Приклади |
|---|---|---|---|
| 1. | Вербування жертв | Спеціально-створені веб-сайти | http://www.aemal.org/, http://girl.ddo.com.ua/ |
| | | Комп'ютерні соціальні мережі | «Facebook», «Twitter», «Linkedin», «Instagram», «Вконтакте», «Одноклассники», «Профессионалы» |
| | | Дошки оголошень | www.ss.ua, olx.ua, www.ria.com, www.sudver.com, inforico.ua, www.doshka.net, k4.at.ua, www.stop.kiev.ua, www.ukrboard.com.ua |
| 2. | Комунікація | Електронна пошта | Evolution, KMail, Mozilla Thunderbird, Netscape Mail, Outlook Express, TheBat! |
| | | Чати | http://www.e-chat.co/, http://chat.icq.com/icqchat/, http://www.chat-avenue.com/, http://www.omegle.com/, http://tinychat.com/, http://www.ukranianwomendating.com/, http://www.wireclub.com/places/ukra |
| | | Інтернет-пейджери | ICQ, QIP, MSN, Google Talk, Pidgin, AIM, Trillian, Windows Live Messenger, Yahoo Messenger |
| | | IP-телефонія та інші мультимедійні засоби спілкування | Skype, Viber, Whatsapp |
| | | Забезпечення анонімності | Proxy servers (HTTP, SOCKS, CGI), Dark-net (Tor, 2IP) |
| | | Безпечна передача інформації в мережі | Засоби шифрування (PGP, Signal, Truecrypt), засоби стеганографії |
| 3. | Контролювання та експлуатація | Онлайн-порностудії | http://love-video-chat.ru/online.html http://www.medow.ru |
| | | Мережні сховища (хмари, Peer-to-peer, FTP, Відео-хостинги) | https://cloud.mail.ru, https://www.dropbox.com, https://yadi.sk, https://drive.google.com, https://mega.co.nz, http://www.ge.tt, uTorrent |
| | | Веб-сайти з надання послуг сексуального характеру, продажу органів тощо | http://ukr-biz.net/tags/b1260.htm http://sexkiev.net http://minuet.biz/main |
| 4. | Одержання коштів від експлуатації жертв | Електронні гроші | Яндекс.Деньги, WebMoney, QIWI, PayPal, Moneybookers, Bitcoin, Paxum |
| | | Площадки, які можуть бути використані для легалізації | WesternUnion, MoneyGram+WebMoney, WebMoney+Forex |

Слід мати на увазі, що існує декілька варіантів, якими можуть скористатися торговці людьми для виходу в Інтернет. Найбільш типовими серед них є вихід до мережі:

1) з використанням проводового каналу:

- з помешкання, користувач якого має підключення до мережі Інтернет за договором;
- зі стороннього місця (наприклад, Інтернет-кафе тощо);

2) з використанням безпроводового каналу:

- контрактне підключення;
- передплачене підключення;
- безкоштовний доступ (наприклад, підключення за технологією Wi-Fi або WiMAX у аеропортах, готелях, кафе, незахищені безпроводові мережі тощо).

Найбільш сприятливою є ситуація, коли особа виходить до мережі Інтернет через провайдера, з яким у неї укладено двосторонній договір про обслуговування. У такому випадку є можливість через офіційний запит до провайдера дізнатися установочні дані шуканої особи. Така взаємодія передбачена згідно зі ст. 39 Закону України «Про телекомунікації».

Про приналежність мережного ідентифікатора (тобто тих даних, які використовуються для виходу в мережу) конкретній особі може свідчити:

- налаштування на комп'ютері підозрюваного, які забезпечують доступ через відповідний ідентифікатор;
- наявність на комп'ютері цієї особи повідомлень, надісланих за відповідними контактними даними (жертв торгівлі людьми);
- наявність у провайдера лог-файлів, що засвідчують доступ до ідентифікатора з комп'ютера підозрюваного;
- наявність в інших абонентів повідомлень від підозрюваного з пов'язаного з ним ідентифікатора.

ВИДАЛЕННЯ ІНФОРМАЦІЇ З ІНТЕРНЕТ-РЕСУРСІВ, ЩО МІСТЯТЬ ПРОТИПРАВНИЙ КОНТЕНТ, ПОВ'ЯЗАНИЙ З ТОРГІВЛЕЮ ЛЮДЬМИ, МОЖЕ ВІДБУВАТИСЯ НА ПІДСТАВІ ПОДАННЯ ПРАЦІВНИКА ПОЛІЦІЇ ЗГІДНО З П. 2 ТА П. 3 Ч. 1 СТ. 23 ЗАКОНУ УКРАЇНИ «ПРО НАЦІОНАЛЬНУ ПОЛІЦІЮ».

**ЗАВДАННЯ**

**ЗАПРОПОНУЙТЕ АЛГОРИТМ ДІЙ ПРАЦІВНИКА ПРАВООХОРОННИХ ОРГАНІВ У ВИПАДКУ, КОЛИ ВСТАНОВЛЕНО, ЩО ПРАВОПОРУШНИК ВИХОДИВ ДО МЕРЕЖІ ІЗ ЗАКЛАДУ ШВИДКОГО ХАРЧУВАННЯ, У ЯКОМУ ЗДІЙСНЮЄТЬСЯ НАДАННЯ БЕЗКОШТОВНОГО WI-FI ДОСТУПУ ВІДВІДУВАЧАМ.**

**МОДУЛЬ 2**

# ЗАГАЛЬНІ ПИТАННЯ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ ОРГАНАМИ ДЛЯ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ

## 1. ПОНЯТТЯ «ЕЛЕКТРОННИЙ ДОКАЗ», ЇХ ЗБИРАННЯ, НАЛЕЖНІСТЬ ТА ДОПУСТИМІСТЬ

### ПОНЯТТЯ «ЕЛЕКТРОННИЙ ДОКАЗ»

Відповідно до ст. 94 Кримінального процесуального кодексу (далі – КПК) кожен доказ у кримінальному провадженні має оцінюватися з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення. Саме ці властивості повинні враховуватися слідчим, прокурором, слідчим суддею, судом під час оцінки кожного доказу (ст. 94 КПК).

Пошук інформації при розслідуванні злочинів, пов'язаних із торгівлею людьми, має за основну мету отримання відповідних доказів, на підставі яких суд вирішує питання про вину підозрюваного у вчиненні злочину. Згідно із ч. 2 ст. 84 КПК України процесуальними джерелами доказів є (рис. 1):

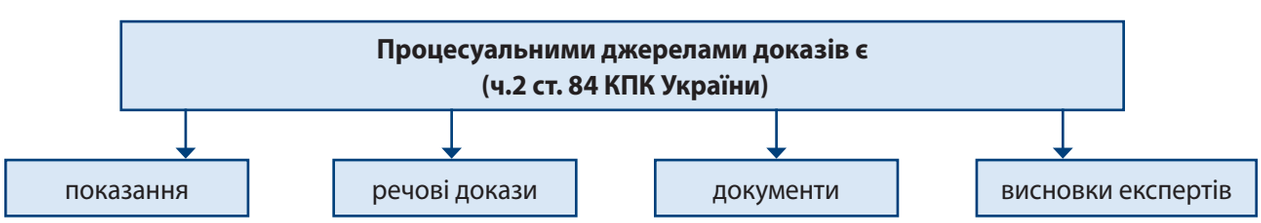



*Рис. 1. Види процесуальних джерел доказів*

Злочинна поведінка може відбиватися у різних цифрових слідах, які можуть стати у встановленому законом порядку доказами.

Цифровими джерелами інформації є електронні пристрої: комп'ютери та периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери і інші портативні пристрої, в тому числі пристрої для зберігання інформації, а також мережа Інтернет. Інформація з цих джерел не має відокремленої фізичної форми.

Цифрові джерела інформації також, як і звичайні джерела доказів, повинні відображати ті ж самі обставини і фактичну інформацію, які існували на момент вчинення правопорушення, і відповідно потребують демонстрації того, що дані не піддавалися змінам, додаванню або видаленню і в них не вносилися (не можуть бути внесені) ніякі правки.

Електронні дані не мають матеріального втілення, тому їх набагато легше змінити або підробити, ніж традиційні форми доказів Для забезпечення довіри до електронних доказів потрібне обчислення ґеш-функції від вилучених даних (за алгоритмами SHA-1, SHA-2 або SHA-3) і подальший контроль отриманого значенням (дайджесту) при оцінці, дослідженні і представленні електронних доказів.

До 2017 року в Україні була відсутня єдина стала термінології, яка б визначала докази, одержані з носіїв цифрових даних, а також чітко не визначено порядок роботи з ними. Тому на практиці нерідко виникають питання щодо правильного оформлення таких доказів та їх представлення в суді.

Одну із перших спроб визначитися із термінами зробила Академія прокуратури України, на початку 2017 року, у навчально-практичному посібнику «Доказування у кримінальному провадженні», де висловили міркування, що **електронні докази** – *це інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах (ЄРДР) та відповідає вимогам ст. 84 КПК України*.

03.10.2017 року Верховна Рада України прийняла проект закону № 6232 «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів». У даному документі пропонується розуміти під електронними доказами інформацію в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатись, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах та ін.), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [23].

Зважаючи на те, що законодавець загалом погодився із введенням в обіг відповідного терміну вважаємо правильним використовувати саме його для позначення доказів, одержаних з цифрових джерел.

## ХАРАКТЕРИСТИКА ЕЛЕКТРОННИХ ДОКАЗІВ

Докази із цифрових джерел інформації в чомусь схожі з традиційними, але в той же час, вони мають низку унікальних характеристик:

- н**еможливість безпосереднього виявлення людиною на фізичному рівні.** Знайти і оцінити, чи належать певні дані до події злочину без застосування програмно-технічних засобів неможливо.
- **нестійкість**. На деяких пристроях або за певних обставин під час звичайної експлуатації пристрою інформація в його пам'яті може змінюватися (а значить, і докази, які там містяться). Наприклад, при розрядці пристрою, нестачі пам'яті або оптимізації розміщення даних система накладає (записує) нову інформацію поверх старої. Комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (великої вологості або високої температури) і електромагнітних полів.
- **зміна або знищення в процесі звичайної експлуатації пристрою**. Пам'ять комп'ютерних пристроїв постійно змінюється за запитом користувачів («зберегти документ», «скопіювати файл») або операційної системи («виділити місце для програми», «тимчасово зберегти дані для обміну між пристроями»). Останнє відбувається автоматично.
- **копіювання без втрати якості**. Цифрові дані можна копіювати необмежену кількість разів, і кожна наступна копія нічим не буде відрізнятися від оригіналу, що дозволяє паралельне і незалежне дослідження різних копій одного і того ж електронного доказу, не зачіпаючи при цьому оригінал.

Результат справи багато в чому залежить від того, наскільки правильно зібрані і оброблені докази, тому слід неухильно дотримуватися загальних принципів роботи з доказами із цифрових джерел інформації.

**Кваліфіковане поводження**. Кожний електронний пристрій має свої унікальні характеристики, які потрібно знати і враховувати при вилученні електронних доказів для зменшення ризику їх ненавмисної модифікації, що у свою чергу може привести до оскарження цілісності доказів в суді і зменшення або навіть знищення їх доказової сили.

**Постійний перегляд і оновлення процедур, методів та інструментів**. Нові технології з'являються і розвиваються з неймовірною швидкістю, тому методи і процедури роботи з доказами із цифрових джерел інформації потрібно постійно переглядати та оновлювати.

**Використання належних процедур, методів та інструментів**. Для отримання вилученими даними доказової сили необхідним є в кожному конкретному випадку вибір таких методів, процедур та інструментів роботи з цифровими доказами, щоб інші незалежні фахівці могли відтворити і перевірити описані в них дії.

**Допустимість**. Кінцева мета використання доказів із цифрових джерел інформації полягає в тому, щоб підтвердити або спростувати спірні факти, тому для визнання допустимості доказів порядок їх отримання повинен відповідати вимогам КПК України.

При оцінці належності електронних доказів із цифрових джерел інформації можуть використовуватися наступні критерії:

- **справжність**. Докази повинні встановлювати факти таким чином, щоб їх не можна було оскаржити і щоб це відображало їх початковий стан;
- **повнота**. Докази, а також зроблені на їх підставі висновки, повинні відображати ситуацію в цілому, а не описувати її в зручному або бажаному світлі;
- **надійність**. Порядок збору і подальшого поводження з доказами не повинен викликати сумнівів щодо їх автентичності та достовірності;
- **переконливість**. Докази повинні бути переконливими щодо фактів, які вони підтверджують. Особи, які покладаються на ці докази в суді, повинні бути здатні переконати суд в їх правдивості.

Існує багато онлайн-джерел інформації, які можуть стати джерелами цифрових доказів при проведенні розслідування. В Керівництві з питань електронних доказів для працівників поліції, прокуратури та судів, розробленого під егідою Ради Європи [24] (далі – Керівництво з питань електронних доказів) наведено перелік найбільш поширених видів онлайн-джерел інформації і даних, які вони можуть містити (табл. 1).

*Таблиця 2. Види онлайн-джерел інформації і даних, які вони містять*

| Джерело | Дані |
|---|---|
| Звичайний веб-сайт | • Вихідний код<br>• Коментарі до коду<br>• Приховані поля<br>• Посилання на зовнішні сайти<br>• Онлайн-реклама<br>• Коди авторизації домену<br>• Коди WebSense/AdSense/SearchSense<br>• Метадані (наприклад, про створення/останню зміну)<br>• Попередні версії на archive.org |
| Сайти соціальних мереж | • Вихідний код<br>• Внутрішні ідентифікатори<br>• Системні компоненти чату<br>• Коди WebSense/AdSense/SearchSense<br>• Метадані (наприклад, про створення/останню зміну) |
| Сайти блогів | • Внутрішні ідентифікатори (блогу, користувача, потоку)<br>• Коди авторизації домену<br>• Mashup: Twitter<br>• Mashup: FaceBook<br>• Mashup: Twitter<br>• Mashup: Picasa / Flickr<br>• Mashup: Скорочені URL<br>• Коди WebSense/AdSense/SearchSense<br>• Метадані (наприклад, про створення/останню зміну) |

| Джерело | Дані |
|---|---|
| Сайти електронної пошти | • Системні компоненти чату<br>• Голосові компоненти чату<br>• Внутрішні ідентифікатори |
| Скорочені URL | • Публічна статистика служби<br>• Дата створення |
| Рекламні мережі | • Внутрішні ідентифікатори<br>• Слід грошових потоків |
| Мережі зберігання контенту | • Внутрішні ідентифікатори (файлу, кошики, користувача, ...)<br>• Ґеші контенту<br>• Контролі версій даних<br>• Сліди грошових потоків |
| Однорангові (P2P) мережі | • DNS-записи<br>• Призначені IP<br>• Використовувані порти<br>• Геш-фрагменти |

## ПРИНЦИПИ РОБОТИ З ЕЛЕКТРОННИМИ ДОКАЗАМИ

При роботі з доказами із цифрових джерел інформації слід використовувати наступні принципи.

### Принцип № 1 – Цілісність даних

*Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв або носіїв інформації, які можуть використовуватися в якості доказів у суді.*

Не можна вносити зміни в дані або пристрій – як до самого обладнання, так і до програмного забезпечення. Необхідно забезпечити цілісність відібраного матеріалу та збереження історії його передачі шляхом безперервного інструментального і документального контролю обчисленого при вилученні даних дайджесту. Цей обов'язок поширюється на всіх осіб, в розпорядження яких переходять ці пристрої або дані;

Доступ до даних пристрою під час його роботи повинен здійснюватися кваліфікованим фахівцем із мінімальним впливом на самі дані.

### Принцип № 2 – Документування процесу

*Необхідно документувати будь-які дії, які здійснюються щодо доказів із цифрових джерел інформації, щоб незалежна третя сторона могла повторити ці дії і отримати аналогічний результат.*

Необхідно максимально точно описати всі дії осіб на місці злочину, щоб за необхідності третя сторона могла відтворити ці дії. Потрібно забезпечити докладний опис процесу пошуку і виїмки, умов зберігання і порядку переміщення електронних даних і зберігати цю інформацію;

Це ж правило застосовується до будь-яких подальших дій по обробці та дослідженню електронних доказів.

### Принцип № 3 – Підтримка спеціалістів/експертів

*Якщо є підстави вважати, що під час огляду/обшуку можуть бути виявлені цифрові джерела інформації, то слід заручитися підтримкою спеціалістів/експертів і по можливості забезпечити їх присутність на місці огляду/обшуку.*

До пошуку і збору електронних доказів бажано залучати спеціалістів із відповідними знаннями і навичками, які можуть бути перевірені незалежною стороною. Спеціалісти повинні мати:

- спеціальні знання і досвід у відповідній сфері;
- досвід і навички поводження із цифровими джерелами інформації;
- розуміння досліджуваного питання;
- необхідні правові знання;
- відповідні комунікаційні навички (що дозволяють їм давати усні та письмові пояснення);
- достатні і необхідні мовні навички;
- правові підстави для залучення у процесуальні дії.

### Принцип № 4 – Належна підготовка

*Якщо під час огляду/обшуку не присутні спеціалісти із цифрових джерел інформації, то особи, які здійснюють слідчі дії на місці огляду/обшуку, повинні володіти необхідними знаннями для виявлення і збору доказів.*

Збір доказів і/або доступ до оригінальних даних на електронних пристроях і цифрових накопичувачах слід проводити особам, які мають необхідну підготовку і забезпечує їм можливість пояснювати необхідність і наслідки своїх дій.

### Принцип № 5 – Законність

*Особи і органи, які ведуть розслідування, зобов'язані дотримуватися законодавства, загальних криміналістичних та процесуальних принципів.*

Як вже було зазначено докази, одержані в рамках розслідування, повинні відповідати вимогам достовірності, належності і допустимості. Вказані вимоги висуваються як до форми одержаних відомостей, так і їх змісту. Ці вимоги є справедливими і для електронних доказів. Для того, щоб грамотно задокументувати відомості з цифрових джерел, потрібно враховувати функціональні особливості технологій, з використанням яких їх було створено, збережено, передано тощо.

Особливо часто правоохоронним органам доводиться стикатися з ситуацією, коли потрібно задокументувати веб-контент, тобто інформацію з веб-сторінок. У рамках виконання цієї процедури можуть виникати певні складнощі, зважаючи на те, що правопорушники, провайдери, хостери здатні оперативно змінювати описані сторінки та місце їх розміщення.

На теперішній час вже напрацьована певна практика відповідного документування та використання одержаних доказів у кримінальному процесі. Серед них потрібно виділити наступні:

- *фіксація вихідного коду веб-сторінки* (наприклад, ззовні проста персональна сторінка у Facebook у своєму вихідному веб-коді може містити десятки посилань на ідентифікатор користувача, а також сотні ідентифікаторів зображень й інших користувачів, які є друзями. Приховати або замаскувати ці посилання у вихідному коді – завдання із розряду нездійсненних. Для збереження вихідного HTML-коду веб-сторінки достатньо у браузері вибрати опцію «Зберегти сторінку як» або «Файл – Зберегти як». Також у контекстному меню є опція «Подивитися вихідний код», який можна зберегти як текстовий файл. Після збереження відповідних файлів потрібно обчислити їх дайджест (ґеш-функцію SHA-2) з метою подальшого контролю цілісності отриманої інформації). З метою фіксації вмісту усього веб-сайту, а не окремої веб-сторінки, можна створити копію сайту для перегляду в автономному режимі, наприклад, за допомогою програми HTTrack Website Copier, яка завантажує пов'язані веб-об'єкти за визначеною глибиною і дозволяє відкрити веб-сайт з усіма зображеннями в автономному режимі. Це може стати в нагоді, коли потрібно показати вміст веб-сайту в суді. Але

потрібно розуміти, що в цьому випадку змінюється вихідний код веб-сайту і такі інструменти часто не в змозі скопіювати цілий веб-сайт разом з усіма пов'язаними медіа-файлами і сайтами;

- *зйомка відеокамерою* (перед зйомкою основного джерела доречним буде зняти процес відкриття будь-якого відомого сайту новин для отримання додаткової часової мітки. Підробити відеозапис набагато складніше, ніж скріншот веб-сторінки. Не зайвим буде, також обчислити дайджест отриманих відеофайлів. При використанні відеокамери потрібно знати про таке явище, як аберація об'єктива, яке виникає за рахунок спотворень на матриці відеокамери. Аберацію об'єктива відеокамери можна звірити з відзнятими матеріалами, що допоможе підтвердити використання саме цього пристрою для отримання конкретного відеозапису);
- *відеозахоплення екрану* (video screen capture). Замість відеокамери можна використовувати спеціальні програми для цифрового відеозапису інформації, яка виводиться на екран. Доречним є використання безкоштовних програм з відкритим вихідним кодом. Потрібно пам'ятати, що запис буде використовуватися в якості доказу у судовому процесі і відповідно відео не може містити ніяких додаткових ефектів, редагувань або змін кодування для програвання на інших пристроях. Доцільно здійснювати запис всього екрану цілком, що підвищує прозорість процесу збору доказів. Якщо буде потреба у збільшенні фрагменту екрану, щоб підкреслити якусь деталь, то можна використати функцію збереження об'єкта веб-браузера або екранний збільшувач операційної системи, не можна після запису редагувати відеофайл для збільшення окремих деталей. Відеозапис має розміщуватися в одному файлі та не мати розривів і пауз.

Використання відеозапису має свої недоліки. Наприклад, на спеціальному сервері може бути створена підроблена сторінка або сайт, а на комп'ютері змінені DNS-записи або маршрутизація, і тоді замість оригінального веб-сайту користувач потрапить на підроблену сторінку. Для підтвердження справжності веб-сторінки в подібних ситуаціях можна записати процес отримання непрямого доступу (через проксі) до веб-сторінки, наприклад через сервіс Google Translate. Для цього в адресному рядку браузеру потрібно ввести адресу потрібного сайту (target.net) наступним чином:

https://translate.google.com/translate?sl=en&tl=en&u=http://target.net,

де виставити напрям перекладу на оригінальну мову веб-сторінки. В цьому випадку сервер Google підключається до серверу, де знаходиться потрібна веб-сторінка, запитує зазначений веб-ресурс і передає отримані дані оглядачу. Якщо записати процес перевірки на відео, то можна підтвердити, що здійснюється огляд справжньої веб-сторінки, при цьому час і дата відвідування Google Translate, IP-адреса і URL будуть відображені в журналах серверів Google.

Щоб збільшити доказову силу відеозапису, можна продемонструвати на камеру додаткові технічні дані досліджуваної веб-сторінки. Наприклад, можна скористатися сервісом http://www.webconfs.com/http-header-check.php, який відображає HTTP-заголовки заданого домена. Як правило, заголовок містить поле «дата», в якому міститься дата і локальний час надана веб-сервером, де розміщений сайт. На рис. 2 наведено приклад HTTP-заголовку для домену www.ukr.net.

- *відповідь провайдера на запит щодо змісту сайту.*

Відповідні матеріали можливо долучити до матеріалів кримінального провадження як докази.

Для фіксації технічних аспектів процесу розслідування можна скористатися аналізатором протоколів, наприклад, програмою з відкритим вихідним кодом WireShark. Аналізатор протоколів фіксує усі дані, в тому числі і зашифровані, за всіма протоколами. Зашифровані дані мають обмежену цінність як доказ, якщо не буде встановлений ключ шифрування.

При роботі з веб-орієнтованими даними в якості компромісу між простотою і деталізацією процесу можна запустити веб-сеанс через реєструючий проксі-сервер, який знаходиться між веб-браузером і цільовим веб-сервером. Цей спосіб є простішим з технічної точки зору і його можна поєднати з різними сервісами, які в режимі реального часу підписують і проставляють часові мітки в створюваних журналах реєстрації.

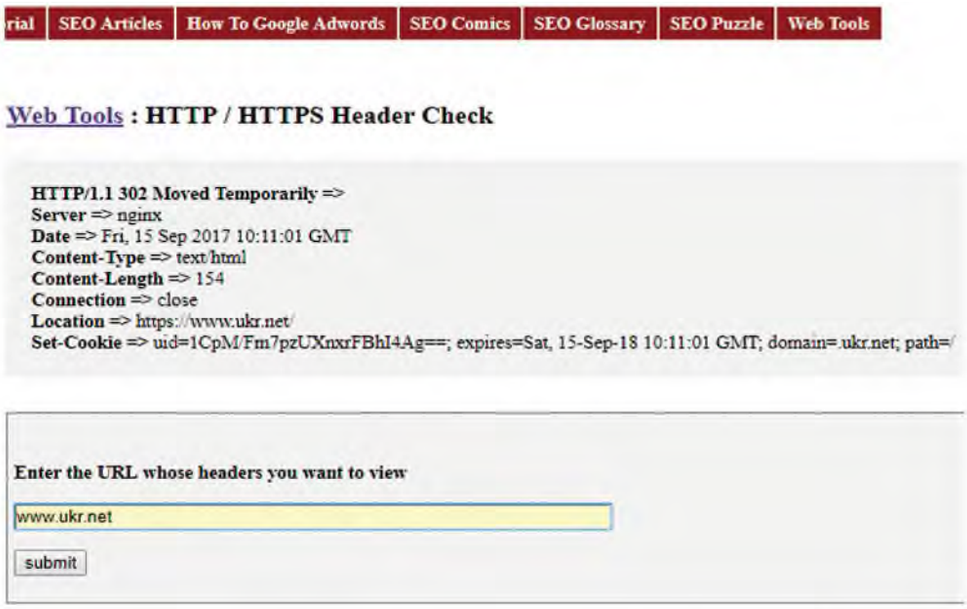



*Рис. 2. HTTP-заголовок домену www.ukr.net від сервісу www.webconfs.com*

Ще одним методом забезпечення достовірності електронних доказів може бути проставлення довірчих часових міток, тобто фіксація довіреною третьою стороною часу створення або зміни електронного документа. При цьому, як правило, використовуватися і електронний цифровий підпис. Практична реалізації цього методу потребує використання сервісів засвідчення часу електронних документів, наприклад, https://tsa.safecreative.org.

Закріплення електронних доказів, одержаних в результаті передбачених КПК, слідчих чи негласних слідчих (розшукових) дій здійснюється з дотриманням декількох вимог до форми і змісту. Перша група вимог передбачає процесуальне оформлення відповідних протоколів, залучення у разі необхідності спеціаліста та понятих, вжиття заходів із належного збереження цифрових носіїв даних, важливих для кримінального процесу. Друга група вимог висувається до змістовного наповнення інформації, її якісної та кількісної складової. В останньому випадку слід особливу увагу звернути на повноту одержаних відомостей, для того, щоб вони у подальшому могли бути представлені як в судовому засіданні, так і передані на дослідження експерту.

Слід пам'ятати, що хоча в окремих слідчих діях участь понятих не є обов'язковою, але з іншого боку вона надає більшої вагомості одержаним доказам. При цьому поняті мають бути обізнаними, хоча б на базовому рівні, в інформаційних технологіях, а мова протоколювання повинна бути максимально зрозумілою для пересічної особи. У рамках фіксації електронних доказів також слід орієнтувати слідчого на застосування носіїв інформації, які не можуть бути повторно перезаписані, для того щоб у подальшому обвинувачений або сторона захисту не могли стверджувати про створення дописів в електронних носіях з боку правоохоронців. Також для уникнення суперечок можна додатково виносити на експертизу питання про наявність в електронних доказах ознак стороннього втручання, зокрема монтажу.

Самі носії інформації, а також інші докази, одержані в результаті проведення слідчих та негласних слідчих (розшукових) дій, повинні бути належним чином описуватися, упаковуватися та опечатуватися, щоб убезпечити їх від пошкодження і втрати доказових властивостей.

На міжнародному рівні прокурорам рекомендовано не подавати проти обвинувачуваних доказів, які, як їм відомо, або як передбачається на достатніх підставах, були отримані за допомогою джерел або методів, що суперечать закону. У разі яких-небудь сумнівів прокурори повинні запросити суд установити прийнятність цих доказів (п. 28 Рекомендації Rec (2000) 19 Комітету Міністрів Ради Європи державам-членам щодо ролі прокуратури в системі кримінального правосуддя, ухваленої 6 жовтня 2000 року) [25, п. 28].

## 2. ЗАГАЛЬНІ ОСОБЛИВОСТІ РОБОТИ З ДОКАЗАМИ, ОДЕРЖАНИМ В РЕЗУЛЬТАТІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

При проведенні досудового розслідування злочинів правоохоронні оргнаи нерідко зустрічаються з ситуацією коли гласні слідчі (розшукові) дії не в повній мірі забезпечують отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні.

Таким прикладом можуть бути кримінальні провадження в яких відсутні свідки злочину, а показання потерпілого, який має сумнівну репутацію, в судовому засіданні будуть спростовані показами обвинуваченого.

Саме, тому при проведенні досудового розслідування мають широко використовуватись негласні слідчі (розшукові) дії (далі – НСРД), які дозволяють отримати інформацію про злочин або особу, яка його вчинила, без її відома, з'ясувати її дійсні наміри, виявити обставини, що викривають, так і ті, що виправдовують майбутнього підозрюваного, обвинуваченого.

До НСРД, які найчастіше можуть використовуватись при проведенні досудового розслідування злочинів торгівлі людьми слід віднести:

1. Аудіо-, відеоконтроль особи (ст. 260 КПК України), який полягає в негласній фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо;

ТАК, СВЯТОШИНСЬКИЙ РАЙОННИЙ СУД М. КИЄВА ВІД 14.12.2015 РОКУ У ВИРОКУ ЗА Ч.2 СТ.149 КК УКРАЇНИ ВИЗНАВ ДОПУСТИМИМ ТА НАЛЕЖНИМ ДОКАЗОМ ПРОТОКОЛ ПРО РЕЗУЛЬТАТИ ПРОВЕДЕННЯ НЕГЛАСНОЇ СЛІДЧОЇ (РОЗШУКОВОЇ) ДІЇ – АУДІО-, ВІДЕОКОНТРОЛЬ ОСОБИ, ЯКИЙ МІСТИВ СТЕНОГРАМУ РОЗМОВИ, В ЯКІЙ ОБВИНУВАЧЕНА ПОВІДОМЛЯЄ, ЩО ПОТЕРПІЛУ ЗУСТРІНУТЬ У ІНШІЙ КРАЇНІ І СПОЧАТКУ ЇЙ НЕОБХІДНО БУДЕ ВІДПРАЦЮВАТИ 6000 ДОЛАРІВ США ЗА КВИТОК, ВІЗУ, САЛОН КРАСИ ДЛЯ ПІДТРИМАННЯ ВІДПОВІДНОЇ ЗОВНІШНОСТІ, ПРОЖИВАННЯ ТОЩО, А ТАКОЖ ПРО УМОВИ ОПЛАТИ ЗА СЕКСУАЛЬНІ ПОСЛУГИ – 400 ДОЛАРІВ США ЗА ГОДИНУ. ПРИ ЦЬОМУ ОБВИНУВАЧЕНА ФОТОГРАФУЄ ПОТЕРПІЛУ НА КАМЕРУ МОБІЛЬНОГО ТЕЛЕФОНУ І КОМУСЬ В ТЕЛЕФОННІЙ РОЗМОВІ ПОВІДОМЛЯЄ ПРО ЇЇ ПРИЛІТ.

2. Зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), дозволяє за допомогою спеціальних технічних засобів, встановлених на транспортних телекомунікаційних мережах, здійснювати спостереження, відбір та фіксацію змісту телефонних розмов, контролювати іншу інформацію, яка передаються телефонними каналами зв'язку, (SMS, MMS-повідомлення, передача відомостей факсимільним зв'язком, модемним зв'язком тощо), стосовно вербування, комунікації з особами, що піддаються трудовій або сексуальній експлуатації, їх переміщення за кордон, контролю за умовами їх експлуатації, а також отримання за це коштів.

Крім того, вказана негласна слідча (розшукова) дія може проводиться з метою отримання відомостей, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі. Такі заходи можуть здійснюватися у тому числі для отримання відомостей з каналу зв'язку за IP-адресою мережі Інтернет, в результаті чого фіксується інформація про діяльність т.з. порностудій, інших місць, що використовуються для сексуальної експлуатації.

Протоколи за наслідками проведення вищезазначеної НСРД можуть містити дані про зустрічі і телефонні розмови злочинців з потерпілими в яких оговорюються умови проживання останніх, отримання ними винагороди за надання послуг сексуального характеру, характер таких послуг, порядок виплати боргу за відправку до іншої країни, харчування, опис перспектив достатнього і стабільного заробітку з позитивного боку. Зняттям інформації з транспортних телекомунікаційних мереж також може підтверджуватись уразливий стан потерпілих, оскільки останні нерідко у телефонних розмовах повідомляють злочинців

про тяжкі захворювання родичів, необхідність коштовного лікування, переїзд з непідконтрольної Україні території, низькі статки.

Злочинці ж спілкуючись між собою називають потерпілих товаром, оговорюючи при цьому ціни, що свідчить про здійснення незаконних угод, об'єктом якої є людина.

3. Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України) полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в комп'ютерах, автоматичних системах, комп'ютерній мережі, інших електронних носіях інформації щодо обставин функціонування порностудій, місць надання сексуальних послуг, підпільних цехів, інших місць, де здійснюється сексуальна або трудова експлуатація.
4. Обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України) полягає в таємному проникненні слідчого чи уповноваженої особи без відома власника чи володільця, приховано, під псевдонімом або із застосуванням технічних засобів у приміщення та інше володіння для встановлення технічних засобів аудіо-, відеоконтролю особи або безпосередньо з метою виявлення і фіксації слідів злочину, проведення огляду, виявлення документів, речей, що мають значення для досудового розслідування, виготовлення копій чи їх зразків, виявлення осіб, які розшукуються, або з іншою метою для досягнення цілей кримінального провадження.
5. Спостереження за особою в публічно доступних місцях (ст. 269 КПК України) полягає у візуальному спостереженні за особою слідчим чи уповноваженою особою для фіксації її пересування, контактів, поведінки, перебування в певному, публічно доступному місці тощо або застосуванні з цією метою спеціальних технічних засобів для спостереження.
6. Контроль за вчиненням злочину (ст. 271 КПК України) у формах оперативної закупки, спеціального слідчого експерименту.

*Оперативна закупка* полягає в імітації придбання або отримання, у тому числі безоплатного, у фізичних та юридичних осіб незалежно від форм власності товару, обіг якого обмежений чи заборонений чинним законодавством, з метою викриття і документування факту вчинення злочину та особи, яка його вчинила.

*Спеціальний слідчий експеримент* полягає у створенні слідчим та оперативним підрозділом відповідних умов в обстановці, максимально наближеній до реальної, з метою перевірки дійсних намірів певної особи, у діях якої вбачаються ознаки тяжкого чи особливо тяжкого злочину, спостереження за її поведінкою та прийняттям нею рішень щодо вчинення злочину.

*Імітування обстановки злочину* полягає в діях слідчого, уповноваженої особи, з використанням імітаційних засобів, які створюють у оточуючих уяву про вчинення реального злочину, з метою його запобігання та викриття відомої чи невідомої особи (осіб), яка планувала чи замовляла його вчинення

ПРИКЛАД ВДАЛОГО ПРОВЕДЕННЯ КОНТРОЛЮ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ ВІДЗНАЧЕНИЙ У ВИРОКУ АПЕЛЯЦІЙНОГО СУДУ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ ВІД 29.06.2017, ЯКИМ КОНСТАТОВАНО ЗБІР СТОРОНОЮ ОБВИНУВАЧЕННЯ НАЛЕЖНИХ ТА ДОПУСТИМИХ ДОКАЗІВ.

ТАК, ЗГІДНО ВИРОКУ, ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТ. 149 КК УКРАЇНИ, ПРОКУРОРОМ ВИНЕСЕНО ПОСТАНОВУ ПРО КОНТРОЛЬ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ У ФОРМІ СПЕЦІАЛЬНОГО СЛІДЧОГО ЕКСПЕРИМЕНТУ ТА ПОГОДЖЕНО КЛОПОТАННЯ СЛІДЧОГО ПРО ПРОВЕДЕННЯ НСРД, А САМЕ ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ АУДІО- І ВІДЕОФІКСАЦІЇ, З ПРОТОКОЛІВ ПРОВЕДЕННЯ ЯКИХ ВСТАНОВЛЕНО, ЩО ОБВИНУВАЧЕНА ПІД ЧАС ПРОВЕДЕННЯ СПІВБЕСІДИ З ПОТЕРПІЛИМИ ЗДІЙСНИЛА ЇХ ВЕРБОВКУ ТА ПЛАНУВАННЯ ЇХ ПЕРЕПРАВЛЕННЯ В М. САНКТ-ПЕТЕРБУРГ, РОСІЙСЬКОЇ ФЕДЕРАЦІЇ З МЕТОЮ ПОДАЛЬШОЇ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ, ВІДПОВІДАЛА НА ПИТАННЯ ДІВЧАТ, ОПИСУВАЛИ ДЕТАЛІ ПОЇЗДКИ ТА ПОДРОБИЦІ ОПЛАТИ ЗА НАДАННЯ ІНТИМНИХ ПОСЛУГ ТА УМОВИ ПРОЖИВАННЯ [26].

Хоча специфіка розслідування злочину, передбаченого ст. 149 КК України передбачає спостереження за поведінкою підозрюваного з метою перевірки його дійсних намірів та прийняттям рішень у обстановці максимально наближеній до реальної, що відповідає опису такої НСРД, як контроль за вчиненням злочину у формі спеціального слідчого експерименту, аналіз судових рішень свідчить про факти проведення контролю за вчиненням злочину і у формі імітування обстановки злочину.

ТАК, НАПРИКЛАД ВИРОКОМ СВЯТОШИНСЬКОГО РАЙОННОГО СУДУ М. КИЄВА ВІД 14.12.2015 РОКУ ГРОМАДЯНКУ УКРАЇНИ ВИЗНАНА ВИНУВАТОЮ У ПРЕД'ЯВЛЕНОМУ ОБВИНУВАЧЕННІ ЗА Ч.2 СТ.149 КК УКРАЇНИ.

ПІД ЧАС РОЗСЛІДУВАННЯ ПРОВЕДЕНО КОНТРОЛЬ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ, У ФОРМІ ІМІТУВАННЯ ОБСТАНОВКИ ЗЛОЧИНУ. ПРИ ЦЬОМУ ПРОКУРОР НАДАВ ДОРУЧЕННЯ ПРО ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ УПОВНОВАЖЕНИМ ОСОБАМ УБЗПТЛ ГУ МВС УКРАЇНИ В М. КИЄВІ.

ЗГІДНО З ПРОТОКОЛОМ ПРО ПРОВЕДЕННЯ НЕГЛАСНОЇ СЛІДЧОЇ (РОЗШУКОВОЇ) ДІЇ – КОНТРОЛЮ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ У ФОРМІ ІМІТУВАННЯ ОБСТАНОВКИ ЗЛОЧИНУ ПОТЕРПІЛА З МЕТОЮ ЗАПОБІГАННЯ ВЧИНЕННЯ ЗЛОЧИНУ ТА ВИКРИТТЯ ЗЛОЧИНУ ПОГОДИЛАСЯ НА ПРОПОЗИЦІЮ ВИЇХАТИ ДО М. ДУБАЇ З МЕТОЮ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ. СПІВРОБІТНИКАМИ УБЗПТЛ ГУ МВС УКРАЇНИ В М. КИЄВІ ПРОВЕДЕНИЙ ІНСТРУКТАЖ ПОТЕРПІЛОЇ НА ПРЕДМЕТ ІМІТУВАННЯ ЗАЦІКАВЛЕНОСТІ ВИЇЗДУ ДО М. ДУБАЇ. В ПОДАЛЬШОМУ ОБВИНУВАЧЕНА ОРГАНІЗУВАЛА ВИЛІТ ПОТЕРПІЛОЇ У М. ДУБАЇ З МІЖНАРОДНОГО АЕРОПОРТУ «БОРИСПІЛЬ» ПІСЛЯ ЧОГО БУЛА ЗАПРОШЕНА ДО КІМНАТИ ПРИЙОМУ ГРОМАДЯН СПІВРОБІТНИКАМИ УБЗПТЛ ГУ МВС УКРАЇНИ В М. КИЄВІ, ДЕ В ПРИСУТНОСТІ ПОНЯТИХ ПРОВЕДЕНО ОГЛЯД МІСЦЯ ПОДІЇ ЗІ СКЛАДАННЯМ ВІДПОВІДНОГО ПРОТОКОЛУ [27].

АПЕЛЯЦІЙНИЙ СУД ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ У ВИРОКУ ВІД 29.06.2017 ЗА Ч. 2 СТ. 149 КК УКРАЇНИ, ВИЗНАВ НАЛЕЖНИМ ТА ДОПУСТИМИМ ДОКАЗОМ ПОСТАНОВУ ПРОКУРОРА ПРО КОНТРОЛЬ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ У ФОРМІ СПЕЦІАЛЬНОГО СЛІДЧОГО ЕКСПЕРИМЕНТУ ТА ПРОТОКОЛ ПРО РЕЗУЛЬТАТИ КОНТРОЛЮ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ ЯКИМИ ПІДТВЕРДЖЕНО ФАКТ ВЕРБОВКИ ТА ПЛАНУВАННЯ ПЕРЕПРАВЛЕННЯ ОСІБ ЖІНОЧОЇ СТАТІ ДО М. САНКТ-ПЕТЕРБУРГ, РОСІЙСЬКОЇ ФЕДЕРАЦІЇ З МЕТОЮ ПОДАЛЬШОЇ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ.

ОДНОЧАСНО СУД ВИЗНАВ БЕЗПІДСТАВНИМИ ДОВОДИ ЗАХИСНИКА ПРО ТЕ, ЩО ЗЛОЧИН НЕ БУЛО Б СКОЄНО БЕЗ ВТРУЧАННЯ ПРАВООХОРОННИХ ОРГАНІВ, ОСКІЛЬКИ ДІЇ ПРАВООХОРОННИХ ОРГАНІВ ПРИ ЗДІЙСНЕННІ КОНТРОЛЮ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ НЕ БУЛИ АКТИВНИМИ, З ЇХ БОКУ НЕ ВСТАНОВЛЕНО СПОНУКАННЯ ДО ВЧИНЕННЯ ЗЛОЧИНУ, ТАКИХ ЯК, ПРОЯВ ІНІЦІАТИВИ У КОНТАКТАХ З ОСОБОЮ, ПОВТОРНІ ПРОПОЗИЦІЇ, НАПОЛЕГЛИВІ НАГАДУВАННЯ, А НА МОМЕНТ КОНТРОЛЮ ЗА ВЧИНЕННЯМ ЗЛОЧИНУ У ПРАВООХОРОННИХ ОРГАНІВ БУЛИ ОБ'ЄКТИВНІ ДАНІ ПРО ТЕ, ЩО ОБВИНУВАЧЕНА БУЛА ВТЯГНУТА У ЗЛОЧИННУ ДІЯЛЬНІСТЬ І ЙМОВІРНІСТЬ ВЧИНЕННЯ НЕЮ ЗЛОЧИНУ БУЛА СУТТЄВОЮ [27].

7. Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України) полягає в організації слідчим і оперативним підрозділом введення уповноваженої ними особи, яка відповідно до закону виконує спеціальне завдання, в організовану групу чи злочинну організацію під легендою прикриття для отримання речей і документів, відомостей про її структуру, способи і методи злочинної діяльності, які мають значення для розслідування злочину або злочинів, які вчиняються цими групами.
8. Установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, у тому числі мобільного терміналу, систем зв'язку та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження.

Використання інституту негласних слідчих (розшукових) дій у досудовому розслідуванні злочинів щодо торгівлі людьми, особливо організованих їхніх форм, є дієвим засобом боротьби з цим злочином і, водночас, покладає на слідчі органи та слідчих суддів додаткові обов'язки щодо дотримання прав людини і належної процедури в процесі втручання у приватну сферу особи, яку можуть зачіпати такі дії.

Оскільки злочин, передбачений ч. 1 ст. 149 КК України, є тяжким, а ч. ч. 2, 3 ст. 149 – особливо тяжким, у кожному кримінальному провадженні про торгівлю людьми КПК України надає право проводити негласні слідчі (розшукові) дії, які в істотній у кримінальних справах щодо торгівлі людьми мірі втручаються у права і свободи людини. Водночас закон дозволяє проводити їх лише у разі, коли відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб, і після отримання дозволу слідчого судді (ч. 2 ст. 146 КПК України). Слід мати на увазі, що на провадження про торгівлю людьми не поширюється дія ст. 250 КПК України щодо можливості проведення негласної слідчої (розшукової) дії до винесення ухвали слідчого судді у певних виняткових невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого чи особливо тяжкого злочину, оскільки розділ III КК України не зазначений у відповідному вичерпному переліку цієї норми.

Фіксація ходу і результатів негласних слідчих (розшукових) дій за чинним КПК має відповідати загальним правилам фіксації кримінального провадження. Результати негласних слідчих (розшукових) дій використовуватимуться при доказуванні на тих самих підставах, що й результати проведення інших слідчих дій.

Негласні слідчі (розшукові) дій за чинним кримінальним процесуальним законодавством України вправі проводити слідчий, який здійснює досудове розслідування, або за дорученням слідчого — уповноважені оперативні підрозділи. У чинному КПК України підстави та порядок проведення негласних слідчих (розшукових) дій детально врегульовано у ст.ст. 246-275. Недотримання встановленого законом порядку проведення негласних слідчих (розшукових) дій буде мати своїм наслідком визнання судом недопустимими зібрані у такий спосіб докази.

Більш детально питання проведення негласних слідчих (розшукових) дій та використання їхніх результатів у кримінальному провадженні регулює Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їхніх результатів у кримінальному провадженні, яка була затверджена спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України та Міністерства юстиції України від 16.11.2012 року № 114/1042/516/936/1687/5 [28, с. 27].

Використання у доказуванні даних, отриманих у порядку НСРД, все ж дещо відрізняється від використання з такою ж метою інформації, отриманої під час проведення слідчих (розшукових) дій, оскільки передбачає необхідність зняття з інформації грифа секретності.

Аналіз наведених прикладів судової практики переконливо демонструє, що і ЄСПЛ, і національні суди України різних інстанцій дотримуються єдиної позиції, відповідно до якої для перевірки допустимості доказової інформації, отриманої за результатами НСРД, суд повинен мати можливість ознайомитися із документами, якими надано дозвіл на зазначену слідчу дію. За умови відсутності у суду такої можливості, результати відповідної НСРД можуть оцінюватися як недопустимі докази та не можуть бути використані при обґрунтуванні судового рішення

Власне процедура засекречування та розсекречування будь-яких матеріальних носіїв інформації стосовно НСРД (постанов слідчого, прокурора про проведення НСРД, клопотань про дозвіл на проведення НСРД, ухвал слідчих суддів, протоколів за результатами проведення НСРД тощо) є єдиною та регламентується розділом 5 Інструкції і в цілому зводиться до такого алгоритму:

- засекречування матеріальних носіїв інформації здійснюється слідчим, прокурором, працівником уповноваженого оперативного підрозділу, слідчим суддею шляхом надання на підставі Зводу відомостей, що становлять державну таємницю, відповідному документу грифа секретності;

- після завершення проведення НСРД грифи секретності матеріальних носіїв інформації щодо їх проведення підлягають розсекреченню на підставі рішення прокурора, який здійснює повноваження прокурора в конкретному кримінальному провадженні у формі процесуального керівництва досудовим розслідуванням, з урахуванням обставин кримінального провадження та необхідності використання матеріалів НСРД як доказів. Таке рішення оформлюється постановою прокурора, який здійснює повноваження прокурора в конкретному кримінальному провадженні у формі процесуального керівництва досудовим розслідуванням, що погоджується керівником прокуратури;
- після отримання клопотання про необхідність скасування грифів секретності матеріальних носіїв інформації щодо проведення НСРД та відповідних документів керівником органу, де здійснювалося їх засекречування, створюється експертна комісія з питань таємниць, якій доручається підготовка рішень про скасування грифів секретності;
- експертна комісія створюється у складі не менше трьох осіб, зокрема фахівців, які мають відповідний рівень знань та досвід роботи у сфері охорони державної таємниці (залежно від органу: слідчий суддя, слідчий, прокурор у конкретному кримінальному провадженні, керівник слідчого чи оперативного підрозділу), працівники режимно-секретних підрозділів, які мають допуск до державної таємниці відповідної форми;
- скасування грифів секретності здійснюється працівниками режимно-секретного органу шляхом закреслення однією тонкою лінією попереднього грифа секретності та написання знизу або поруч позначки «Не таємно». Такі виправлення із зазначенням дати засвідчуються підписом начальника режимно-секретного органу або його заступника та скріплюється печаткою режимно-секретного органу [29].

СЛІД ПАМ'ЯТАТИ, ЩО ВІДПОВІДНО ДО ПРАВОВОГО ВИСНОВКУ ВЕРХОВНОГО СУДУ УКРАЇНИ ЗРОБЛЕНОГО 16.03.2017 У СПРАВІ № 5-364КС16 НЕВІДКРИТТЯ МАТЕРІАЛІВ СТОРОНАМИ В ПОРЯДКУ СТАТТІ 290 КПК УКРАЇНИ Є ОКРЕМОЮ ПІДСТАВОЮ ДЛЯ ВИЗНАННЯ ТАКИХ МАТЕРІАЛІВ НЕДОПУСТИМИМИ ЯК ДОКАЗИ.

ПРИ ЦЬОМУ, ВІДКРИТТЮ, ОКРІМ ПРОТОКОЛІВ, У ЯКИХ ЗАФІКСОВАНО ХІД ТА РЕЗУЛЬТАТИ ПРОВЕДЕННЯ ПЕВНИХ ДІЙ, В ОБОВ'ЯЗКОВОМУ ПОРЯДКУ ПІДЛЯГАЮТЬ І МАТЕРІАЛИ, ЯКІ Є ПРАВОВОЮ ПІДСТАВОЮ ПРОВЕДЕННЯ ТАКИХ ДІЙ (УХВАЛИ, ПОСТАНОВИ, КЛОПОТАННЯ), ЩО ЗАБЕЗПЕЧИТЬ МОЖЛИВІСТЬ ПЕРЕВІРКИ СТОРОНОЮ ЗАХИСТУ ТА СУДОМ ДОПУСТИМОСТІ РЕЗУЛЬТАТІВ ТАКИХ ДІЙ ЯК ДОКАЗІВ [30].

Окремо потрібно зупинитись на дотриманні вимог закону при оформленні результатів НСРД.

Так, фіксація ходу і результатів негласних слідчих (розшукових) дій повинна відповідати загальним правилам фіксації кримінального провадження, передбаченим цим КПК України. За результатами проведення негласної слідчої (розшукової) дії складається протокол, до якого в разі необхідності долучаються додатки.

Проводити негласні слідчі (розшукові) дії, а отже і складати протоколи про їх результати, має право слідчий, який здійснює досудове розслідування злочину, або за його дорученням – уповноважені оперативні підрозділи Національної поліції, органів безпеки, Національного антикорупційного бюро України, Державного бюро розслідувань, органів, що здійснюють контроль за додержанням податкового і митного законодавства, органів Державної кримінально-виконавчої служби України, органів Державної прикордонної служби України. За рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій можуть залучатися також інші особи.

Таким чином, саме доручення слідчого або рішення слідчого чи прокурора, яке приймається у формі постанови надає право оперативному працівнику, складати протоколи про результати НСРД.

Однак, як свідчить практика, таке доручення на відміну від протоколів про результати НСРД та ухвал слідчого судді про дозвіл на їх проведення практично не розсекречуються, хоча воно є єдиною підставою для оперативного працівника складати протокол.

Тому, процесуальний керівник у кримінальному провадженні повинен приймати рішення про розсекречення не лише стосовно клопотань, ухвал, протоколів, а й щодо доручень слідчих про проведення НСРД.

Недотримання такої процедури може призвести до визнання доказу недопустимим з тих підстав, що прокурор за відсутності доручення, з якого знято гриф секретності, не зможе довести у судовому засіданні, законність складання оперативним працівником відповідного протоколу. За таких обставин суд, пославшись на ч. 3 ст. 87 КПК України, визнає недопустимими докази, що було отримано після початку кримінального провадження шляхом реалізації органами досудового розслідування чи прокуратури своїх повноважень, не передбачених цим Кодексом, для забезпечення досудового розслідування кримінальних правопорушень.

## 3. ОКРЕМІ АСПЕКТИ АНАЛІТИЧНОЇ РОБОТИ ПРАВООХОРОННИХ ОРГАНІВ

Зміщення акцентів на превентивну діяльність замість реактивної в частині поліцейського реагування на протиправну діяльність зумовлює пошук ефективних рішень, які б допомогли швидко покращити стан оперативної обстановки в країні, зокрема в частині протидії злочинам у сфері торгівлі людьми. Для вирішення цього завдання вбачається корисним вивчення зарубіжних практик, використання яких позитивно вплинуло на якість правоохоронної діяльності. У цьому контексті слід звернути увагу на застосовувану західними правоохоронними органами методологію кримінальної (поліцейської) розвідки (criminal intelligence process).

З метою організації ефективного та якісного виконання обов'язків, покладених на поліцейських Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми Національної поліції України наказом Національної поліції України від 17.07.2017 року № 719 створено сектор кримінального аналізу, а наказом від 08.08.2017 року № 827 – сектор боротьби зі злочинами у сфері працевлаштування за кордоном.

Методологія кримінальної розвідки покладена в основу низки спеціалізованих програмних рішень для правоохоронних органів (Crimeview Server, My Neighborhood Map System, CrimeReports Plus). У цьому сенсі слід згадати і розроблену за участі працівників ГУНП України в Харківській області систему RICAS (Real-time Intelligence Crime Analytics System), з використанням якої можливо розкрити окремі злочини, навіть не виходячи з кабінету (police.kh.ua).

Сенс кримінальної розвідки полягає у накопиченні розвідувальної інформації (criminal intelligence), яка відповідним чином аналізується. У результаті формуються висновки, які містять пропозиції щодо подальшого руху кримінального розслідування.

Розвідувальну інформацію прийнято поділяти на два види:

- *стратегічну* (яка стосується довготермінових цілей правоохоронних органів. Вона зазвичай відображає поточні та перспективні тенденції у злочинному середовищі, загрози громадській безпеці та порядку тощо).
- *оперативну* (забезпечує групу, яка бере участь в розслідуванні, версіями та висновками стосовно будь-яких протизаконних дій. Вона включає в себе припущення та висновки стосовно організованих злочинних угруповань, груп або окремих осіб, втягнених у злочинну діяльність, їх методів, можливостей, вразливих місць тощо, які можуть бути використані в діяльності правоохоронних органів) [31, с. 9].

Загальновідомими стратегіями кримінальної розвідки є:

- «Національна розвідувальна модель» (National Intelligence Model), застосовувана у Великобританії [32];
- «Національний план розподілу розвідувальної інформації» (National Criminal Intelligence Sharing Plan), розроблений у США [33].

Із вказаними стратегіями тісно пов'язана інша дефініція – «організація діяльності поліції на основі розвідувальних даних» або «модель поліцейської діяльності» (Intelligence-Led Policing (ILP)) [35, с. 101]. Останній термін співвідноситься із описаними стратегіями таким чином, що стратегії визначають структуру, у рамках якої ILP може бути застосована у правоохоронних органах [35, с. 435].

Кримінальна (поліцейська) розвідка містить декілька основних етапів, які об'єднано у циклічне коло. У різних стратегіях ці етапи незначно різняться між собою, проте сенс залишається приблизно однаковим:

- збирання даних;
- оцінка даних;
- обробка даних;
- аналіз даних;
- поширення інформації;
- повторна оцінка інформації [36, с. 2].

На кожному етапі використовуються різні методології аналітичної роботи. Однією з таких методологій є розроблена на початку 1970-х років ANACAPA, яка застосовується серед іншого у ФБР та Скотланд-Ярді.

Розглянемо зазначені етапи та методологію більш докладно.

Так, збирання даних передбачає їх одержання з різних джерел: відкритих, службових, секретних. При цьому говорять про різні види розвідок: з відкритих джерел (OSINT), агентурну (HUMINT), радіотехнічну (SIGINT) тощо.

Після того, як дані було належним чином зібрано відбувається їх оцінка, за допомогою якої визначається надійність набутої інформації. Найбільш часто застосовуваними системами оцінки є: 4x4, 5x5, 6x6. Система 4x4, наприклад, використовується Європолом. В інших правоохоронних органах західних країн застосовуються подібні системи. Наприклад, у Великобританії широкого поширення набула система оцінки 5x5. За потреби інформація може бути з легкістю конвертована з однієї системи в іншу.

Загальний процес оцінки можна представити дослідженням ступенів надійності джерела та актуальності інформації. Наприклад, у системі оцінки 4x4 використовуються чотири ступені оцінки джерела інформації та чотири ступені оцінки самої інформації, у системах 5x5 та 6x6 таких критеріїв відповідно п'ять та шість. В окремих випадках у бланках оцінки потрібно вносити інформацію про ступінь поширення відповідної інформації, так звані «коди обробки». Слід зауважити, що чим простішою є система оцінки, тим меншою є її суб'єктивність.

На етапі обробки даних відбувається їх структуризація (приведення до певного формату) та інтеграція (об'єднання інформації з різних джерел).

Інтегровані дані мають бути належним чином проаналізовані та інтерпретовані. Для цього серед іншого будують діаграми, які допомагають наочно побачити картину в цілому. При цьому слід пам'ятати, що діаграми не є кінцевим продуктом аналізу, а є лише додатком до висновків.

Існує достатньо багато видів таких діаграм, найбільш популярними з них є дерево зв'язків (link charting) та дерево подій (event charting).

Перед тим як побудувати означені діаграми, потрібно визначити їх фокус (об'єкт, який цікавить правоохоронні органи) та скласти матрицю асоціацій (для визначення зв'язків між об'єктами).

Назви об'єктів (фізичних осіб) у матриці розташовуються в алфавітному порядку зверху до низу. Після фізичних осіб у такому ж порядку розташовуються назви інших об'єктів, наприклад, юридичних осіб.

Після створення матриці асоціацій відбувається її заповнення відповідними кодами зв'язку (табл. 2).

*Таблиця 3. Коди зв'язку*

| | |
|---|---|
| ● | Підтверджено зв'язок між об'єктами |
| ○ | Можливий зв'язок між об'єктами |
| + | Підтверджене членство в юридичній особі |
| – | Можливе членство в юридичній особі |
| → | Підтверджені права володіння без активної участі в роботі юридичної особи |
| ▶ | Можливі права володіння без активної участі в роботі юридичної особи |

Після заповнення матриці підраховується кількість відповідних зв'язків. Для кожного об'єкта враховується сума зв'язків по вертикалі та по горизонталі (рис. 3).

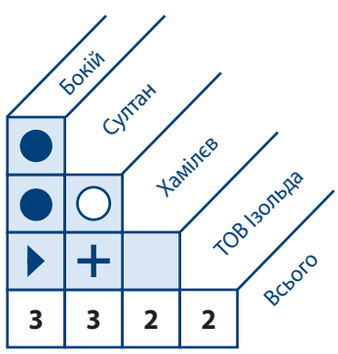



*Рис. 3. Заповнена матриця асоціацій*

З використанням заповненої матриці асоціацій здійснюється побудова попередньої діаграми. При цьому фізичні особи відображаються у вигляді кіл, юридичні – прямокутниками, підтверджені зв'язки – суцільною лінією (рис. 4 а)), можливі – пунктиром (рис. 4 б)). Членство у юридичній особі позначається розміщенням відповідного кола у середині прямокутника (рис. 4 в)). Підтверджені або можливі права володіння відповідно позначаються суцільною та пунктирною лініями (рис. 4 г)).


*Рис. 4. Графічне відображення асоціацій*

Побудована попередня діаграма відображена на рис. 5.

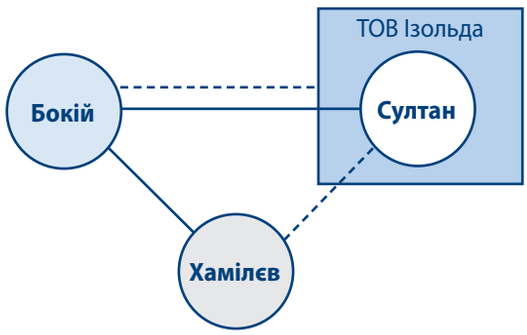



*Рис. 5. Попередня діаграма*

Якщо у попередній діаграмі присутні лінії, що перетинаються, або недостатньо проглядається фокус діаграми тощо, то вона переробляється з урахуванням виявлених недоліків, аби бути більш доступною для сприйняття. Розміщення блоків при цьому здійснюється на власний розсуд аналітика. У результаті одержується кінцева діаграма зв'язків.

Для відображення хронології подій по аналогії з деревом зв'язків можна побудувати дерево подій (рис. 6).

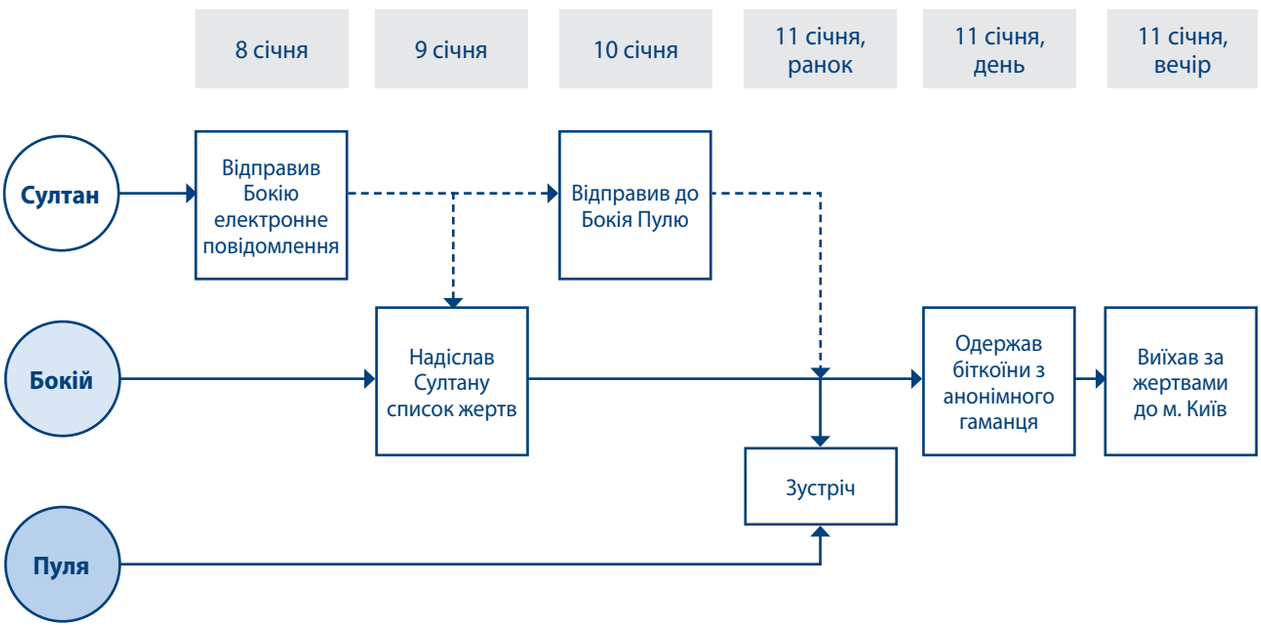



*Рис. 6. Дерево подій матричного типу*

Для створення таких діаграм дуже корисно використовувати спеціалізоване програмне забезпечення. У якості прикладів в даному контексті можна назвати Datasploit, i2, Maltego, Splunk.

Система Datasploit (https://github.com/upgoingstar/datasploit) буде корисною для збирання та аналізу інформації про домен, електронну пошту тощо, Splunk (https://www.splunk.com) – для збирання та аналізу машинних даних, наприклад, лог-файлів.

Програма Maltego у безкоштовному виконанні (https://www.paterva.com/) цілком може бути застосована для роботи з невеликим обсягом даних, у той час як i2 (www.ibm.com/software/products/ru/analysts-notebook) орієнтована на роботу з так званими «big data» (рис. 7).

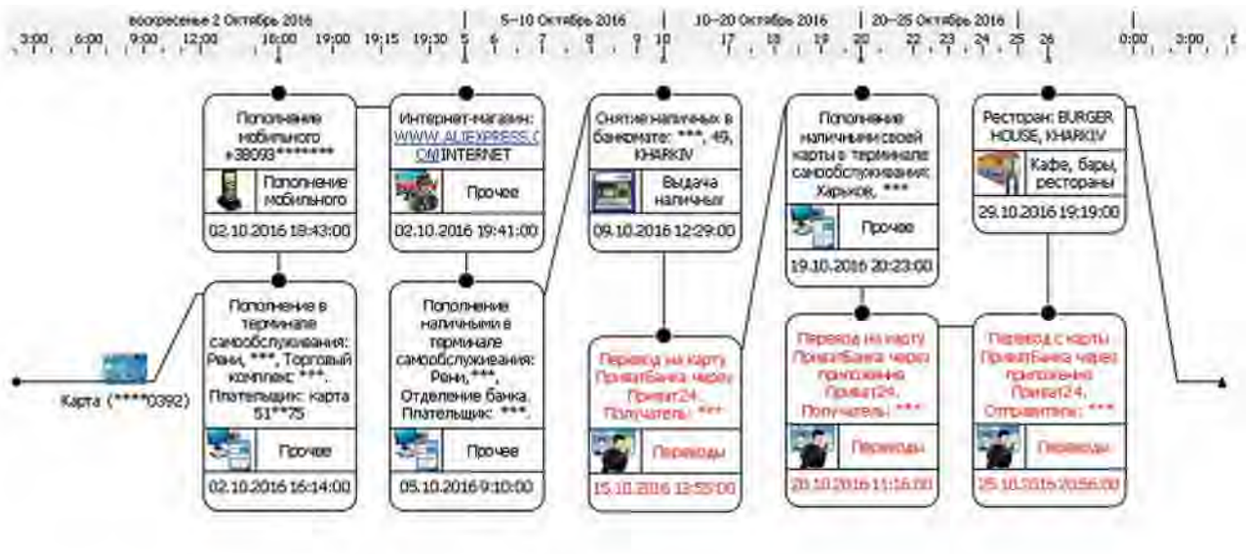



*Рис. 7. Часова діаграма руху коштів*

Слід наголосити, що від виду вихідних даних може залежати методика побудови та вигляд відповідної діаграми. Наприклад, це можна спостерігати на прикладі аналізу телефонних з'єднань.

Для побудови відповідної діаграми телефонних з'єднань за наявними даними використовується заповнена трикутна матриця, яка виглядає, як на рис. 8.

Під час побудови матриці номери телефонів потрібно розміщувати у порядку зростання, щоб було легко відшукати потрібний номер у матриці. Усі наявні номери вносяться у заголовки матриці таким чином, щоб номери, які розміщені у n-му стовпчику та n-му рядку заголовку матриці були однаковими, а на перетині ставляться відповідні позначки, які вказують на кількість з'єднань. Підсумкова кількість з'єднань, відображатиметься на діаграмі.


*Рис. 8. Матриця з'єднань*

Для побудови відповідної діаграми можна використати кола, лінії зі стрілками, які вказуватимуть напрям з'єднання, та позначку, що відображатиме кількість таких з'єднань (рис. 9).

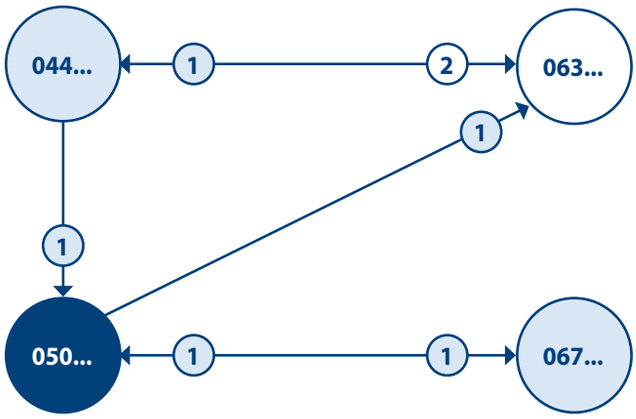



*Рис. 9. Діаграма телефонних з'єднань*

Варто відзначити, що окрім телефонних номерів у вузлах графу може бути розташовано логічні адреси відповідних терміналів, наприклад, комп'ютерів тощо.

Велику допомогу у побудові графів з'єднань надає спеціалізоване програмне забезпечення. У цьому сенсі варто згадати програму «Мобильный криминалист: Детектив», у якій присутня функція побудови графу зв'язків як в середині одного пристрою (рис. 10), так і об'єднаного у рамках однієї справи графу контактів декількох пристроїв (рис. 11).

*Рис. 10. Графічний аналіз контактів одного пристрою*

Більшими колами позначено контакти, з якими найчастіше відбувався зв'язок з використанням досліджуваних мобільних пристроїв.

Після побудови діаграм за визначеними методами внаслідок інтерпретації даних формується аналітичний продукт – висновки, яких виділяють чотири види: гіпотеза, прогноз, розрахунок, умовивід.

Висновки мають містити інформацію про: ключову особу чи осіб (WHO?); кримінальне діяння (WHAT?); методику дій (HOW?); місцезнаходження (WHERE?); мотив (WHY?); період часу (WHEN?). Дана система запитань одержала назву 5W+H.

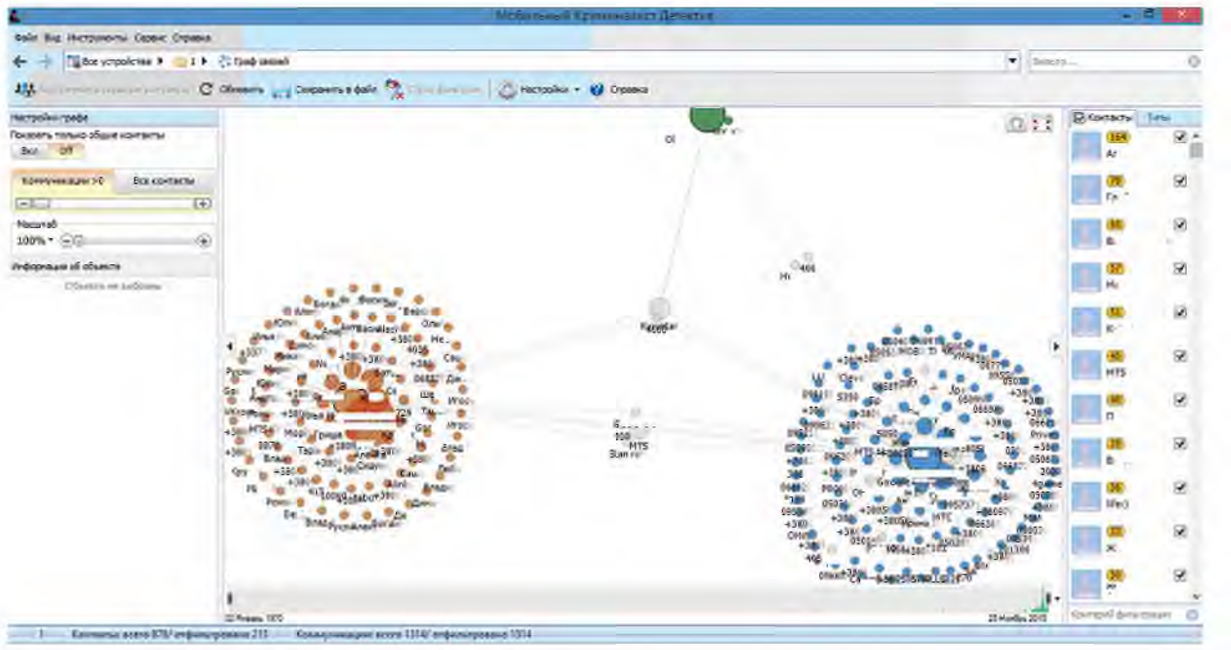


*Рис. 11. Графічний аналіз контактів декількох пристроїв*

У різних моделях поліцейської розвідки форми висновків можуть різнитися. Наприклад, у Британській моделі кінцевий продукт аналізу може подаватися у вигляді:

- стратегічного аналізу, за допомогою якого виробляються довготермінові плани діяльності правоохоронних органів, розробляється стратегія та вимоги до кримінальної розвідки;
- тактичного аналізу, на підставі якого здійснюється розробка короткотермінових планів діяльності поліції згідно із загальною стратегією, а також може використовуватися для доповнення існуючих вимог до кримінальної розвідки;
- цільового профілю стосовно конкретної особи (підозрюваного чи жертви) або групи осіб у відповідності до стратегічних пріоритетів;
- проблемного профілю, в якому проаналізовано конкретний злочин або серію подій тощо [31, с. 67].

ПРИКЛАД ВИСНОВКУ: СУЛТАН (WHO?) Є ГОЛОВОЮ ЗЛОЧИННОГО УГРУПОВАННЯ, ПРИЧЕТНОГО ДО ТОРГІВЛІ ЛЮДЬМИ (WHAT?). ВІН ЗДІЙСНЮЄ СВОЮ ДІЯЛЬНІСТЬ ЧЕРЕЗ ПОМІЧНИКІВ, ВЕРБУЮЧИ ЖЕРТВ ЧЕРЕЗ ІНТЕРНЕТ ІЗ ПОДАЛЬШИМ ЇХ ПЕРЕПРАВЛЕННЯМ ЗА КОРДОН (HOW?) З МЕТОЮ ОДЕРЖАННЯ ВИГОДИ (WHY?). ГРУПА ПРОМИШЛЯЄ У ЦЕНТРАЛЬНИХ РЕГІОНАХ УКРАЇНИ (WHERE?) ОСТАННІ 7 РОКІВ (WHEN?).

Висновки підлягають *поширенню* у формі звітів, презентацій, тижневих оглядів, цільових інструктажів тощо.

Після завершення циклічного кола кримінальної розвідки відбувається повторна оцінка, яка спрямовується на удосконалення аналітичного продукту.

Кримінальна розвідка – це колективний процес, а тому одній людині практично нереально домогтися успіху в розслідуванні більш-менш серйозного злочину у прийнятні строки. Для цього повинен працювати злагоджений колектив. Удосконалення знань, наполеглива праця та постійне навчання колективу дозволять значно покращити його оперативно-службову діяльність, зокрема у сфері протидії злочинам, пов'язаним з торгівлею людьми [37].

## 4. ЗАГАЛЬНИЙ ПОРЯДОК ПОШУКУ ІНФОРМАЦІЇ ПРАВООХОРОННИМИ ОРГАНАМИ ПРО ОБ'ЄКТИ В МЕРЕЖІ

У рамках протидії торгівлі людьми правоохоронним органам часто доводиться здійснювати первинний пошук інформації про певні об'єкти в мережі. Такий пошук можна умовно розділити на два види:

- пошук інформації про осіб;
- пошук інформації про інші об'єкти.

Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за мережними ідентифікаторами, тобто за тими обліковими даними, які особа залишила по собі в мережі. Як правило, такими ідентифікаторами виступають адреса електронної поштової скриньки, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема часто обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного штибу розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P) [38, с. 256], які будуть розглянуті далі.

ЗБИРАННЯ ІНФОРМАЦІЇ, ДОСТУПНОЇ ЧЕРЕЗ ВІДКРИТІ ДЖЕРЕЛА, МОЖЕ КЛАСИФІКУВАТИСЯ ЯК ПОСЯГАННЯ НА НЕДОТОРКАННІСТЬ ПРИВАТНОГО ЖИТТЯ. ЗОКРЕМА, ЄВРОПЕЙСЬКИМ СУДОМ З ПРАВ ЛЮДИНИ, У СПРАВІ ШВЕЦІЯ ПРОТИ СЕГЕРСТЕД ВІБЕРГ (SEGERSTEDT-WIBERG V. SWEDEN [39]) ДІЇ ПОЛІЦІЇ ЗІ ЗБИРАННЯ ІНФОРМАЦІЇ, ЯКА Є ВІДКРИТО ДОСТУПНОЮ ДЛЯ КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ, КВАЛІФІКОВАНО ЯК ПОРУШЕННЯ ПРАВА НА НЕДОТОРКАННІСТЬ ПРИВАТНОГО ЖИТТЯ, ГАРАНТОВАНЕ СТАТТЕЮ 8 КОНВЕНЦІЇ РАДИ ЄВРОПИ «ПРО ЗАХИСТ ПРАВ ЛЮДИНИ І ОСНОВОПОЛОЖНИХ СВОБОД» ВІД 04.11.1950 (РАТИФІКОВАНО ВЕРХОВНОЮ РАДОЮ УКРАЇНИ 17.07.1997). СИСТЕМАТИЧНЕ ЗБИРАННЯ ІНФОРМАЦІЇ РОЗЦІНЮЄТЬСЯ ЯК ВТРУЧАННЯ У ПРИВАТНЕ ЖИТТЯ У ЗВ'ЯЗКУ З ТИМ, ЩО ОСОБА, ЯКА РОЗМІЩУЄ ІНФОРМАЦІЮ, РОЗРАХОВУЄ НА ЗБЕРІГАННЯ ВІДОМОСТЕЙ ТА ВІДСУТНІСТЬ МОНІТОРИНГУ ЗА ЙОГО ПРОФІЛЕМ. ЗБИРАННЯ ВІДОМОСТЕЙ Є ДОПУСТИМИМ ТІЛЬКИ ЗГІДНО З ЗАКОНОМ ТА В ЦІЛЯХ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ (СТ. 8 (2) КОНВЕНЦІЇ) [40, С. 131].

Нерідко місцезнаходження терміналу та самої особи не співпадають. Враховуючи наведене, можна окреслити декілька напрямів щодо визначення місцезнаходження як терміналу, так і самої особи за її мережними ідентифікаторами.

По-перше, це встановлення особи за допомогою офіційного запиту до власника ресурсу або провайдера (оператора) телекомунікацій.

У зв'язку з тим, що значна кількість розподілених ресурсів розташована за межами національної юрисдикції, такий спосіб часто не дає бажаного результату (складний процес, зволікання або взагалі відсутність відповіді).

Другим способом встановлення особи може виступати пошук інформації за певним ідентифікатором за допомогою різних сервісів та ресурсів. Для цього, перш за все, необхідно скористатися можливостями Інтегрованої інформаційно-пошукової системи органів внутрішніх справ. У рамках використання даного способу також можуть бути застосовані пошукові системи Google, Yahoo, Meta тощо.

В процесі пошуку засобами пошукових систем корисним буде знання спеціалізованих операторів, з якими можна ознайомитись на офіційних сайтах інформаційно-пошукових систем. Зазвичай, базові оператори є однаковими в усіх цих системах. Наприклад, фраза в лапках, введена у пошуковому вікні багатьох пошукових систем, означатиме пошук фрази цілком.

Якщо потрібно дізнатися, де зустрічається логін до електронної пошти, в Google можна скористатися запитом: intext:"login@*ru|ua|com|net", у результаті виконання якого буде знайдено сторінки, у змісті яких зустрічається текст, який починається символами login@ та закінчується символами ru, ua, com або net.

У випадку, коли правоохоронець не повною мірою володіє мовою спеціальних запитів в інформаційно-пошукових системах, йому буде корисною функція розширеного пошуку:

Google: Налаштування > Розширений пошук.

Після пошуку з використанням відкритих та відомчих інформаційно-пошукових систем необхідно проаналізувати інформацію про шуканий об'єкт в соціальних мережах, на форумах, поштових серверах тощо.

Серед *корисних ресурсів* для пошуку слід виділити:

- findface.ru для встановлення особи за фотографією;
- агрегатор інформації з соціальних мереж www.radaris.com;
- набір інструментів для збирання інформації з відкритих джерел osintframework.com;
- агрегатор інформації про юридичних осіб youcontrol.com.ua;
- сервіс пошуку розташування точок доступу Wi-Fi за MAC-адресою або назвою (для пошуку потрібно зареєструватись) wigle.net.

Окрім наведеного велику *бібліотеку пошукових ресурсів* можна завантажити за посиланням http://osint.academy/2016/10/20/biblioteka-otkrytyh-istochnikov/.

Для аналізу зібраних даних може бути використано програми Maltego та i2. Існує також низка сервісів, які спеціалізуються на аналізі даних з соціальних мереж:

- stalkscan.com (Facebook);
- yasiv.com/vk, vk.city4me.com (Вконтакте).

Указом президента України від 15.05.2017 №133/2017 Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» Інтернет-провайдерам заборонено надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru» (www.mail.ru) та соціально-орієнтованих ресурсів «Вконтакте» (www.vk.com) та «Одноклассники» (www.ok.ru). Однак, робота з вказаними мережами повністю не заблокована, через їх використання «в обхід» встановлених заборон за допомогою VPN (virtual private network) або браузера Tor, чим можуть скористуватись злочинці, а тому і правоохоронці повинні мати навички роботи з вказаними ресурсами.

У разі, якщо отриманих відомостей не вистачає, необхідно скористатися іншими інформаційними ресурсами (наприклад, nomer.org, lookup.com), зокрема, приватними базами, які надають інформацію для маркетингових досліджень. Якщо у наявності є електронне поштове відправлення шуканої особи, слід ретельно проаналізувати його заголовок та вибудувати маршрут руху листа для планування подальших дій.

Не зайвим буде **звернення до служб безпеки найбільших банків** України, для отримання оперативної інформації щодо їх можливих клієнтів.

ПОТРІБНО ВІДМІТИТИ, ЩО ВЕЛИКА КІЛЬКІСТЬ МЕРЕЖНИХ РЕСУРСІВ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ, НЕ ІНДЕКСУЮТЬСЯ ПОШУКОВИМИ СИСТЕМАМИ. ВІДТАК ЇХ ДОСТАТНЬО СКЛАДНО ВИЯВИТИ БЕЗ ЗАСТОСУВАННЯ АРСЕНАЛУ ТРАДИЦІЙНИХ ОПЕРАТИВНО-РОЗШУКОВИХ СИЛ І ЗАСОБІВ. ДЛЯ ПОШУКУ ТАКИХ РЕСУРСІВ У РОЗВИНЕНИХ КРАЇНАХ ВИКОРИСТОВУЄТЬСЯ СПЕЦІАЛЬНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ [41].

Одним із способів встановлення особи за мережним ідентифікатором є використання систем відновлення паролів різних ресурсів. Зокрема, таким чином можна визначити номери телефонів [42], віднайти профіль особи у соціальних мережах тощо. У подальшому, аналізуючи зміст та геопозначки відповідних фотографій, можна встановити місця перебування особи у певний проміжок часу. Знаючи місця пересування особи, можна у 95% випадків однозначно її ототожнити, що на практиці було доведено дослідниками з Масачусетського технологічного інституту і Католицького університету в Левені [43].

У рамках пошуку в мережі можуть бути застосовані й інші інструменти. Наприклад в системі Windows вбудовані утиліти дозволяють одержати:

- інформацію про комп'ютер, за яким працює користувач (утиліта ipconfig);
- дані про робочу станцію, з використанням її імені (утиліта nbtstat);
- відомості про наявні мережі Microsoft (утиліта net);
- статистику протоколів і поточних мережних підключень TCP/IP (утиліта netstat);
- інформацію про стан каналів зв'язку (утиліта ping);
- інформацію про маршрут руху пакетів (утиліта tracert);
- інформацію про доменні імена та IP-адреси з Інтернет-реєстратур (утиліта nslookup).

Пошук інформації про інші об'єкти в мережі здійснюється по аналогії із вищевикладеним алгоритмом. Разом з тим варто зауважити, що торговці людьми у своїй діяльності застосовують специфічну термінологію, як от PTHC (pre-teen hard core) (рис. 2), PTSC, xxxx from 12 yo, hard candy, LS тощо. Тому правоохоронцю для успішного пошуку відповідної інформації слід розумітися у цих специфічних термінах та вводити їх у пошукові запити.

Крім зазначених способів встановити особу та ототожнити її, здійснювати пошук інших об'єктів можливо також оперативним шляхом через здійснення низки заходів.

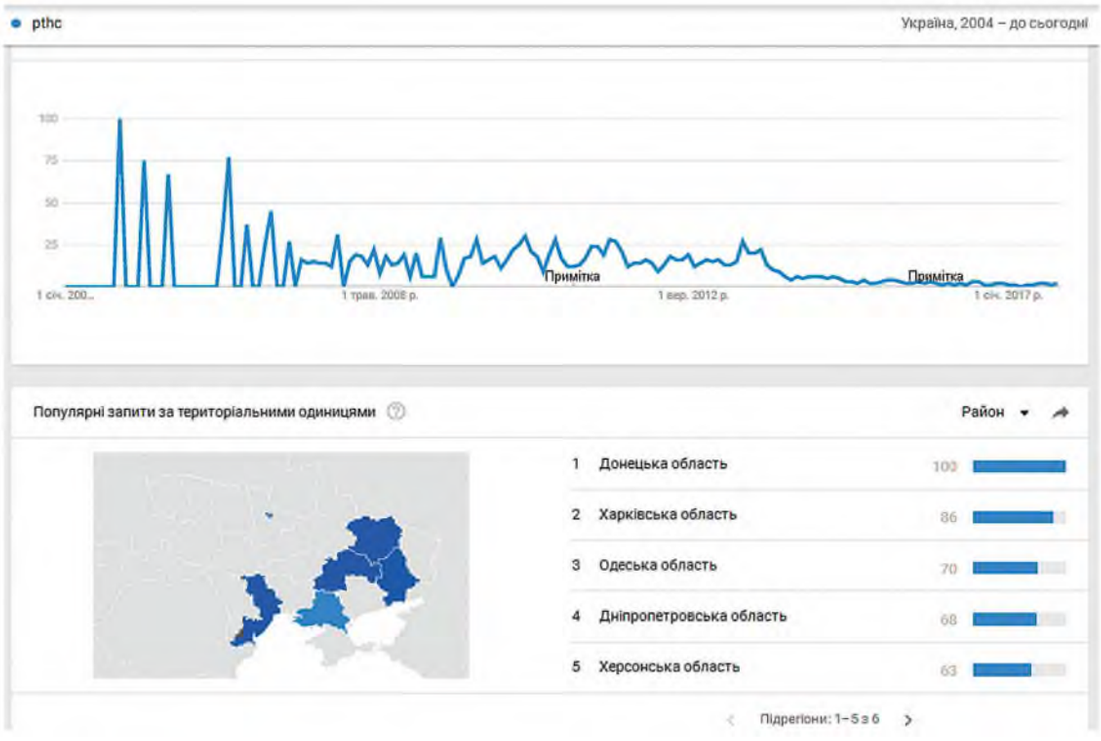



*Рис. 12. Географічна статистика Google щодо частоти пошукових запитів терміну PTHC в Україні (https://trends.google.com/trends/explore?date=all&geo=UA&q=pthc&hl=uk)*

Варто відмітити, що наведені способи не є вичерпними. Багато в чому конкретна методика пошуку залежить від наявної ситуації, тому правоохоронцю для ефективної реалізації описаного у даній роботі завдання слід бути не лише юридично, але й технічно обізнаним працівником та постійно підвищувати свій професійний рівень, відслідковуючи новітні методики та розробки, які зможуть допомогти у вирішенні завдань боротьби зі злочинністю. Також, слід пам'ятати, що правоохоронні органи завжди повинні дотримуватись балансу між попередженням та припиненням злочинів, з одного боку, і інтересами особи та його / її правом на приватність, з іншого боку. Згідно з основними принципами, зазначеними в Рекомендації Ради Європи № R (87) 15 щодо використання приватних даних поліцією, збирання приватних даних повинно відбуватись тільки з метою попередження реальної небезпеки чи припинення злочину, а використання і передача таких даних повинна обмежуватись лише правоохоронними цілями.

**ЗАВДАННЯ**

**ЗДІЙСНИТИ ПОШУК ДАНИХ БУДЬ-ЯКОЇ ВІДОМОЇ ОСОБИ ЗА ЇЇ ЕЛЕКТРОННОЮ ПОШТОЮ ТА МЕРЕЖНИМ ПСЕВДОНІМОМ АБО ІНШИМИ ПЕРВИННИМИ ДАНИМИ. СИСТЕМАТИЗУВАТИ ЗНАЙДЕНІ ВІДОМОСТІ**

## МОДУЛЬ 2

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ ВЕРБУВАННЯ ЖЕРТВ

### 1. СПЕЦІАЛЬНО СТВОРЕНІ ВЕБ-САЙТИ

Як зазначено у дослідженні «Торгівля людьми: вербування через Інтернет», зробленому під егідою Ради Європи, використання інформаційних технологій для вербування жертв не є новою формою торгівлі людьми, а є лише новим інструментом, який мають на озброєнні злочинці [44, с. 21]. Як і раніше головними формами експлуатації при цьому залишаються сексуальна, трудова та торгівля органами.

ЗГІДНО ЗІ ЗВІТОМ ООН 2016 РОКУ ЩОДО СТАНУ ТОРГІВЛІ ЛЮДЬМИ У СВІТІ В 2014 РОЦІ ЗАГАЛОМ БУЛО ВИЯВЛЕНО 14333 ЖЕРТВ ТАКОЇ ДІЯЛЬНОСТІ, З ЯКИХ 7635 ПОСТРАЖДАЛИ ВІД СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ, 5537 – ТРУДОВОЇ, 51 ОСОБА СТАЛА ЖЕРТВОЮ ТОРГІВЛІ ОРГАНАМИ, 1110 ОСІБ ПОСТРАЖДАЛИ В ІНШИХ СФЕРАХ. ВОДНОЧАС У ТОМУ Ж 2014 РОЦІ У РОЗСЛІДУВАННЯХ ФІГУРУВАЛО 15580 ОСІБ, ПРИЧЕТНИХ ДО ТОРГІВЛІ ЛЮДЬМИ. ТАКЕ КІЛЬКІСНЕ СПІВВІДНОШЕННЯ НЕ НА КОРИСТЬ ЖЕРТВ ТОРГІВЛІ ЛЮДЬМИ МОЖЕ СВІДЧИТИ ПРО ВИСОКУ ЛАТЕНТНІСТЬ ВКАЗАНИХ ЗЛОЧИНІВ [45].

Оголошення, розміщені в Інтернеті, через які вербуються потенційні жертви торгівлі людьми, надають доступ до цілої низки зацікавлених осіб.

Правопорушниками створюються активні веб-сайти пошуку моделей та фотомоделей або шлюбні агенції, які виступають платформою для вербування потенційних жертв торгівлі людьми.

Менеджери таких веб-сайтів можуть надавати можливість встановлення контактів з клієнтами, а також подорожування, водночас бути причетними до оборудок з сексуальною експлуатацією під вивіскою ескорт-служби або до поширення порнографічних матеріалів.

Також, зловмисники, відповідальні за вербування жертв, розміщують і додають відгуки, які підтверджують привабливість пропозиції, на різних чатах і в коментарях. Таким чином, молодь – потенційні жертви торгівлі людьми – наражаються на більший ризик, оскільки вони є активними Інтернет-користувачами. Часто торговці знаходять своїх жертв, не виходячи з дому.

Відповідні веб-сайти можуть бути виконані у різних формах, зокрема у вигляді шлюбних агенцій або сайтів знайомств. Онлайнові шлюбні агенції також можуть відігравати значну роль як посередники в оборудках торгівлі жінками. Не випадково чимало таких агенцій працює у країнах, звідки походить велика кількість жертв торгівлі людьми.

Щоб зареєструватися на веб-сайті, жінкам часто доводиться сплачувати реєстраційний внесок, який може бути різним, але іноді доходить до кількох сотень євро. Для більшості жінок, враховуючи їхній заробіток у тій чи іншій країні, це значна сума грошей. Якщо жінка не має звідки сплатити вступний внесок, це може породити так званий механізм боргу або кабали. Менеджери таких веб-сайтів можуть надавати можливість встановлення контактів з клієнтами, а також подорожування, але також можуть бути причетними до оборудок з сексуальною експлуатацією під вивіскою ескорт-служби або до поширення порнографічних матеріалів.

За даними Європолу, особи, причетні до роботи ескорт-служб та різних агенцій знайомств, особисто і фінансово пов'язані з тими, хто займається торгівлею людьми та порнографічними сайтами. Тому слід розрізняти між веб-сайтами, які пропонують можливість купити наречену (рабиню) (рис. 13), та агенціями знайомств, які функціонують як веб-сайти, де розміщується незаконний контент (рис. 14).


*Рис. 13. Стартова сторінка сайту з продажу рабинь*


*Рис. 14. Стартова сторінка сайту агентства знайомств*

Також спеціальні сайти, задіяні у вербуванні жертв торгівлі людьми, можуть мати наповнення у вигляді пропозицій з працевлаштування. Агентства зайнятості часто є першою ланкою у ланцюжку торгівлі людьми з метою трудової експлуатації. Зараз існує чимало інтернет-сайтів, через які можна шукати роботу. Оголошення можуть подавати шукачі роботи, які потім чекають на пропозицію, або пропозиції можуть розміщуватися в оголошеннях, а зацікавлені особи можуть звернутися до компанії або особи, які опублікували оголошення.

В МЕРЕЖІ ІНТЕРНЕТ ІСНУЮТЬ ТАК ЗВАНІ ГІБРИДНІ («MASHUP») ВЕБ-САЙТИ, ЯКІ ОБ'ЄДНУЮТЬ ДАНІ З ДЕКІЛЬКОХ ІНШИХ ДЖЕРЕЛ. В КОНТЕКСТІ ТОРГІВЛІ ЛЮДЬМИ, ЯК ПРИКЛАД ГІБРИДНОГО ВЕБ-ЗАСТОСУВАННЯ, МОЖНА УЯВИТИ ВЕБ-СЕРВІС, ЩО ЗБЕРІГАЄ ДАНІ КОРИСТУВАЧА НА DROPBOX, ВИКОРИСТОВУЄ АВТЕНТИФІКАЦІЮ ЧЕРЕЗ FACEBOOK, ПРОВОДИТЬ ПЛАТЕЖІ ЧЕРЕЗ PAYPAL І РОЗСИЛАЄ КОРИСТУВАЧАМ РЕЛЕВАНТНУ ІНФОРМАЦІЮ ЧЕРЕЗ TWITTER. ЦЕ І Є «ГІБРИД», ТОБТО ОБ'ЄДНАННЯ РІЗНИХ СЕРВІСІВ АБО ВЕБ-САЙТІВ. В ЦЬОМУ ВИПАДКУ ЕЛЕКТРОННІ ДОКАЗИ ТЕЖ ЗНАХОДЯТЬСЯ НА РІЗНИХ СЕРВІСАХ І У РІЗНИХ ПРОВАЙДЕРІВ. ГІБРИДНИЙ ХАРАКТЕР ОНЛАЙН-СЕРВІСУ ДОПОМАГАЄ ВСТАНОВИТИ РІЗНІ ДЖЕРЕЛА ДОКАЗІВ ДЛЯ ПІДТВЕРДЖЕННЯ ОДНОГО ФАКТУ, ЩО МАЄ ЗНАЧЕННЯ ДЛЯ РОЗСЛІДУВАННЯ.

Сьогодні злочинні групи під виглядом законослухняних компаній підписують контракти, переважно для роботи у Західній Європі, гарантуючи виплату заробітної плати після виконання певної роботи, наприклад, демонтажу будівлі. У таких випадках злочинні групи шукають працівників, яких можна використати як дешеву робочу силу, занижуючи їхню зарплатню, не забезпечуючи мінімальних умов праці, проживання і соціального забезпечення та дотримання правил організації трудового розпорядку тощо. У таких випадках інформаційні технології переважно використовуються для вербування жертв, як правило чоловіків, з Центральної та Східної Європи.

ЗА ДАНИМИ МІЖНАРОДНОЇ ОРГАНІЗАЦІЇ З МІГРАЦІЇ В УКРАЇНІ НЕВПИННО ЗБІЛЬШУЄТЬСЯ КІЛЬКІСТЬ ЧОЛОВІКІВ, ЯКІ ПОСТРАЖДАЛИ ВІД ТОРГІВЛІ ЛЮДЬМИ. ТАК, ЯКЩО У 2014 РОЦІ ЇХ ДОЛЯ У ЗАГАЛЬНІЙ КІЛЬКОСТІ ЖЕРТВ ТОРГІВЛІ ЛЮДЬМИ СКЛАДАЛА 14 %, ТО ВЖЕ У ЧЕРВНІ 2017 РОКУ ЦЯ ДОЛЯ СЯГНУЛА 62 %. АНАЛІЗ КІЛЬКОСТІ ПОСТРАЖДАЛИХ ЧОЛОВІКІВ ЗА ПЕРІОД 2004-2017 РР. ДЕМОНСТРУЄ ТЕНДЕНЦІЮ ДО ПОСТІЙНОГО ЗРОСТАННЯ ДОЛІ ЧОЛОВІКІВ СЕРЕД ЖЕРТВ ТОРГІВЛІ ЛЮДЬМИ [46].

В КІНЦІ ЖОВТНЯ 2016 ПРАЦІВНИКАМИ УПРАВЛІНЬ ПО БОРОТЬБІ ЗІ ЗЛОЧИНАМИ, ПОВ'ЯЗАНИМИ З ТОРГІВЛЕЮ ЛЮДЬМИ, ГОЛОВНИХ УПРАВЛІНЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ І М. КИЄВА ВСТАНОВЛЕНА ГРУПА ОСІБ, ЯКА В ПЕРІОД З 2014 ДО 2016 РОКІВ НА ТЕРИТОРІЇ ДНІПРОПЕТРОВСЬКОЇ, КИЇВСЬКОЇ ТА ІНШИХ ОБЛАСТЕЙ УКРАЇНИ ЗДІЙСНЮВАЛИ ВЕРБУВАННЯ ПОТЕРПІЛИХ З МЕТОЮ ЕКСПЛУАТАЦІЇ, А САМЕ ЗАЛУЧЕННЯ ДО ЗЛОЧИННОЇ

ДІЯЛЬНОСТІ НА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ. СВОЮ ЗЛОЧИННУ ДІЯЛЬНІСТЬ ЗДІЙСНЮВАЛИ ЧЕРЕЗ ВСЕСВІТНЮ МЕРЕЖУ ІНТЕРНЕТ, А ТАКОЖ ЗА ДОПОМОГОЮ РЕКЛАМНИХ ЛИСТІВОК, ЯКІ РОЗМІЩУВАЛИСЯ В ГРОМАДСЬКИХ МІСЦЯХ, ЗАПРОШУВАЛИСЯ ОСОБИ У ВІЦІ ВІД 20 РОКІВ, ДЛЯ РОБОТИ КУР'ЄРАМИ ЕКСПЕДИТОРІВ ФАСОВАНОГО ТОВАРУ, З ВІДРЯДЖЕННЯМ ЗА КОРДОН. НАДАЛІ, ПІСЛЯ ПРИБУТТЯ ЗАВЕРБОВАНИХ ОСІБ В РОСІЙСЬКІЙ ФЕДЕРАЦІЇ, ЗАЛУЧАЛИ ДО НЕЗАКОННОГО ЗБУТУ НАРКОТИКІВ, В ТОМУ ЧИСЛІ ІЗ ЗАСТОСУВАННЯМ ПОГРОЗ. НЕЗАЛЕЖНО ВІД ТОГО, ПОГОДЖУВАЛИСЯ ДАНІ ОСОБИ БРАТИ УЧАСТЬ У ЗЛОЧИННІЙ ДІЯЛЬНОСТІ, В ПОДАЛЬШОМУ ЇХ ЗАТРИМУВАЛИ ПРАВООХОРОННІ ОРГАНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ І ПІД ПРИВОДОМ ЗАЛУЧЕННЯ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ УТРИМУВАЛИ ПІД ВАРТОЮ.

ЗА ДАНИМ ФАКТОМ ПОРУШЕНО 5 КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ПО 11 ЕПІЗОДАХ, ЗА ОЗНАКАМИ КРИМІНАЛЬНИХ ЗЛОЧИНІВ, ПЕРЕДБАЧЕНИХ Ч. 2 СТ. 149 КК УКРАЇНИ. ЧОТИРИ ОСНОВНІ ОРГАНІЗАТОРИ ЗАЗНАЧЕНОГО УГРУПОВАННЯ ЗАТРИМАНІ І ЗАРАЗ ПЕРЕБУВАЮТЬ ПІД ВАРТОЮ. ПРИБЛИЗНА КІЛЬКІСТЬ ОСІБ, ЯКІ ЙМОВІРНО Є ПОСТРАЖДАЛИМИ ВІД ТАКОЇ ДІЯЛЬНОСТІ (ТОРГІВЛІ ЛЮДЬМИ) ДОСЯГАЄ 50-ТИ ЧОЛОВІК, АЛЕ І ЦЕ НЕ ОСТАТОЧНІ ДАНІ, ОСКІЛЬКИ ЗВЕРНЕННЯ ЩЕ НАДХОДЯТЬ З РІЗНИХ РЕГІОНІВ УКРАЇНИ ВІД РОДИЧІВ І БЛИЗЬКИХ ЦИХ ОСІБ.

В Інтернеті також можна зустріти немало сайтів ескорт-агентств. Ескорт-агентства – це компанії, які надають ескорт-партнерів клієнтам, переважно для сексуальних послуг. Ескорт-агентства часто вербують людей для роботи ескорт-партнерами, публікуючи оголошення в Інтернеті, журналі або газеті.

Слід зазначити, що діяльність веб-сайтів з пошуку моделей, сайтів ескорт-агентств та сайтів з пропозицією працевлаштування свідчать про наявність ознак складу злочинів, передбачених ст. 149 «Торгівля людьми або інша незаконна угода щодо людини», 303 «Сутенерство або втягнення особи в заняття проституцією» КК України, а тому при розслідуванні вказаних злочинів та складанні протоколів огляду сайтів на яких розміщуються відповідні пропозиції слід зазначити, які ознаки вказують на протиправну діяльність злочинців (інтимні фотографії, ціна за надання сексуальних послуг, оголошення про найм жінок або чоловіків для зайняття проституцією, контактні відомості).

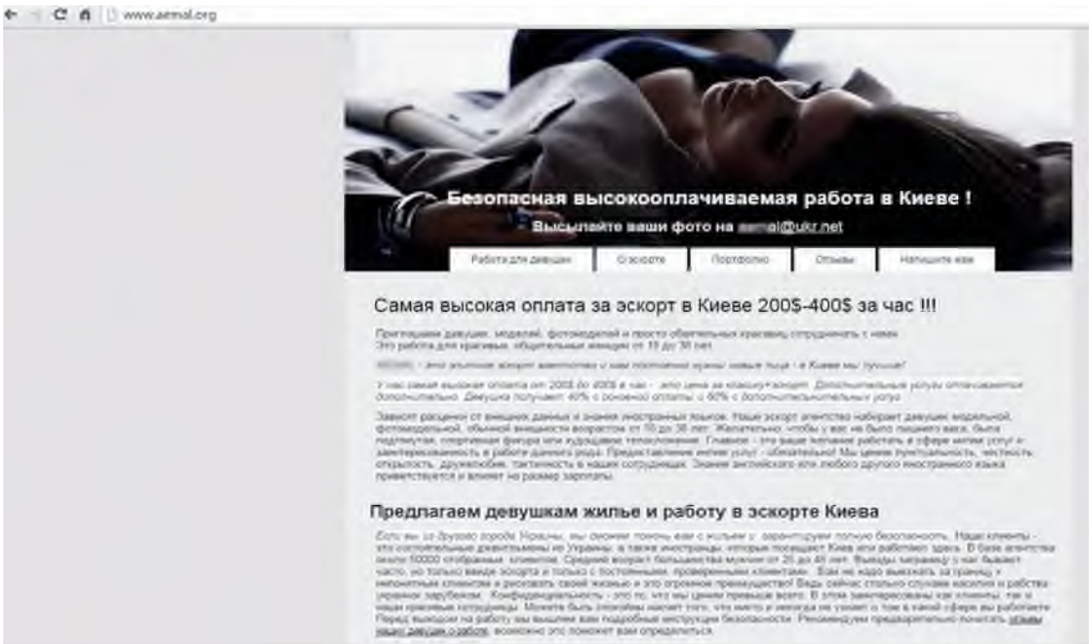



*Рис. 15. Стартова сторінка сайту ескорт-агентства*

Адже, для доведення систематичності, наприклад, торгівлі людьми або здійснення інших незаконних угод, об'єктом яких є людина, необхідним буде пов'язати діяльність відповідних сайтів у мережі Інтернет з:

- конкретною особою, яка замовила виготовлення такого сайту;
- оплатила послуги його адміністрування;
- наповнила відповідним контентом, а саме фотографіями, номерами мобільних телефонів;
- неодноразово відвідувала сайт.

Наведемо приклад ідентифікації таких агентств (рис. 15) правоохоронними органами.

Ідентифікацію та збір інформації слід розпочинати зі встановлення даних реєстратора доменного імені та хостингу. Інформацію про їх належність можна зібрати за допомогою **сервісів Whois** (http://centralops.net, https://whoer.net). В українському сегменті рекомендується також використовувати ресурс hostmaster.ua. У випадку використання зловмисником CloudFlare з метою деанонімізації варто спробувати застосувати ресурс http://www.crimeflare.com/cgi-bin/cflist2/3346, сервіс Reverse SSL.

Знання принципів розподілу IP-адрес і реєстрації DNS-імен дає можливість правильно запросити офіційними каналами контактну інформацію у DNS-реєстратора, перетворити доменне ім'я в IP-адресу і встановити власника IP-адреси в конкретний період часу. Для перетворення доменних імен в IP-адреси існує також велика кількість програмних інструментів і веб-сайтів, наприклад, DnsStuff (www.dnsstuff.com), DomainTools (www.domaintools.com) та інші, але потрібно мати на увазі, що найкращий спосіб отримати дані – це звернутися до вихідного реєстратора.

У даному прикладі, за допомогою сервісу «1whois.ru» (рис. 16) встановлюємо, хто надає послуги хостингу для сайту http://www.***al.org та на кого зареєстровано вказане доменне ім'я.


*Рис. 16. Відповідь Whois-сервісу*

Згідно з одержаними даними, сайт розміщується на сервері з IP-адресою 91.237.250.18, яка належить компанії «Antiddos Protections Ltd – Украина» (рис. 17).

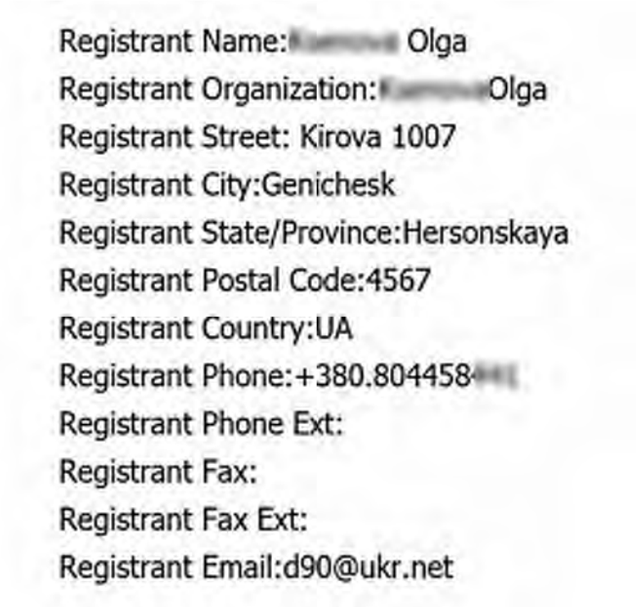



*Рис. 17. Дані щодо реєстрації доменного імені*

Після встановлення інформації про володільця сайту з використанням сервісів Whois відомості про правопорушника можна отримати, надіславши провайдеру (оператору) телекомунікацій відповідний запит (у даному випадку з метою одержання даних щодо особи, яка замовила для цього сайту послуги хостингу та захисту інформації). Паралельно у рамках відкритого кримінального провадження слід ініціювати **одержання вказаних даних через процедуру тимчасового доступу до речей і документів**.

Як видно із зазначених даних, при реєстрації доменного імені ***al.org в якості контактної електронної пошти було вказано адресу d90@ukr.net, яка належить до адресного простору Української компанії «Укрнет». Це дає можливість надіслати до товариства «Укрнет» офіційний запит на отримання контактних даних власника цієї поштової скриньки, переліку IP-адрес, з яких здійснюється доступ до неї. Крім цього, необхідно отримати рішення суду на вилучення історії листування абонента. Аналогічні дії слід провести щодо електронної адреси, яка вказана в якості контактної на веб-сайті ***al@ukr.net.

Також з метою одержання інших даних щодо користувача, який зареєстрував доменне ім'я http://www.***al.org варто каналами Інтерполу звернутися на адресу компанії cloudns.net, яка його обслуговує.

Взагалі, якщо необхідно одержувати дані від провайдерів Інтернет-послуг, розташованих за межами національної юрисдикції, правоохоронним органам слід діяти через Національне бюро Інтерполу. Разом з тим слід першочергово звернутись до провайдерів Інтернет-послуг із запитом про **збереження потрібних даних** через форму зворотного зв'язку або іншим способом. Це робиться для того, аби запобігти видаленню даних до завершення процедури отримання відповідних дозволів на їх вилучення.

Прохання щодо збереження даних повинно містити коротке викладення суті правопорушення, що має місце в даному випадку, точний опис даних, які необхідно зберегти, стисле викладення того, яке відношення до правопорушення мають ці дані, та заяву про те, що слідом за цим запитом надійде офіційне клопотання про розкриття даних [47, с. 4].

Наведемо декілька контактних даних для збереження і одержання інформації (табл. 4).

Усі контакти необхідно здійснювати виключно через службову електронну поштову адресу (закінчується на gov.ua).

*Таблиця 4*

| Назва ресурсу | Контактні дані для взаємодії |
|---|---|
| www.amazon.com | subpoena@amazon.com |
| www.apple.com | subpoenas@apple.com |
| www.blackberry.com | pso.us@blackberry.com |
| www.cloudflare.com | abuse+law@cloudflare.com |
| www.dropbox.com | legalcompliance@dropbox.com (https://dl.dropboxusercontent.com/s/chy2h514ht8j2hz/Dropbox%20Law%20Enforcement%20Handbook.pdf?dl=0) |
| www.facebook.com | records@facebook.com або www.facebook.com/records |
| www.google.com | uslawenforcement@google.com |
| www.instagram.com | lawenforcement@instagram.com або www.facebook.com/records |
| www.linkedin.com | https://www.linkedin.com/help/linkedin/answer/16880 |
| www.mail.com | legalnotice@mail.com |
| www.msn.com | lealert@microsoft.com |
| www.myspace.com | compliance@support.myspace.com або у надзвичайних випадках lawenforcement@support.myspace.com |
| www.skype.com | lerm@skype.net |
| www.twitter.com | lawenforcement@twitter.com або https://support.twitter.com/forms/lawenforcement |
| www.whatsapp.com | rdang@fortisgc.com |
| www.yahoo.com | lawenforcement-request-delivery@yahoo-inc.com |

Подальший збір даних необхідно здійснити шляхом моніторингу всієї інформації в мережі Інтернет щодо даних, отриманих вище. Так, пошук за критерієм електронної адреси d90@ukr.net, дозволить ідентифікувати ескортне агентство, яке є відповідальним за вказаний вид протиправної діяльності (рис. 18-а, 18-б). Зверніть увагу, що відповідний пошук здійснюється із застосуванням лапок «», які вказують на пошук точної фрази.

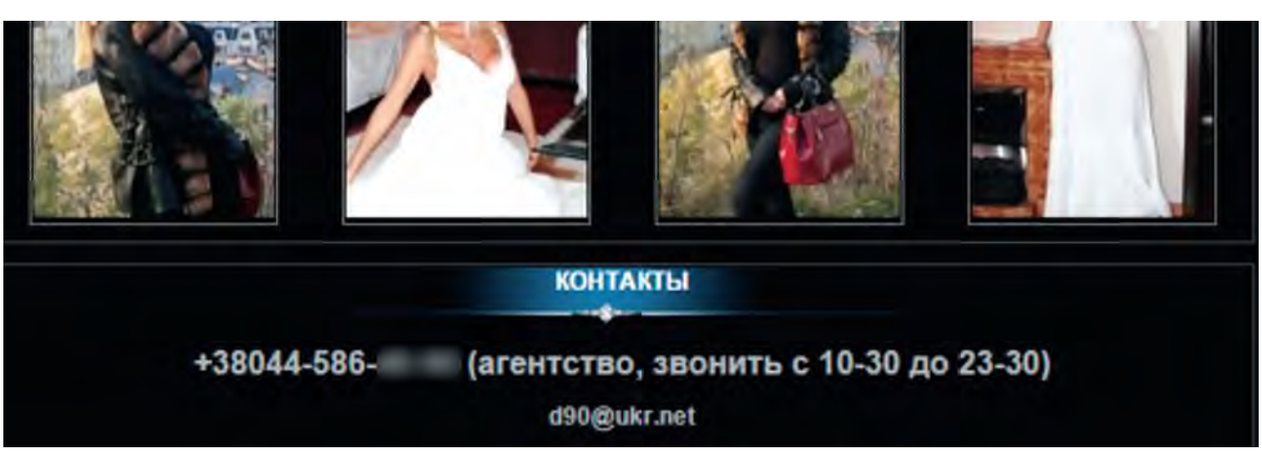



*Рис. 18-а. Сайт, на якому зустрічається шукана адреса електронної пошти*

Вихідний код сторінки сайту містить більше інформації, ніж та, що відображається на екрані, наприклад:

- коментарі користувача/розробника (можна знайти паролі, ідентифікатори або посилання на місце розташування);
- приховані поля;
- посилання на зовнішні сайти, на яких можна знайти незалежні джерела доказів.

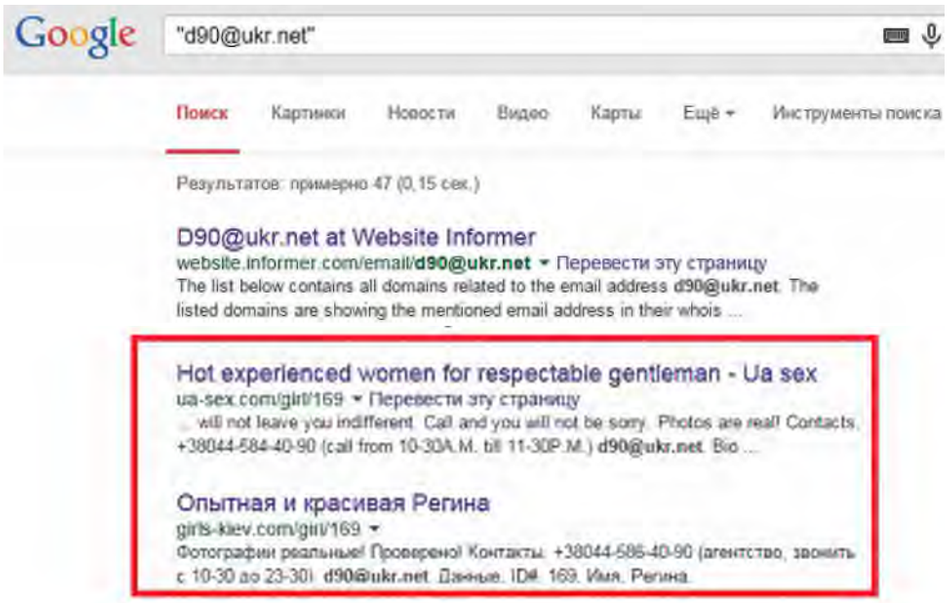



*Рис. 18-б. Результати пошукового запиту в пошуковій системі Google*

Також у вихідному коді існують метадані, які можуть бути джерелом інформації про саму веб-сторінку, наприклад, інформація про дату останньої модифікації веб-ресурсу (веб-сторінки, зображення тощо). На рис. 19 показаний фрагмент знімку екрану, де виведено інформацію про час останньої модифікації одного із зображень веб-сторінки, яка отримана за допомогою безкоштовного додатку HttpFox для Mozilla Firefox. Існує багато подібних розширень для різних браузерів, при використанні яких зі звичайної сторінки можна отримати багато корисної для розслідування інформації.

| Response Header | Value |
|---|---|
| Server | nginx |
| Date | Tue, 12 Sep 2017 08:39:07 GMT |
| Content-Type | image/png |
| Content-Length | 342 |
| Connection | keep-alive |
| Last-Modified | Fri, 08 Sep 2017 12:42:00 GMT |
| ETag | "59b29018-156" |
| Expires | Tue, 19 Sep 2017 08:39:07 GMT |
| Cache-Control | max-age=604800 |

*Рис. 19. Метадані веб-ресурсу*

Слід зауважити, що кримінальна діяльність, пов'язана з сексуальним насильством над жертвами з використанням веб-сайтів, несе у собі більший ризик, ніж класичні порнографічні сайти, оскільки такі факти складно приховати. Це примушує злочинців вчинювати інші кримінальні правопорушення для забезпечення належного функціонування такої торгівлі, наприклад, підробку документів, інструментів оплати, корупції.

**ЗАВДАННЯ**

**ЗА ДОПОМОГОЮ ВІДОМИХ СЕРВІСІВ ВСТАНОВІТЬ ПРИНАЛЕЖНІСТЬ IP-АДРЕСИ 79.108.18.4**

## 2. КОМП'ЮТЕРНІ СОЦІАЛЬНІ МЕРЕЖІ

Термін «соціальні мережі» – відносно нове явище інформаційних технологій і має різні визначення. Технології соціальних мереж приймають різноманітні форми і, по суті, засновані на мережних інтернет-технологіях, включаючи електронні журнали та інтернет-форуми, веб-журнали, соціальні блоґи, мікроблоґи, вікі, соціальні медіа, підкасти, фотографії або зображення, відео, рейтинги та соціальні закладки [48]. Одними з найбільш популярних соціальних мереж в Україні є «Facebook», «Twitter», «Linkedin», «Instagram».

У контексті торгівлі людьми, злочинці можуть скористатися цими сайтами для виявлення і експлуатації жертв у різний спосіб, наприклад, встановивши дружні стосунки з певними типами осіб з бідніших країн, які хочуть стати економічними мігрантами, і пропонуючи їм роботу в обмін на гроші або послуги. Таких жертв можуть заманювати обіцянками роботи, яка насправді не існує або, якщо й існує, то зводиться до підневільного стану або сексуальних послуг. Соціальні медіа пропонують злочинцям елемент анонімності і прикриття, тому вони можуть спілкуватися з жертвами на ранньому етапі, майже не ризикуючи, що їх виявлять або заарештують.

Перевагою для правоохоронних органів є те, що соціальні мережі – це набір інструментів, які можуть бути використані для покращення правоохоронної функції та розширення зв'язків з традиційними та онлайновими спільнотами. Недоліком соціальних мереж для правоохоронців є те, що це надзвичайно складне середовище для роботи, тому провадження з їх використанням службової діяльності пов'язане з величезними труднощами та вимагає чималих трудових і технічних ресурсів.

Нижче пропонуються деякі міркування, покликані допомогти правоохоронним органам покращити розуміння методів виявлення, попередження та розслідування злочинів із застосуванням соціальних мереж:

1) *використання псевдонімів*. Багато інтернет-користувачів, не тільки злочинців, використовують цілу низку псевдонімів, які відрізняються залежно від того, якою частиною Інтернету вони користуються. Це особливо актуально для сайтів соціальних мереж;

2) *фальшива інформація*. Як і з псевдонімами, суттєвий обсяг інформації, яку можна одержати з Інтернету, має ненадійні вказівки на джерело її походження та об'єктивність, тому завжди слід бути обачним і шукати підтвердження достовірності одержаних відомостей;

3) *збір доказів*. Сайти соціальних мереж є потужним джерелом доказів, але пам'ятайте про застосування того самого принципу достовірності та допустимості, що і в реальному світі;

4) *визначення місцезнаходження*. Багато користувачів надають чимало подробиць свого місця перебування, статусу, кого вони відвідують та багато інших подробиць стилю свого життя, звичок тощо. Це стосується і жертв торгівлі людьми та самих торговців, які можуть залишити критично важливі докази у різних частинах соціальних мереж;

5) *дослідження новітніх шляхів збору інформації та інформації від широкого загалу*. Історично склалося, що правоохоронні органи використовували традиційні медіа як канал зв'язку з громадськістю для пошуку інформації про злочини чи інші соціальні проблеми, тому соціальні мережі є ідеальною платформою для продовження цього процесу та можуть сприяти загальному збору інформації або підготовці конкретних звітів щодо підозрілої злочинної діяльності та отриманню інших оперативних даних;

6) *важливо налагодити робочі стосунки з провайдерами соціальних мереж*. Правоохоронцям необхідно встановлювати та підтримувати тісні робочі стосунки з компаніями у сфері соціальних медіа (особливо з тими, які активно працюють у регіоні) щодо можливості законного отримання комунікаційних даних. Це допоможе отримати реалістичне розуміння очікувань того, що вони робитимуть одне для одного, особливо запитів на одержання даних та швидкості надання відповідей в рамках місцевих законодавчих та нормативних положень.

7) *слід звертатися до громадськості по інформацію одразу після інциденту.* Важливо не відкладати звернення до громадськості по допомогу та пояснення того, як людям слід надавати інформацію. Найефективнішу відповідь можна отримати, коли люди все ще перебувають під безпосереднім впливом інциденту, до того, як інтерес громадськості ослабне. Цього слід домагатися за рахунок узгодженої медіа стратегії та залучення досвідченого працівника зі зв'язків з громадськістю для відстеження та оцінки можливостей звернення до громадськості та донесення офіційної позиції. Враховуючи розповсюдженість соціальних мереж, при розслідуванні злочинів пов'язаних з торгівлею людьми, не зайвим буде зорієнтувати слідчих та оперативних працівників, на розповсюдження там закликів про допомогу щодо розшуку зниклих осіб, злочинців, які переховуються від сторони обвинувачення, визначення місцезнаходження місця, яке зображено на фотографії, тощо;

8) *правоохоронний орган повинен мати можливість працювати з великими обсягами вхідної інформації.* Потрібно заздалегідь запровадити механізми для негайного збору інформації, а не чекати кілька днів після події для їх впровадження;

9) *слід уважно вивчити всі відповідні оперативні дані та інформацію.* Потрібно критично ставитись до всіх оперативних даних та даних соціальних медіа. Важливо, щоб вся інформація проходила через певний механізм оцінки, детальне вивчення та процес ухвалення рішень для виявлення хибної інформації на ранніх етапах і вживання відповідних дій на основі достовірної інформації;

10) *не слід відкидати традиційні підходи.* Дуже важливо, щоб традиційні підходи, перевірені багатьма роками позитивної практики, не відкидались. Проблема полягає у тому, щоб об'єднати нове зі старим і на основі цього виробити оптимальні практичні підходи, які зможуть забезпечити найкращі та найдостовірніші результати;

11) *виявлення злочинних мереж.* Соціальні медіа – це цінний інструмент, який дозволяє бачити діяльність злочинця на етапі, коли він почувається комфортно. Об'єкти вихваляються і публікують інформацію про свої подорожі, хобі, відвідані місця, зустрічі, коло друзів, членів сім'ї, стосунки, дії тощо;

12) *використання соціальних мереж для збору оперативно значимої інформації.* Використання соціальних медіа у цілях розслідування не є чимось незвичним. Однак це не значить, що проблеми, пов'язані з цією практикою, було подолано. Навпаки, правові аспекти використання соціальних мереж з метою збирання оперативно-розшукової інформації ще не достатньо випробувано в суді. Для правоохоронних органів важливо взаємодіяти із законодавцями для створення прийнятних законів, політики та процедур управління збором доказів, особливо тих, що стосуються роботи правоохоронних органів у соціальних медіа та інших частинах онлайнового світу.

13) *подумайте, хто користуватиметься соціальними мережами для проведення розслідувань.* Правоохоронні органи приймають різні рішення стосовно того, які працівники матимуть право застосовувати соціальні медіа у своїй діяльності.

НАПРИКЛАД, У ВЕЛИКОБРИТАНІЇ СТВОРЕННЯ ЛЕГЕНДОВАНОГО ПРОФІЛЮ СОЦІАЛЬНОЇ МЕРЕЖІ НЕ Є СПЕЦІАЛЬНИМ ЗАХОДОМ ПОЛІЦІЇ, ЯКИЙ ПОТРЕБУЄ САНКЦІОНУВАННЯ. У США ПРАЦІВНИКИ ФБР ТАКОЖ МОЖУТЬ ВИДАВАТИ СЕБЕ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА НЕПОВНОЛІТНІХ, СПІЛКУЮЧИСЬ З ПЕДОФІЛАМИ, ЯК ЦЕ БУЛО, НАПРИКЛАД, У СПРАВІ ПАТРІКА НОТОНА 1999 РОКУ [49, С. 279-280].

Інформація, на яку варто звертати увагу на сайтах соціальних мереж під час документування протиправної діяльності, включає:

- **внутрішні ідентифікатори** (ID), які застосовуються для відстеження будь-якої активності на сайті (користувачі, фотографії, чати, сеанси, групи, позначки «мені подобається» і т.д.).

Наприклад, Facebook використовує ідентифікатор «fbid» (https://www.facebook.com/photo.php?fbid=10103832396388711). Поряд із отриманням скріншоту профіля, зображення тощо підозрюваного доцільно встановити його внутрішній ідентифікатор в базі даних соціальної мережі;

- **чат**. Користувачі соціальних мереж можуть вести відео-, аудіо- або текстові діалоги з іншими користувачами. Відповідно такі чати у коді веб-сторінки містять ідентифікатори користувачів і об'єктів, які передаються в цих діалогах і які необхідно фіксувати слідчому при огляді.
- **зображення**. Зображення, які завантажуються користувачами на сайти найбільш популярних соціальних мереж, пропускаються через «очисні» фільтри, але деякі соціальні мережі та інші веб-сайти публікують їх без попередньої обробки. Зображення можуть містити метадані (як правило, в форматі EXIF): дата і час знімка, фокусна відстань, координати широти і довготи. Існують програми, що дозволяють швидко знайти і завантажити велику кількість зображень, а потім витягти їх метадані у форматі EXIF.

Тепер е розглянемо практичні аспекти використання соціальних мереж для вчинення торгівлі людьми. Як вже зазначалося через свої особливості – масовий характер, можливість залишатися анонімним, можливість пошуку широкого кола осіб, залежно від місця проживання, роботи, інтересів тощо, зробили соціальні мережі одним із найпотужніших інструментів для вербування майбутніх жертв торгівлі людьми.

З цією метою здебільшого створюються спеціалізовані групи, де рекламуються сексуальні послуги, або розміщується реклама «вкрай» вигідних умов працевлаштування жінок за кордоном (рис. 20, 21).

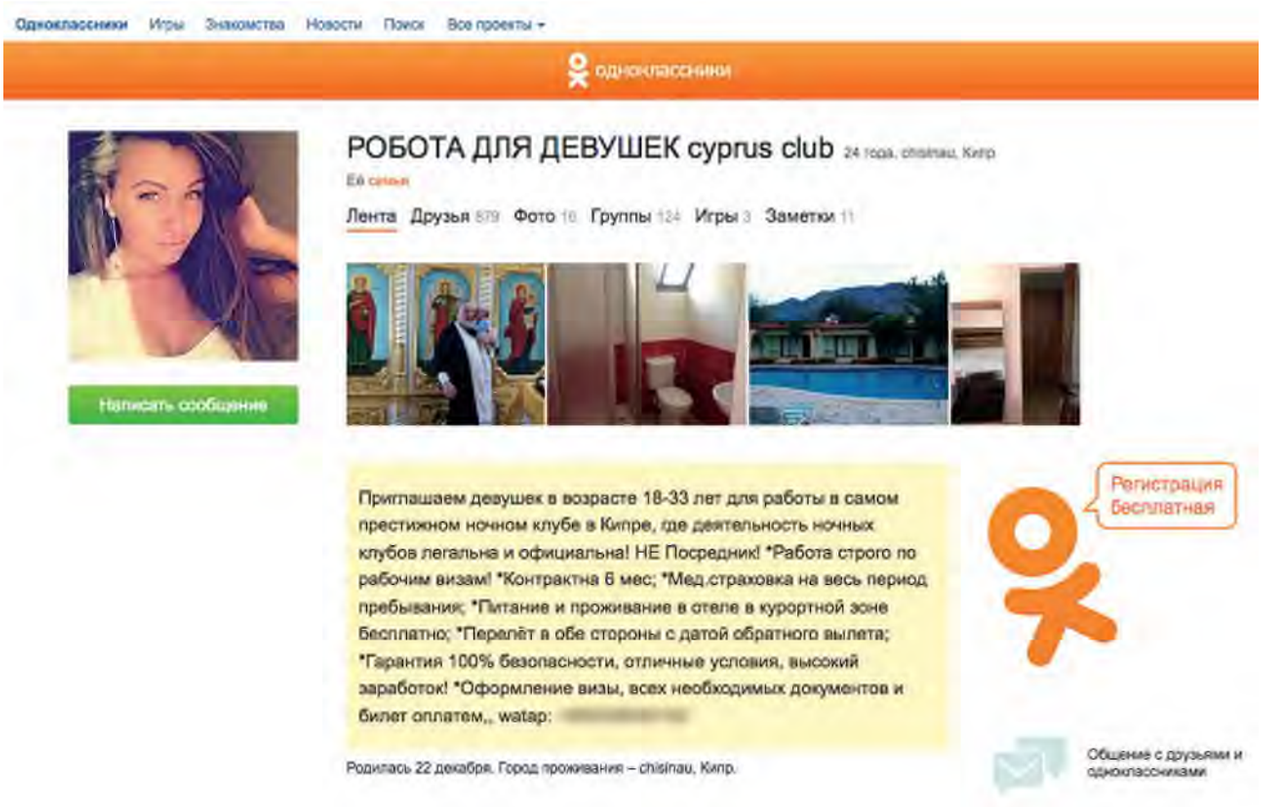



*Рис. 20. Пропозиції з «вигідного» працевлаштування на сайті «Одноклассники»*

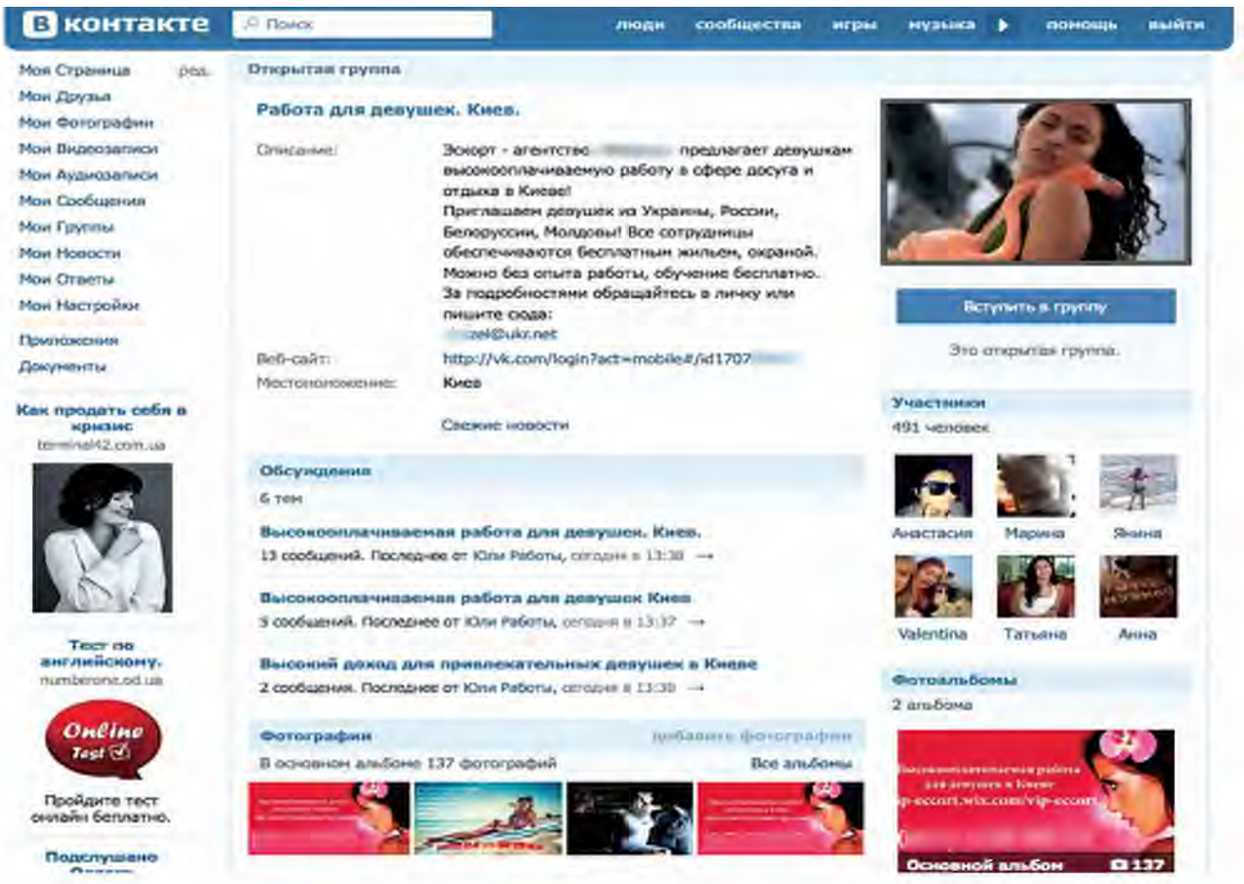



*Рис. 21. Пропозиції з «вигідного» працевлаштування на сайті «Вконтакте»*

У 2014 РОЦІ МЕШКАНКА КИЇВСЬКОЇ ОБЛАСТІ У ЗМОВІ З МЕШКАНКОЮ ІНДІЇ СТВОРИЛА НА СОЦІАЛЬНОМУ ПОРТАЛІ HTTP://WWW.VK.COM СТОРІНКУ КОРИСТУВАЧА, З ЯКОЇ ЗДІЙСНЮВАЛА РОЗПОВСЮДЖЕННЯ ПОВІДОМЛЕНЬ ПРО ПОШУК ЖІНОК ДЛЯ РОБОТИ В ІНДІЇ НА ВИГІДНИХ УМОВАХ ТА, В РАЗІ НЕОБХІДНОСТІ, ВИГОТОВЛЕННЯ ЇМ ЗАКОРДОННИХ ПАСПОРТІВ ГРОМАДЯНИНА УКРАЇНИ, ОФОРМЛЕННЯ ВІЗ ТА БРОНЮВАННЯ КВИТКІВ. НАСПРАВДІ ЗЛОЧИНЦІ МАЛИ НА МЕТІ ВЕРБУВАННЯ ТА ПЕРЕМІЩЕННЯ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНИ ДЛЯ ПОДАЛЬШОГО ВИКОРИСТАННЯ ОСІБ, ЯКІ ВІДГУКНУЛИСЬ НА ОГОЛОШЕННЯ, У СВОЇХ НЕЗАКОННИХ ЦІЛЯХ, ЗОКРЕМА, ПОДАЛЬШОЇ СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ В БОРДЕЛЯХ М. МУМБАЇ.

У РЕЗУЛЬТАТІ ОПЕРАТИВНИХ ДІЙ ПРАВООХОРОННИХ ОРГАНІВ ВКАЗАНУ ЗЛОЧИННУ ДІЯЛЬНІСТЬ БУЛО ПРИПИНЕНО, А МЕШКАНКУ КИЇВСЬКОЇ ОБЛАСТІ ВИЗНАНО ВИННОЮ У ВЧИНЕНІ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО Ч. 2 СТ. 149 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ТА ПРИЗНАЧЕНО ЇЙ ПОКАРАННЯ ЗА ЦІЄЮ СТАТТЕЮ У ВИГЛЯДІ П'ЯТИ РОКІВ ПОЗБАВЛЕННЯ ВОЛІ БЕЗ КОНФІСКАЦІЇ МАЙНА.

Документування такої протиправної діяльності необхідно розпочинати із збору інформації та ідентифікації можливих підозрюваних. Для цього необхідно детально оглянути сторінку соціальної мережі. В даному випадку увагу правоохоронних органів повинна привернути назва ексорт-агенства, контактні дані – адреса електронної поштової скриньки xxxx@ukr.net (адресу змінено) та номера телефонів на візитних картках.

На другому етапі необхідно проаналізувати усіх учасників вказаної групи, що дасть можливість визначити коло потенційних жертв торгівлі людьми, а також зв'язки підозрюваних. Особливої уваги у процесі ідентифікації слід приділити засновнику та адміністратору групи в соціальній мережі (рис. 22), оскільки саме вони є відповідальним за наповнення її новинами, рекламою, спілкування із потенційними жертвами тощо.

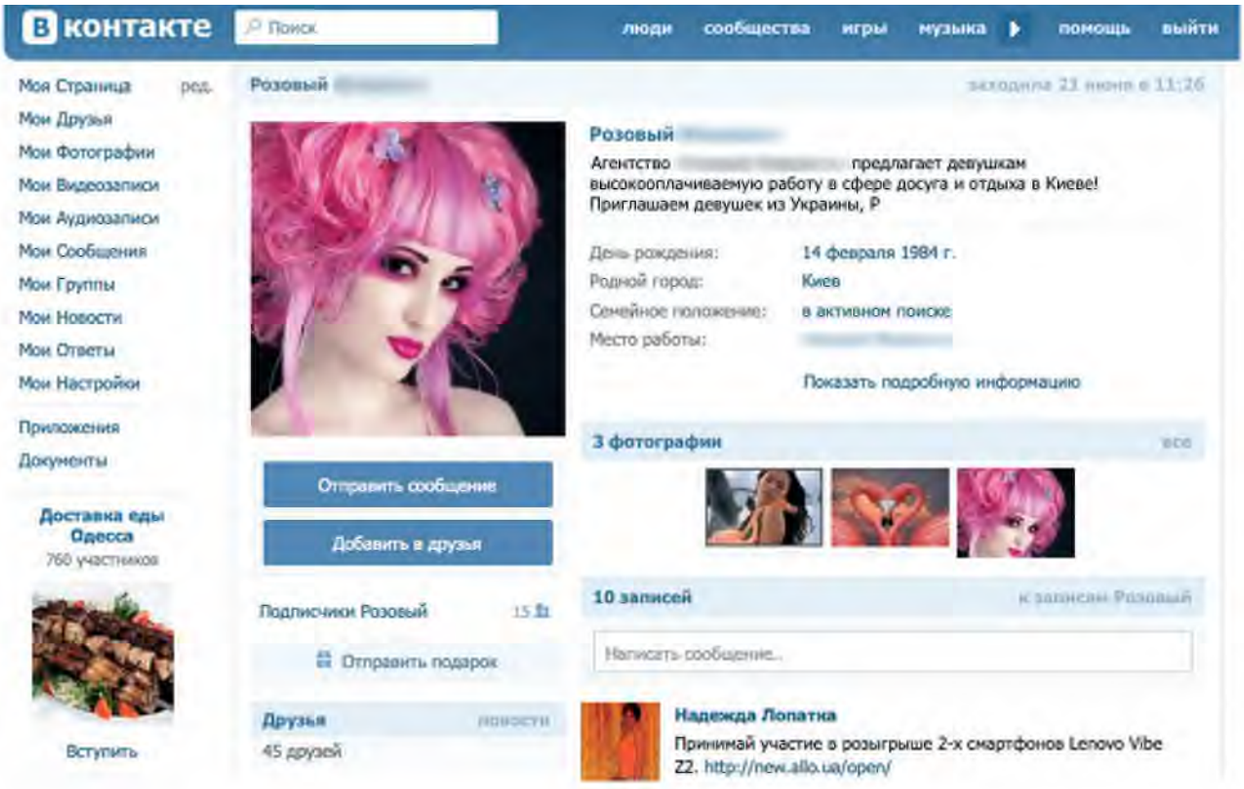



*Рис. 22. Сторінка адміністратора групи на сайті «Вконтакте»*

У даному випадку використовуються вигадані дані, однак сторінка адміністратора дає важливу інформацію щодо можливої дати народження (доволі часто вона вказується правдиво), місця проживання та друзів (рис. 23).

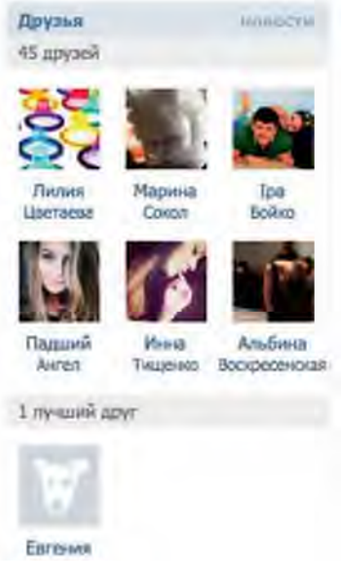



*Рис. 23. Друзі адміністратора групи на сайті «Вконтакте»*

Саме контакти правопорушника дозволяють визначитися із його ймовірним місцем проживання чи навчання (адже якщо 80-90% проживають у Києві, то справедливо припустити, що й сам правопорушник зі столиці).

У наведеному прикладі один із контактів має статус «кращий друг», і додатковий аналіз його сторінки може значно допомогти в ідентифікації шуканої особи.

Під час розслідування слід особливу увагу слід звернути на сторінки, спільноти, які цікавлять чи відвідуються особою, щодо якої накопичується інформація, адже на підставі такого аналізу можна зробити висновок щодо її вподобань, хобі, або, наприклад, салонів краси чи спортивних залів, які вона відвідує тощо. Про ступінь близькості контактів фігуранта, а відповідно й джерело додаткової інформації, свідчить перелік осіб, які оцінюють його фотографії тощо.

Одним із найважливіших прийомів ідентифікації особи є моніторинг через мережу Інтернет усієї контактної інформації, залишеної на особистій сторінці. Це дозволяє максимально повно зібрати необхідні дані.

У даному випадку пошук за електронною адресою, вказаною на сторінці дозволяє встановити номер мобільного телефону, яким користується особа (рис. 24).

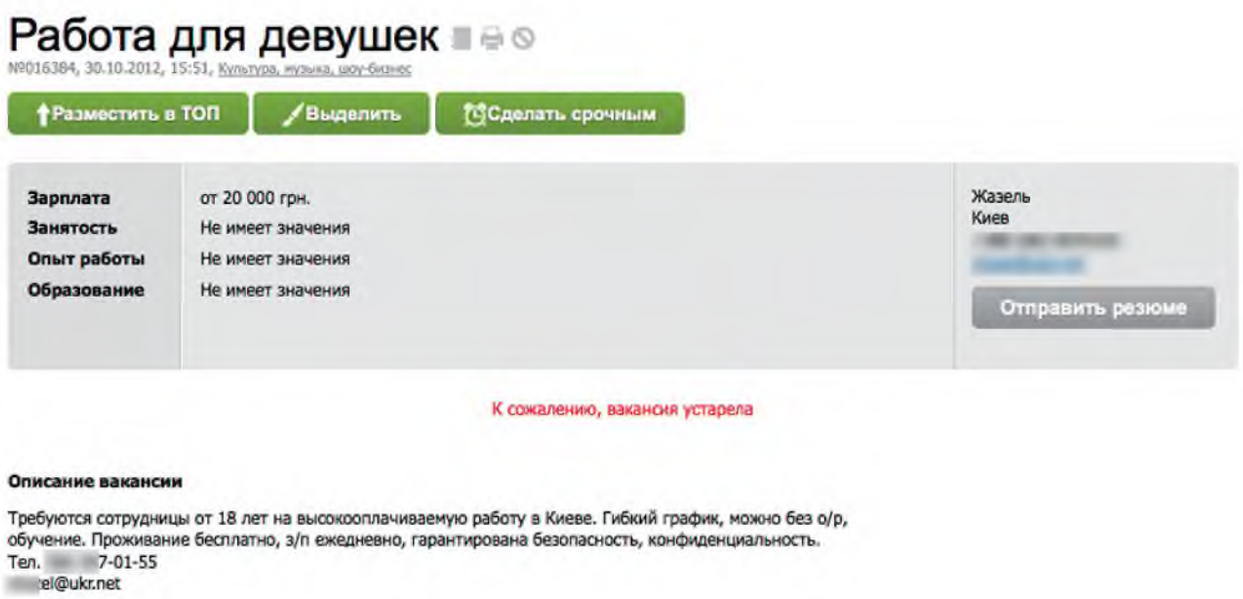



*Рис. 24. Контактні дані шуканої особи*

Моніторинг за номером мобільного телефону дозволяє встановити додаткову адресу електронної пошти (рис. 25).

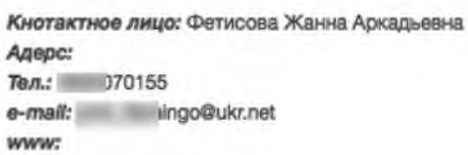



*Рис. 25. Результати додаткового пошуку в мережі за раніше знайденим номером телефону шуканої особи*

Свого часу зловмисники злегковажили і вказану електронну адресу вказали як контактну для одного зі своїх легітимних бізнесів, що в кінцевому результаті дозволило слідчому, застосувавши методи пошуку інформації в мережі Інтернет встановити особу зловмисника та можливе місце сексуальної експлуатації жінок (рис. 26).

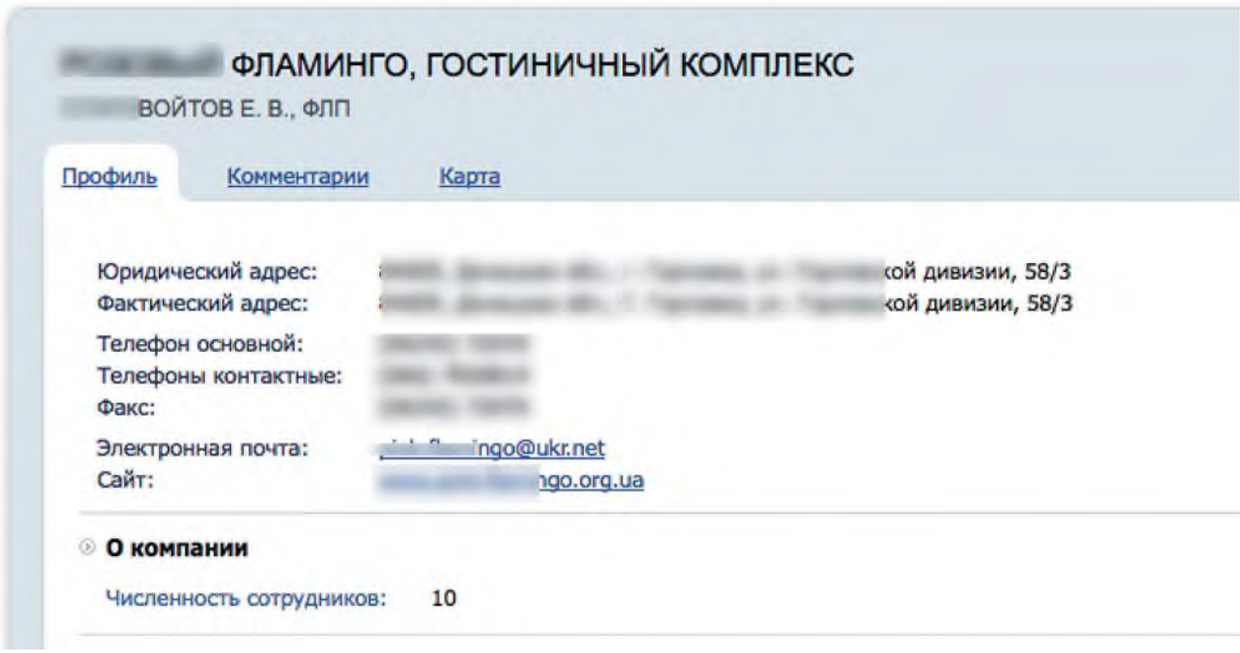



*Рис. 26. Відомості про діяльність правопорушника*

Ще одним прикладом ідентифікації жертви сексуального насильства та злочинця можуть слугувати матеріали кримінального провадження, відкритого у 2013 році за фактом розбещення неповнолітнього та розповсюдження продукції порнографічного характеру, виготовленої за його участю.

До правоохоронних органів України від колег з Молдови надійшли фотознімки із дитячою порнографією, які розповсюджувалися через пірингові мережі. На них було зображено молодого хлопця, який піддавався сексуальному насильству зі сторони двох дорослих.

Детальним аналізом було встановлено, що зйомка проходила у приміщенні, яке могло бути квартирою. Із елементів інтер'єру на себе звернула увагу підлога, обшивка дивану (рис. 27), а також оголошення та нагороди на тематику кінології.

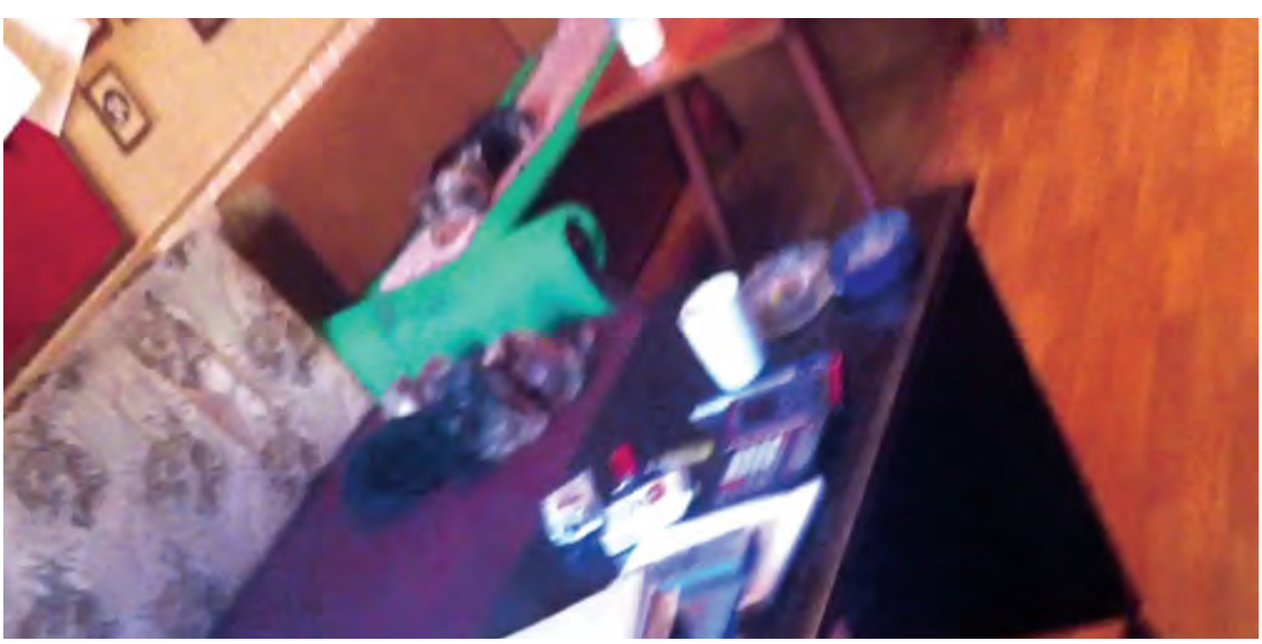


*Рис. 27. Інтер'єр квартири*

Підлога у вигляді паркетного лінолеуму, журнальний стіл, диван із коричневою обшивкою. На стіні були виявлені оголошення про проведення виставки собак (рис. 28).


*Рис. 28. Оголошення у сфері кінології*

Крім цього, на багатьох зображеннях були дві собаки породи Йоркширського тер'єра (рис. 17):

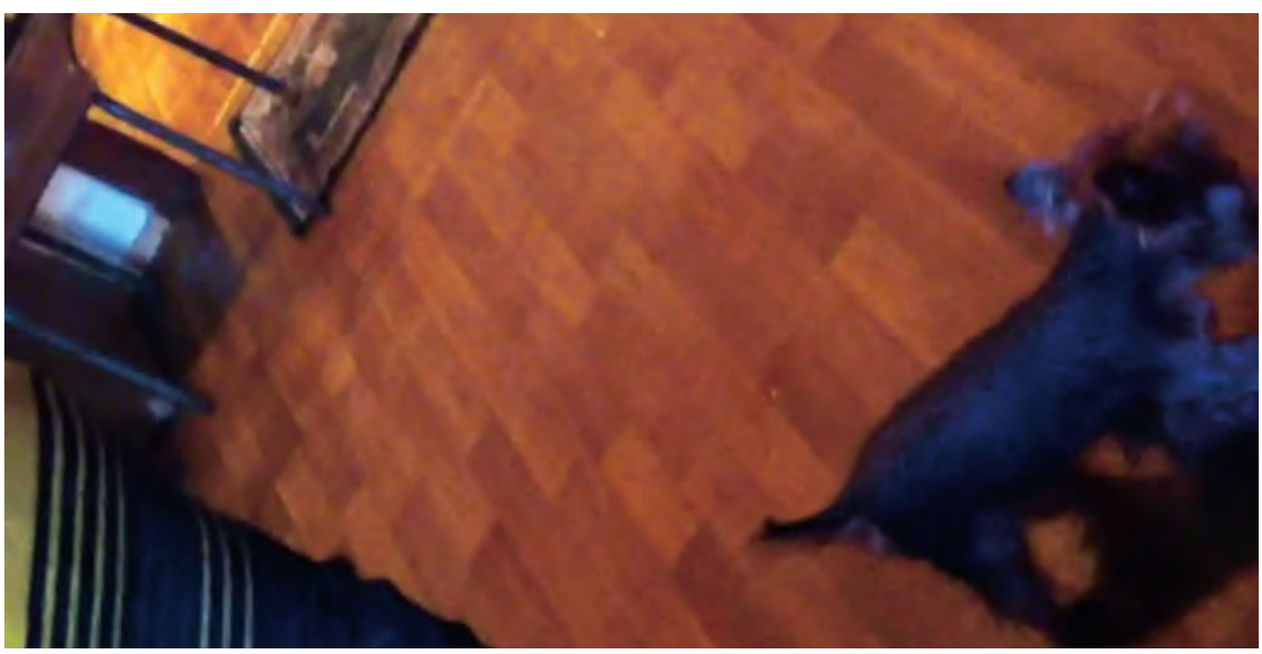


*Рис. 29. Фотографія собаки у квартирі*

Увагу слідчих привернув фотознімок жертви, зроблений на фоні дошки, де було наклеєно аркуш паперу, у нижній частині якого був номер телефону (рис. 30).

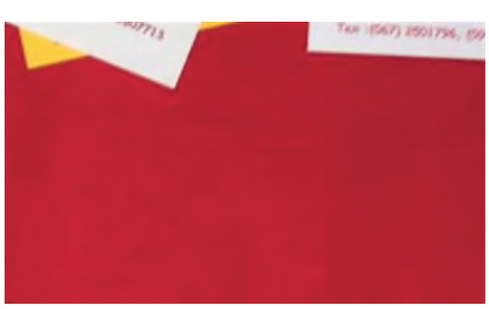


*Рис. 30. Фотографія паперу з номером телефону*

Пошук вказаного телефонного номеру в мережі Інтернет відразу показав, що він належить жінці, яка проживає в Сумській області (рис. 31).

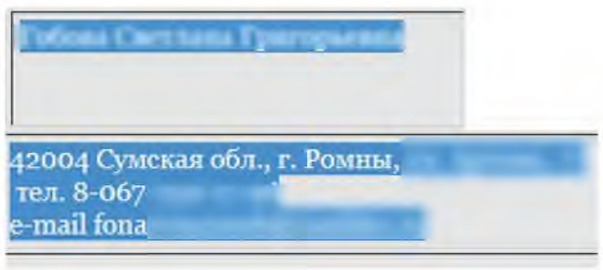



*Рис. 31. Результати пошуку за номером телефону*

Аналіз її сторінки в соціальній мережі «Facebook» показав, що вона професійно займається розведенням породистих собак та є членом місцевого кінологічного клубу. Під час відпрацювання контактів вказаної жінки у соціальній мережі відразу було виявлено, що на титульній сторінці, одного із її друзів було зображено двох собак породи Йоркширського тер'єра, які лежали на дивані із обшивкою, ідентичною до тієї, яка була на фотографіях із сценами сексуального насильства (рис. 32).

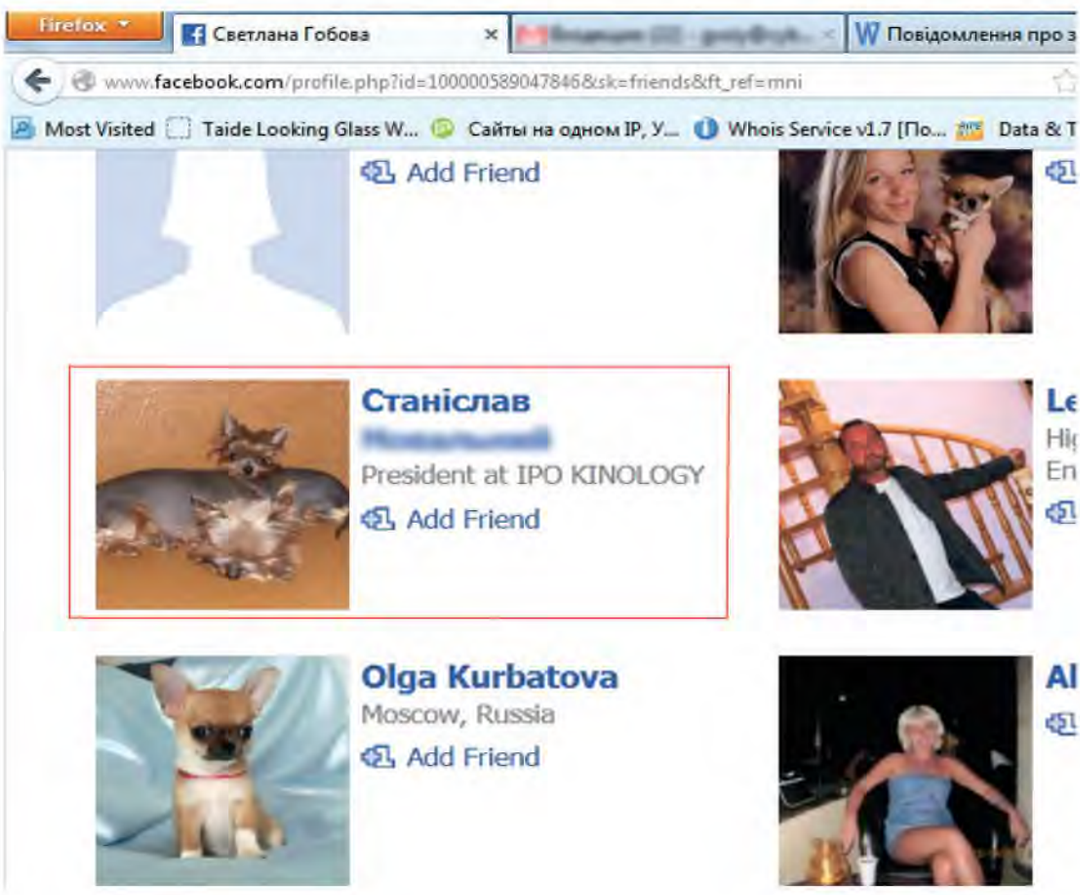



*Рис. 32. Аналіз контактів*

На сторінці цього контакту було фото із подібною до раніше вказаної підлоги в квартирі (рис. 33).

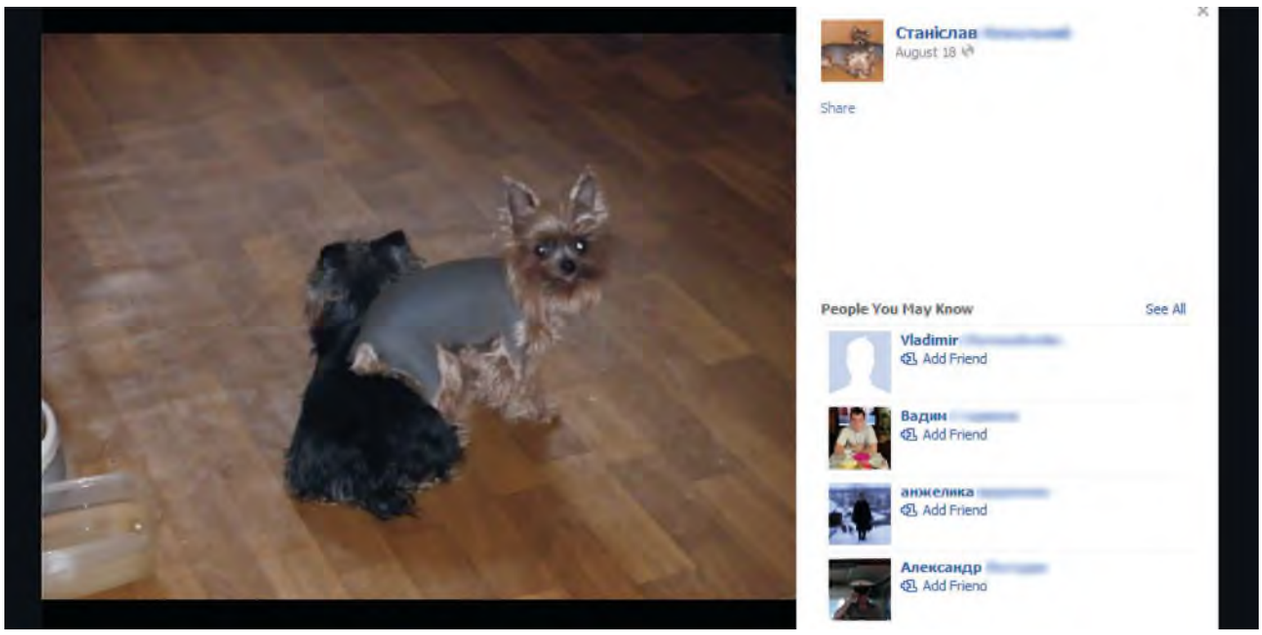



*Рис. 33. Фотографія зі сторінки правопрушника*

У друзях підозрюваного було виявлено сторінку малолітнього хлопчика який став жертвою сексуального насильства (рис. 34).


*Рис. 34. Сторінка жертви*

У подальшому вже проводилися традиційні заходи щодо документування протиправної діяльності підозрюваних.

Наступний приклад ідентифікації жертв торгівлі людьми демонструє успішну взаємодію вітчизняних правоохоронних органів із зарубіжними колегами.

Від правоохоронних органів Великобританії надійшов міжнародно-правовий запит щодо ідентифікації неповнолітніх, які ймовірно стали жертвами сексуального насильства підданого їх країни. Чоловік подорожував країнами Східної Європи, розбещував неповнолітніх та виготовляв порнографічну продукцію за їх участю.

Іноземні колеги надіслали понад 4 Гб матеріалів, виготовлених злочинцями (рис. 35).

*Рис. 35. Одна з фотографій потенційних жертв*

У результаті аналізу зображень правоохоронці дійшли попереднього висновку, що зйомка велася неподалік водойми (рис. 36-38) та якогось великого промислового об'єкту. Крім цього, на окремих фотографіях було зображено дитячий ігровий майданчик «Рошен».

*Рис. 36. Фотографія, на якій видно міст*

*Рис. 37. Фотографія, на якій видно водойму*

*Рис. 38. Фотографія, на якій видно дитячий майданчик*

Пошукові заходи було розпочато з одержання переліку міст, де було збудовано такі ігрові майданчики. Також було висунуто версію, що зйомка велася неподалік теплової чи гідроелектростанції. Порівнявши списки міст із майданчиками «Рошен» та «потенційних» місць проведення зйомки,пошук було звужено до 20 ймовірних міст.

У подальшому для пошуку застосували програмний продукт Google Earth (рис. 39). У результаті проведених заходів вдалося ідентифікувати усіх неповнолітніх (малолітніх), які стали жертвами педофіла.

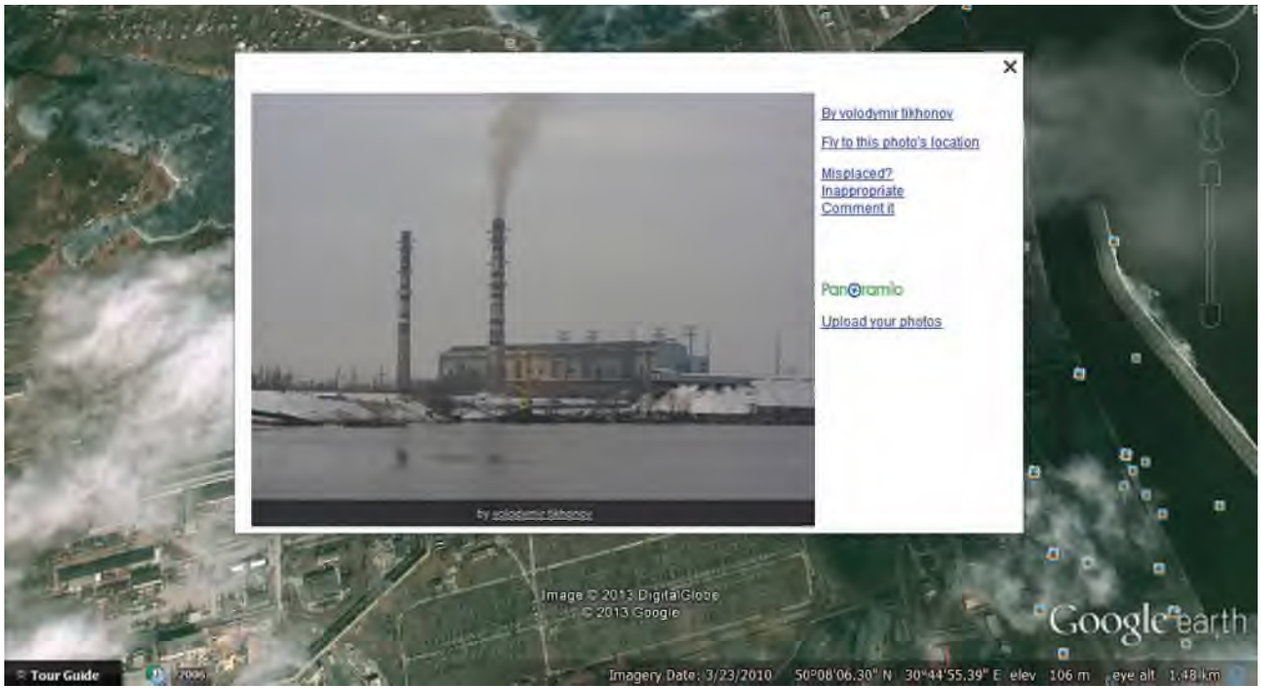



*Рис. 39. результат пошуку з використанням сервісу Google Earth*

Слід відмітити, що велику допомогу у встановленні осіб злочинців, які здійснюють торговці людьми, може надати адміністрація соціальних мереж.

У рамках взаємодії із такими ресурсами буде доцільно звернутися із запитом про надання правової допомоги у кримінальному розслідуванні через Головне слідче Управління та Генеральну прокуратуру України. Нормативно-правовими актами, які регламентують надання такої допомоги є Кримінальний процесуальний кодекс України [50], Європейська конвенція про взаємну допомогу у кримінальних справах від 20 квітня 1959 року, Додатковий протокол до неї, підписний у Страсбурзі 17 березня 1978 року та Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах, підписаний у Страсбурзі 08 листопада 2001 року (ратифікований в Україні 01 червня 2011 року) [51].

У соціальній мережі «Facebook» передбачено он-лайн режим запиту інформації, для цього працівнику правоохоронних органів слід перейти за посиланням https://www.facebook.com/records/x/login, де відкриється вікно реєстрації звернення (рис. 40).

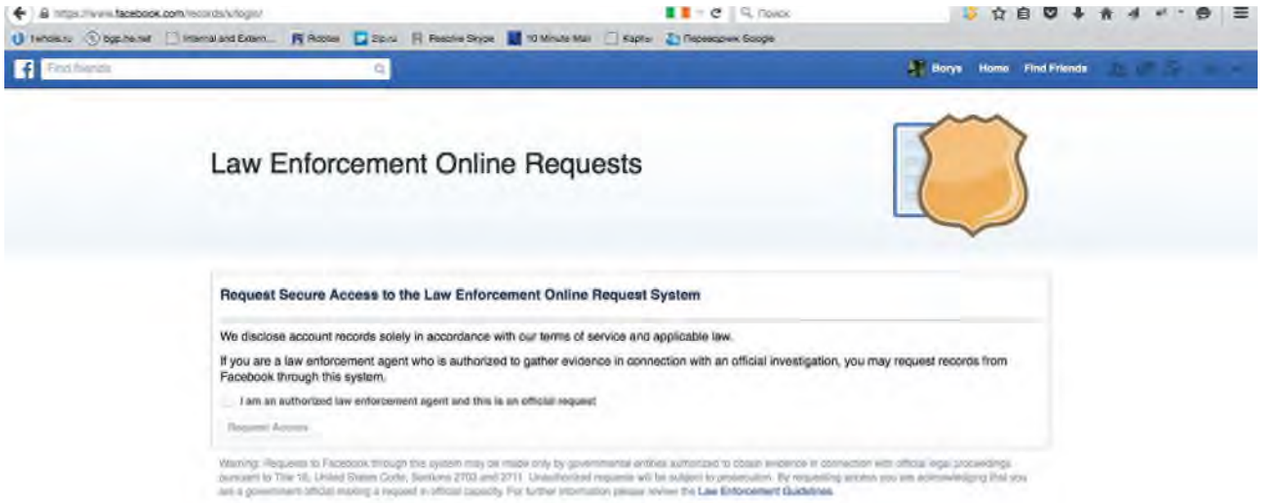



*Рис. 40. Вікно реєстрації звернення*

Далі необхідно зазначити свою службову адресу (рис. 41) електронної пошти (запити із вказівкою облікових записів загальнодоступних поштових сервісів, таких як gmail.com, mail.ru, ukr.net, yahoo.com, hotmail.com тощо реєструватися не будуть).

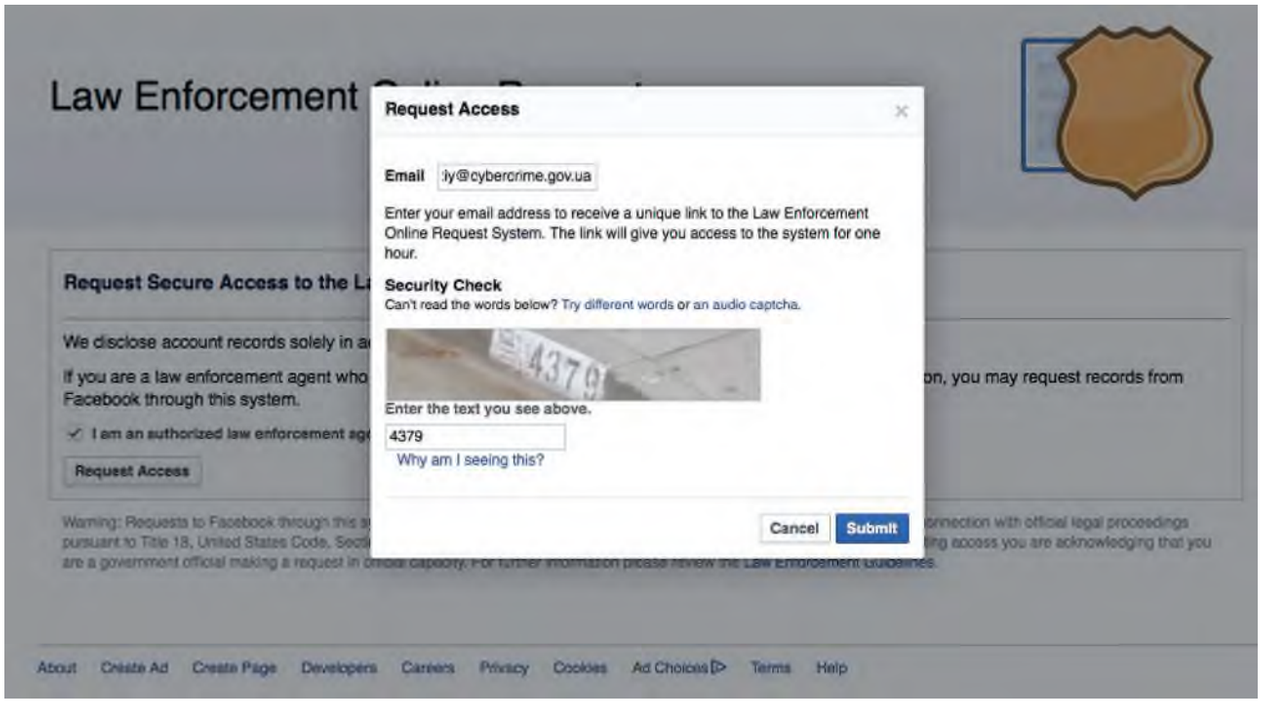



*Рис. 41. Введення адреси електронної пошти правоохороняа*

Після підтвердження введеної адреси електронної пошти відкривається робоче поле для надсилання запитів (рис. 42).

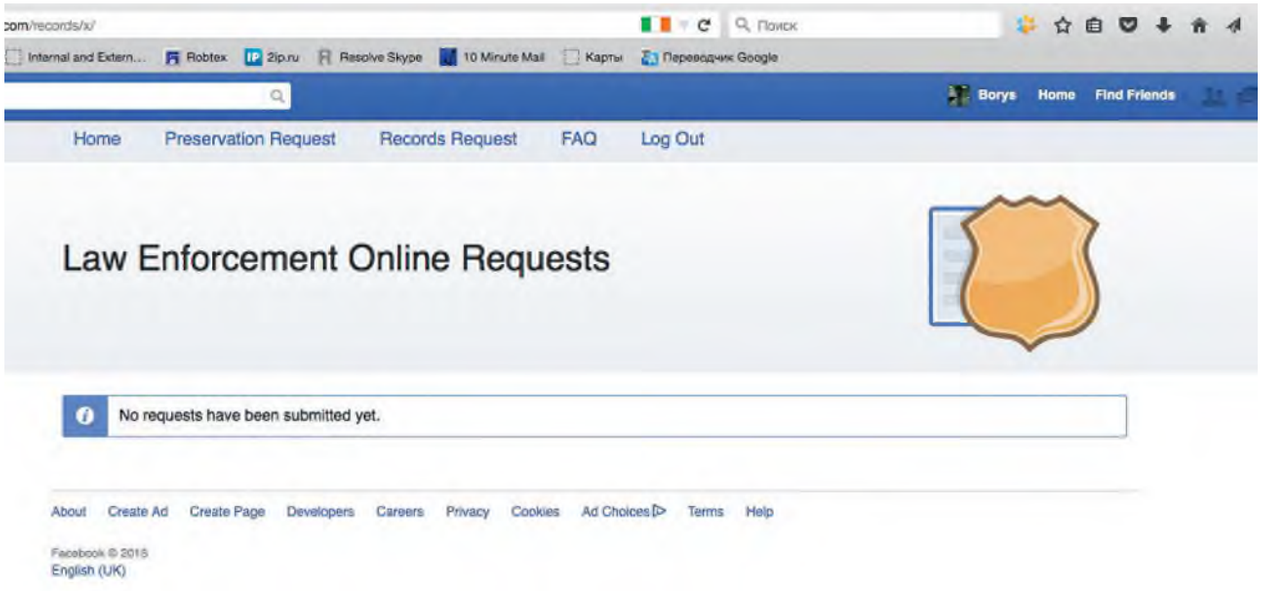



*Рис. 42. Вікно приймання запитів*

Через пункт меню «Preservation request» можна надіслати запит про збереження інформації щодо облікового запису, який становить інтерес для правоохоронних органів. Для цього необхідно зазначити лише номер справи та посилання на обліковий запис у соціальній мережі «Facebook» чи «Instagram» (рис. 43).

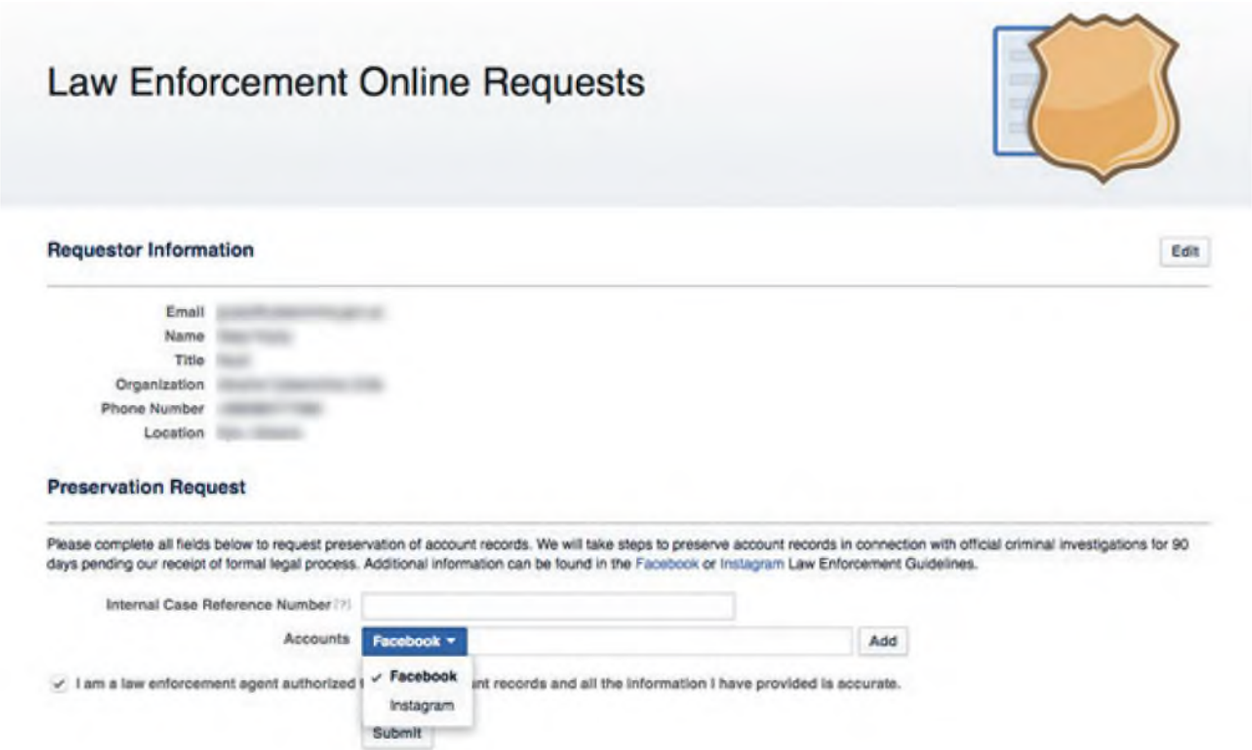



*Рис. 43. Введення запиту*

При надсиланні такого запиту інформацію, яка цікавить правоохоронні органи, буде збережено на серверах компанії «Facebook», а її видача можлива лише після надання рішення суду про доступ до облікового запису користувача.

Саме для таких випадків, а також надання даних щодо IP-адрес доступу до облікового запису, передбачено меню «Records request», де окрім даних щодо справи, вимагається надіслати рішення компетентного органу про отримання інформації (рис. 44).

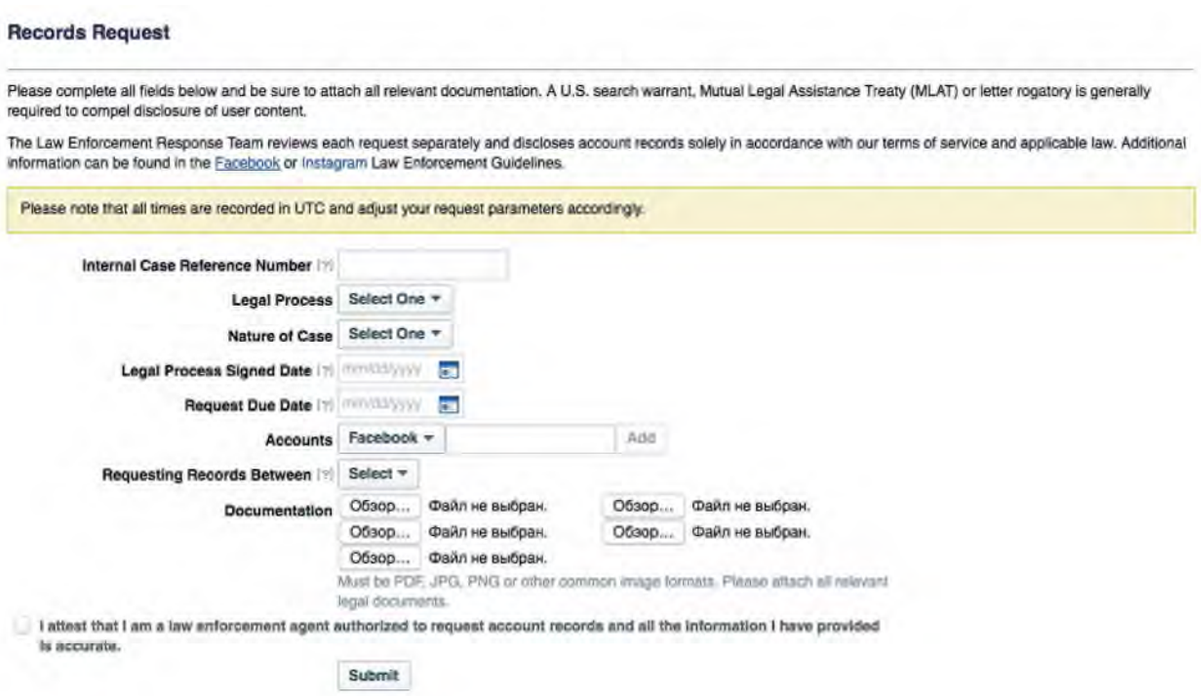



*Рис. 44. Додаткові параметри запиту*

Подібний тип взаємодії з правоохоронними органами пропонує і Twitter (www.support.twitter.com/articles/41949-guidelines-for-law-enforcement).

Для автоматизації процесу побудови зв'язків осіб у соціальній мережі може бути використано додаткове програмне забезпечення (i2, КРОНОС тощо).

**ЗАВДАННЯ**

**ПРОАНАЛІЗУЙТЕ МОЖЛИВОСТІ СЕРВІСУ HTTP://WWW.YASIV.COM/FACEBOOK ЩОДО ПОБУДОВИ ЗВ'ЯЗКІВ ДЛЯ СОЦІАЛЬНОЇ МЕРЕЖІ FACEBOOK**

## 3. ДОШКИ ОГОЛОШЕНЬ

**Електронна дошка оголошень** – це веб-сайт, цілком аналогічний звичайним побутовим дошкам оголошень або ж рекламним газетам. Її вміст – це набір оголошень комерційного та/або некомерційного характеру, які розміщується як на платній, так і на безкоштовній основі, залежно від конкретного сайту. Багато рекламних компаній, що мають паперові видання і що працюють у сфері теле- і радіореклами, створюють і підтримують також власні електронні дошки оголошень.

Електронні дошки оголошень бувають двох видів: ті, що модеруються (ті, у яких є так званий модератор – людина, яка контролює роботу цієї дошки) і ті, що не модеруються – що працюють автоматично [52].

Існують дошки оголошень, які спеціалізуються виключно на працевлаштуванні, при цьому вони дають можливість пошуку як роботи, так і працівників. Найвідомішими з них є kiev.ko.olx.ua, rabota.ua, hh.ua, job.ukr.net, rabotaplus.ua, rabota.ria.com, ищуработу.com.ua.

Злочинці, які вербують жертв торгівлі людьми, зазвичай одночасно розміщують оголошення на декількох дошках оголошень, що значно збільшує ймовірність пошуку та вербування жертви. Зміст оголошення, як правило, побудований таким чином, що завуальовано вказує на характер майбутньої роботи. При цьому вербувальники вміло застосовують прийоми психології, впливаючи на жертву через її вразливий стан, використовуючи як правило, фінансові та соціально побутові проблеми. Такі фрази, як «забезпечте собі та своїм рідним достойне майбутнє...», «достатньо собі завжди у всьому відмовляти, ви жінка і заслуговуєте на краще...», «не втрачайте свою молодість...», «наша робота – це чудова можливість побачити світ...», як правило, завжди діють на підсвідомість та допомагають знайти майбутній жертві «виправдання» своєму вчинку. Не рідко такі оголошення супроводжуються обіцянками забезпечити житлом, навчанням, кишеньковими витратами.

Також електронні дошки оголошень можуть використовуватись легально для розміщення обговорень, які надають поради шукачам дитячої порнографії, у тому числі URL-адреси дитячих порнографічних веб-сайтів та їхні рейтинги.

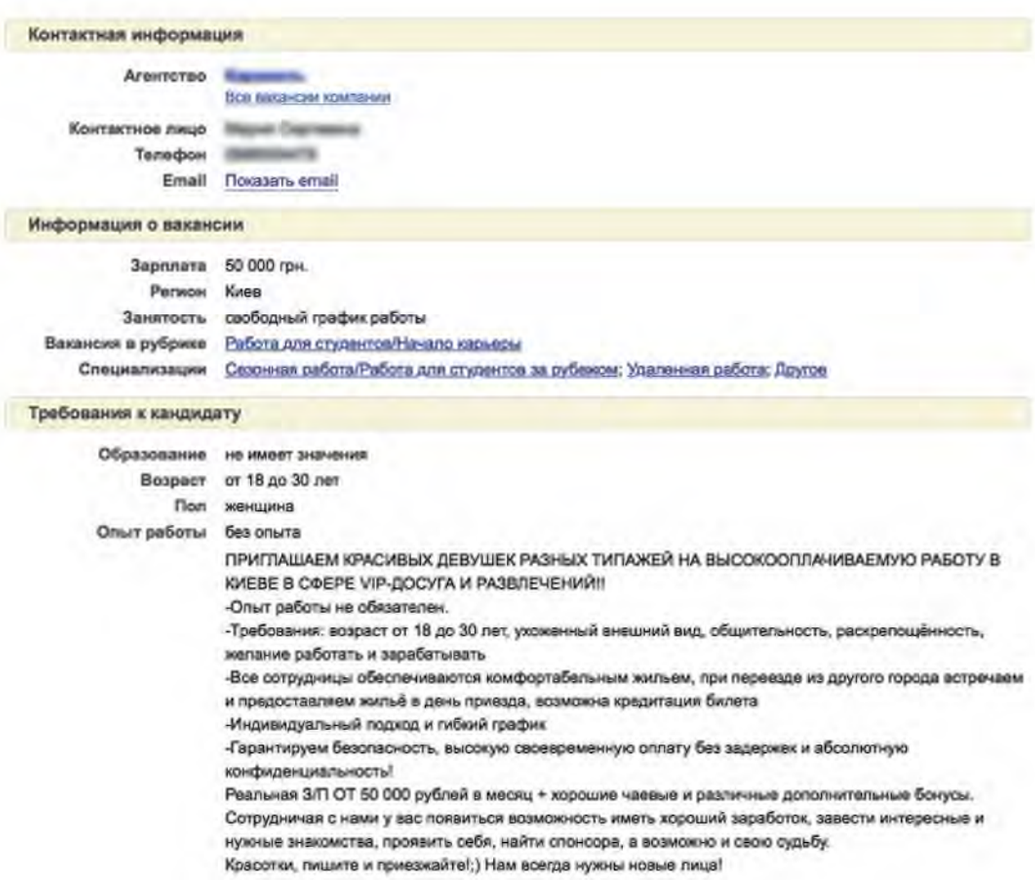
ДЛЯ ВЕРБУВАННЯ ЖІНОК ДВІ ОСОБИ РОЗМІСТИЛИ В МЕРЕЖІ ІНТЕРНЕТ НА САЙТАХ З ПРОПОЗИЦІЯМИ ПРАЦЕВЛАШТУВАННЯ РЕКЛАМНЕ ОГОЛОШЕННЯ, ЗАГАЛЬНИЙ ЗМІСТ ЯКОГО ЗВОДИВСЯ ДО ТОГО, ЩО АГЕНТСТВО ПО ПРАЦЕВЛАШТУВАННЮ ОГОЛОШУЄ НАБІР МОЛОДИХ ЖІНОК ПРИВАБЛИВОЇ ЗОВНІШНОСТІ НА ВИСОКООПЛАЧУВАНУ РОБОТУ В КРАЇНАХ ЄВРОПИ. ФОРМА ТА ЗМІСТ ОГОЛОШЕННЯ НЕ ЗАЛИШАВ СУМНІВІВ, ЩО РОБОТА ПОЛЯГАЄ НАДАННІ СЕКСУАЛЬНИХ ПОСЛУГ ЗА ГРОШОВУ ВИНАГОРОДУ. ДЛЯ КОНТАКТІВ У ОГОЛОШЕННІ БУВ РОЗМІЩЕНИЙ АБОНЕНТСЬКИЙ НОМЕР МОБІЛЬНОГО ТЕЛЕФОНУ, ЕЛЕКТРОННА АДРЕСА ТА НАЗВА САЙТУ, А ТАКОЖ КОНТАКТНА ОСОБА. КОЛИ НА ЗАЗНАЧЕНИЙ У ОГОЛОШЕННІ АБОНЕНТСЬКИЙ НОМЕР МОБІЛЬНОГО ТЕЛЕФОНУ НАДХОДИВ ДЗВІНОК, ЙОГО

ВЛАСНИЦЯ ПОЧИНАЛА ПРОВОДИТИ ВЕРБУВАННЯ ОСОБИ, ЯКА ТЕЛЕФОНУЄ. ВЕРБУВАЛЬНИЦЯ З ПЕРШОЇ РОЗМОВИ ВВОДИЛА ОСОБУ В ОМАНУ. СПЕРШУ СПІЛКУВАННЯ МІЖ ЗАЦІКАВЛЕНОЮ ЖІНКОЮ ВЕЛОСЯ ТІЛЬКИ ПО ТЕЛЕФОНУ. ПІСЛЯ ТОГО, ЯК ЗЛОЧИНЕЦЬ ПЕРЕКОНУВАЛАСЯ У БЕЗПЕЦІ ВЕРБУВАННЯ ЖІНКИ, ВОНА ПРИЗНАЧАЛА ЇЙ ЗУСТРІЧ. НА ЗУСТРІЧ ВЕРБУВАЛЬНИЦЯ ПРИХОДИЛА ЗІ СПІВУЧАСНИКОМ І, ПО ВІДПРАЦЬОВАНІЙ МІЖ НИМИ СХЕМІ, ДОПОВНЮЮЧИ ОДИН ОДНОГО ПОЧИНАЛИ ПОСТУПОВО ЗДІЙСНЮВАТИ ПСИХОЛОГІЧНИЙ ТИСК НА ПОТЕРПІЛУ, З МЕТОЮ СХИЛИТИ ЇЇ ПОЇХАТИ НА ЇХ УМОВАХ ЗА КОРДОН ДЛЯ РОБОТИ ПО НАДАННЮ СЕКСУАЛЬНИХ ПОСЛУГ ЗА ГРОШОВУ ВИНАГОРОДУ.

ПОГОДЖУЮЧИСЬ НА УМОВИ ВЕРБУВАЛЬНИЦЬ ЖІНКИ ВІДРАЗУ ПОТРАПЛЯЛИ ДО НИХ У БОРГОВУ КАБАЛУ, ОСКІЛЬКИ ПОГОДЖУВАЛИСЬ ЇХАТИ ЗА КОРДОН САМЕ НА ТИХ УМОВАХ ТА ЗА ТУ СУМУ ОПЛАТИ СВОЇХ ПОСЛУГ, ЯКІ ЇМ ПРОПОНУВАЛИСЬ В УКРАЇНІ. ЗАГАЛОМ ВСЯ СИСТЕМА СЕКСУАЛЬНОЇ ЕКСПЛУАТАЦІЇ УКРАЇНСЬКИХ МОЛОДИХ ЖІНОК ЗА КОРДОНОМ БУЛА НАЛАГОДЖЕНА ТАКИМ ЧИНОМ, ЩО ПОТЕРПІЛА, НАДАЮЧИ СЕКСУАЛЬНІ ПОСЛУГИ, НЕ МОГЛА ЗАРОБИТИ СОБІ ГРОШОВИХ КОШТІВ, ОСКІЛЬКИ ВЕСЬ ЗАРОБІТОК ПРИВЛАСНЮВАЛИ ЗЛОВМИСНИМИ.

ОБОХ СПІВУЧАСНИКІВ ЗЛОЧИНУ БУЛО ВИЗНАНО ВИННИМИ У ВЧИНЕНІ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО Ч. 2 СТ. 149 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ТА ПРИЗНАЧЕНО ЇМ ПОКАРАННЯ ЗА ЦІЄЮ СТАТТЕЮ ІЗ ЗАСТОСУВАННЯМ СТ. 69 КК УКРАЇНИ У ВИГЛЯДІ П'ЯТИ РОКІВ ПОЗБАВЛЕННЯ ВОЛІ БЕЗ КОНФІСКАЦІЇ МАЙНА [53, С. 172-174].

Документування фактів вербування жертв торгівлі людьми необхідно розпочинати із детального огляду оголошення (рис. 45) та фіксування його за допомогою процесуальних дій. Контактні дані, вказані в оголошенні слід використати для ідентифікації особи, яка його подала. Для цього достатньо скористатися методами пошуку в мережі Інтернет, описаними вище. Як правило, одна й та ж особа розміщує оголошення на різних ресурсах, що дозволяє зібрати максимальну кількість інформації про неї.



**Контактная информация**

Агентство [redacted]
Все вакансии компании

Контактное лицо [redacted]
Телефон [redacted]
Email Показать email

**Информация о вакансии**

Зарплата 50 000 грн.
Регион Киев
Занятость свободный график работы
Вакансия в рубрике Работа для студентов/Начало карьеры
Специализации Сезонная работа/Работа для студентов за рубежом; Удаленная работа; Другое

**Требования к кандидату**

Образование не имеет значения
Возраст от 18 до 30 лет
Пол женщина
Опыт работы без опыта

ПРИГЛАШАЕМ КРАСИВЫХ ДЕВУШЕК РАЗНЫХ ТИПАЖЕЙ НА ВЫСОКООПЛАЧИВАЕМУЮ РАБОТУ В КИЕВЕ В СФЕРЕ VIP-ДОСУГА И РАЗВЛЕЧЕНИЙ!!
-Опыт работы не обязателен.
-Требования: возраст от 18 до 30 лет, ухоженный внешний вид, общительность, раскрепощённость, желание работать и зарабатывать
-Все сотрудницы обеспечиваются комфортабельным жильем, при переезде из другого города встречаем и предоставляем жильё в день приезда, возможна кредитация билета
-Индивидуальный подход и гибкий график
-Гарантируем безопасность, высокую своевременную оплату без задержек и абсолютную конфиденциальность!
Реальная З/П ОТ 50 000 рублей в месяц + хорошие чаевые и различные дополнительные бонусы.
Сотрудничая с нами у вас появиться возможность иметь хороший заработок, завести интересные и нужные знакомства, проявить себя, найти спонсора, а возможно и свою судьбу.
Красотки, пишите и приезжайте!;) Нам всегда нужны новые лица!

*Рис. 45. Типове оголошення про набір дівчат до ескортного агентства*

Зібрану інформацію (номера мобільних телефонів, адреси електронної пошти) також можна використати для проведення слідчих та негласних слідчих (розшукових) дій, передбачених Кримінальним процесуальним кодексом України.

ПІД ЧАС ФІКСУВАННЯ ФАКТУ РОЗМІЩЕННЯ ОГОЛОШЕННЯ В МЕРЕЖІ ІНТЕРНЕТ ДОЦІЛЬНО ЗАЛУЧИТИ СПЕЦІАЛІСТА (НАПРИКЛАД, ПРАЦІВНИКА НАУКОВО-ДОСЛІДНОГО ЕКСПЕРТНО-КРИМІНАЛІСТИЧНОГО ЦЕНТРУ) ТА ЗА НЕОБХІДНІСТЮ ЗДІЙСНЮВАТИ ВІДПОВІДНУ ФОТО-, ВІДЕОФІКСАЦІЮ. ЗА РЕЗУЛЬТАТАМИ ОГЛЯДУ СТОРІНКИ ІЗ ЗАЛУЧЕННЯМ СПЕЦІАЛІСТА НЕОБХІДНО СКЛАСТИ ВІДПОВІДНИЙ АКТ. ПРОТЯГОМ ДОКУМЕНТУВАННЯ НЕОБХІДНО ЗВЕРНУТИ ОСОБЛИВУ УВАГУ НА ЧАС РОЗМІЩЕННЯ ПОВІДОМЛЕННЯ, ЙОГО МОВУ ТА СТИЛЬ НАПИСАННЯ. ТАКА ІНФОРМАЦІЯ МОЖЕ ДОПОМОГТИ ВСТАНОВИТИ ЯК ПРИБЛИЗНИЙ ЧАС ПОЧАТКУ ЗДІЙСНЕННЯ ПРАВОПОРУШЕННЯ, ТАК І МІСЦЕ РОЗТАШУВАННЯ АВТОРА ПОВІДОМЛЕННЯ.

З огляду застосування технологій, документування фактів вербування через дошки оголошень, аналогічне до веб-сайтів. Необхідно пам'ятати, що кожна дошка оголошень має адміністратора (модератора) – особу яка забезпечує технічне обслуговування сайту, а також слідкує (керує) за його наповненням.

Виходячи з цього, спершу необхідно встановити контактні дані такої особи. Це можна зробити за допомогою вже описаного вище сервісу ідентифікації власників мережних вузлів – «Whois» (рис. 46).

Domain Name:JOOBLE.ORG
Domain ID: D159423476-LROR
Creation Date: 2010-06-15T08:48:55Z
Updated Date: 2013-03-23T16:17:37Z
Registry Expiry Date: 2016-06-15T08:48:55Z
Sponsoring Registrar:GoDaddy.com, LLC (R91-LROR)
Sponsoring Registrar IANA ID: 146
WHOIS Server:
Referral URL:
Domain Status: clientDeleteProhibited -- http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited -- http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited -- http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited -- http://www.icann.org/epp#clientUpdateProhibited
Registrant ID:CR90452992
Registrant Name:Ievgen Sobakarov
Registrant Organization:Vertical Search Limited
Registrant Street: Geneva Place, Waterfront Drive
Registrant City:Road Town
Registrant State/Province:Tortola
Registrant Postal Code:VG1110
Registrant Country:VG
Registrant Phone:+44.2032392317
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:jcls.domain@gmail.com

*Рис. 46. Дані сервісу Whois*

Зауважимо, що під час отримання інформації через сервіси ідентифікації власників мережних вузлів (сайтів) доцільно користуватися різними сайтами, оскільки одні з них можуть не повністю показувати інформацію, вказану при реєстрації. Крім цього, в багатьох випадках, особа, яка реєструє доменне ім'я може приховати його за налаштуваннями конфіденційності, тоді потрібно надсилати запити на адресу компаній, які зареєстрували доменне ім'я. Інформацію про більшість доменних імен у зоні «.ua» доцільно отримувати через сервіс https://hostmaster.ua.

Однак, зазвичай контактні дані адміністрації дошки оголошень можна отримати на самому сайті у меню «Контакти», або через форум зворотного зв'язку.

ВИРОКОМ АПЕЛЯЦІЙНОГО СУДУ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ ВІД 29.06.2017 ЗАСУДЖЕНО ДО 5 РОКІВ ПОЗБАВЛЕННЯ ВОЛІ БЕЗ КОНФІСКАЦІЇ МАЙНА ЗА Ч. 2 СТ. 149 КК УКРАЇНИ ОСОБУ, ЯКА РОЗМІСТИЛА НА САЙТІ «HTTP///WWW.JOBEXPERT.COM.UA» ОБ'ЯВУ ЩОДО ПРАЦЕВЛАШТУВАННЯ МОЛОДИХ ОСІБ ЖІНОЧОЇ СТАТІ НА ВИСОКООПЛАЧУВАНУ РОБОТУ ІЗ ЗАРОБІТНОЮ ПЛАТОЮ В СУМІ 1000$ США У СФЕРІ ОБСЛУГОВУВАННЯ БЕЗ НАДАННЯ ІНТИМНИХ ПОСЛУГ, ОДНАК В ПОДАЛЬШОМУ, ЗАСТОСОВУЮЧИ ДО ПОТЕРПІЛИХ ПСИХОЛОГІЧНИЙ ВПЛИВ НА ҐРУНТІ ЇХ МАТЕРІАЛЬНИХ ПРОБЛЕМ ЧЕРЕЗ ВІДСУТНІСТЬ РОБОТИ ТА ЗБІГ ТЯЖКИХ СІМЕЙНИХ ОБСТАВИН, ПРОПОНУВАЛА ЇМ ПРАЦЕВЛАШТУВАТИСЯ В ЯКОСТІ ПОВІЙ ДЛЯ НАДАННЯ ІНТИМНИХ ПОСЛУГ НА ТЕРИТОРІЇ М. САНКТ-ПЕТЕРБУРГ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ.

Модератори та системні адміністратори здебільшого активно співпрацюють із правоохоронними органами та надають інформацію щодо особи, яка опублікувала оголошення. Вона складається із анкетних даних особи (можуть бути вигаданими), контактів (адреси електронної пошти та інколи телефону), способу оплати (коли це передбачено сайтом), та, звичайно, переліком IP-адрес, що використовувалися під час подачі чи редагування оголошення. Ця інформація, звичайно, є найціннішою, оскільки може допомогти ідентифікувати правопорушника.

СЛІД МАТИ НА УВАЗІ, ЩО ІНКОЛИ ЗЛОЧИНЦІ НЕ РОЗМІЩУЮТЬ ОГОЛОШЕННЯ НА ДОШКАХ ВЛАСНОРУЧНО, А КОРИСТУЮТЬСЯ СТОРОННІМИ СЕРВІСАМИ, ЯКІ НАДАЮТЬ ТАКІ ПОСЛУГИ. ТОДІ ЗАМОВНИКА ПОСЛУГИ ТРЕБА ШУКАТИ ЧЕРЕЗ ВКАЗАНІ СЕРВІСИ.

**МОДУЛЬ 4**

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ КОНТРОЛЮ ТА ЕКСПЛУАТАЦІЇ ЖЕРТВ

## 1. ОНЛАЙН-ПОРНОСТУДІЇ

Здешевлення високошвидкісного Інтернету, певна складність виявлення та документування потокового відео працівниками правоохоронних органів, законодавча невизначеність його статусу сприяли тому, що у світі набуло поширення таке явище як онлайн-порностудії. Типова порностудія розташовується на зйомній квартирі або вдома у кожної з працівниць (працівника), яку обладнують спеціальним устаткуванням (комп'ютери, модеми, вебкамери, мікрофони тощо) із підключенням до високошвидкісного Інтернету. Разом з тим варто відмітити, що останнім часом спостерігається тенденція щодо відмови організаторів порностудій від зйомних квартир, оскільки це в декілька разів підвищує ймовірність виявлення її

правоохоронцями. Крім цього, концентрація декількох моделей в одному місті передбачає більш активну участь організатора у забезпеченні роботи студії, а як наслідок документування його причетності до вказаної протиправної діяльності є набагато простішим. Організація ж роботи моделей за принципом «соціальних мереж» – надання лише майданчику для реєстрації, пошуку клієнтів та трансляції відео значно «відмежовує» організатора від злочину, адже він не спілкується безпосередньо із моделями, не поставляє їм комп'ютерну техніку, а отже й довести його вину набагато важче.

У якості працівниць (працівників) залучають, як правило, осіб віком 18-30 років, які за плату виконують бажання клієнтів інтимного характеру в онлайн-режимі. Для передачі інформації використовується потокове відео. Сайти із пропозицією таких послуг здебільшого розташовуються на іноземних серверах та орієнтовані на мешканців США та Західної Європи. Оплата здійснюється через банківські картки або електронні гроші. Працівники порностудії спілкуються з клієнтами англійською мовою. Доступ до відповідних ресурсів з вітчизняних IP-адрес блокується. Тому для пошуку таких ресурсів можна користуватися проксі- або VPN-серверами (див., наприклад, proxy4free.com).

Організатори порностудій можуть вводити в оману жертв, повідомляючи їм, що за вказану діяльність не передбачено відповідальність згідно з українським законодавством. Проте такі дії кваліфікуються як злочин, передбачений ст. 301 Кримінального кодексу України. Дії організаторів порностудій кваліфікуються за ст. 302 Кримінального кодексу України.

Сайт, на якому розташовують порностудію, складається з публічної та приватної частини. У публічній частині клієнт обирає особу для контакту, у приватній вони вже «спілкуються». Для доступу до приватної частини («Private chat») клієнт сплачує певні кошти. Приватні зустрічі можуть записуватися та у наступному розповсюджуватися як порнографічні відео-ролики.

Виявлення роботи онлайн-порностудій може бути здійснено працівником правоохоронних органів або третьою особою, яка у подальшому може виступати в якості заявника.

Документування доцільно розпочати (у випадку відсутності інформації, отриманої в передбаченому законом порядку, щодо діяльності певної студії) із моніторингу соціальних мереж та дощок оголошень про набір моделей для такої роботи. Оголошення можуть бути наступного змісту «работа для красивых девушек в офисе», «работа для моделей в сфере онлайн бизнеса», «набір дівчат для спілкування в чатах», «дівчата модельної зовнішності, робота в сфері інтернет-розваг», «робота за кордоном для файних дівчат», «набір дівчат у групу аніматорів для роботи в Туреччині із приємною зовнішністю, досвід роботи не обов'язковий» тощо.

Для здійснення ефективної протидії роботі онлайн-порностудій потрібні спільні, узгоджені дії підрозділів кіберполіції, підрозділів боротьби зі злочинами, пов'язаними із торгівлею людьми та прокуратури, адже найчастіше первинну інформацію про вчинений злочин отримують оперативні працівники, а слідчий здійснює досудове розслідування під процесуальним керівництвом прокурора. При цьому останній, підтримуючи в подальшому державне обвинувачення, може на попередній стадії орієнтувати та скеровувати слідчого та оперативного працівника на збір саме тих відомостей, які будуть використані в судовому засіданні як докази.

Загальний порядок документування роботи порностудій передбачає:

1) отримання інформації, чи надходження повідомлення про функціонування порностудії, реєстрація відомостей у Єдиному реєстрі досудових розслідувань;

2) ідентифікацію моделей – проводиться шляхом візуального пошуку на веб-сайті із трансляції порнографічного відео;

3) фіксацію факту розповсюдження продукції порнографічного характеру – проводиться шляхом огляду веб-сайту із фіксацією відео-чату зі сценами сексуального характеру. Рекомендовано проводити за участю експерта чи спеціаліста;

4) встановлення методів оплати та отримання коштів організаторами злочинного бізнесу та моделями;

5) встановлення місця розташування порностудії – здійснюється комплексом слідчих (розшукових) заходів, передбачених Кримінальним процесуальним кодексом України;

6) реалізація матеріалів кримінального провадження – проведення санкціонованих обшуків, тимчасового доступу до речей і документів, експертиз, допит фігурантів;

7) подальші слідчі дії.

З метою встановлення та фіксації відповідної злочинної діяльності в режимі реального часу доречним буде проведення уповноваженими підрозділами такої негласної слідчої (розшукової) дії як контроль за вчиненням злочину у формі спеціального слідчого експерименту.

Особливо актуальне значення проведення спеціального слідчого експерименту має для викриття діяльності різного виду порностудій, квартир, готельних номерів, інших приміщень, що використовуються для сексуальної експлуатації та працюють у режимі «он-лайн» (реального часу).

Під час цієї негласної слідчої (розшукової) дії уповноважені оперативні підрозділи з метою перевірки дійсних злочинних намірів певних осіб, використовуючи Інтерент-сайти, Skype та інші Інтернет-ресурси, під виглядом придбання відповідної відеопродукції або інших форм її споживання створюють або беруть участь у створенні обстановки, максимально наближеної до реальної, що дає можливість спостерігати за поведінкою, діями та рішеннями осіб, які організують та вчиняють злочини. При цьому звуки та зображення таких дій, інших обставини того, що відбувається у вказаних приміщеннях в режимі реального часу, фіксуються на компакт-диски, інші електронні носії інформації з метою подальшого використання отриманої в результаті спеціального слідчого експерименту інформації для доказування у кримінальному провадженні.

У разі необхідності документальної фіксації вищевказаних дій доцільним є також здійснення одночасно із спеціальним слідчим експериментом таких негласних слідчих (розшукових) дій як аудіо-, відеоконтроль особи та аудіо-, відеоконтроль місця.

Зазначені матеріали звуко- та відеозапису, на яких зберігається інформація про вчинені злочини, згідно з положеннями ст. 99 КПК України належать до такого процесуального джерела доказів як «Документи». Останні використовуються для доказування виключно за рішенням прокурора, що здійснює процесуальне керівництво досудовим розслідуванням у кримінальному провадженні.

У 2013 РОЦІ У М. ХАРКОВІ БУЛО ВИКРИТО ОНАЛЙН-ПОРНОСТУДІЮ. ПІДСТАВОЮ ДЛЯ ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ СТАЛА ЗАЯВА ОСОБИ, ЯКІЙ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ БУЛО ЗАПРОПОНОВАНО СПІЛКУВАННЯ У ПРИВАТНОМУ ЧАТІ. ЗАЯВНИК ПОГОДИВСЯ НА ПРОПОЗИЦІЮ ПІСЛЯ ЧОГО ПРОТЯГОМ 02 ХВИЛИН 39 СЕКУНД ПРАЦІВНИЦЯ ПОРНОСТУДІЇ, ЗА СПЛАЧЕНУ ЗАЯВНИКОМ ІЗ ВИКОРИСТАННЯМ СИСТЕМИ ІНТЕРНЕТ-БАНКІНГУ ВИНАГОРОДУ В РОЗМІРІ 40 ДОЛАРІВ США, ВИГОТОВЛЯЛА ТА РОЗПОВСЮДЖУВАЛА ОСТАННЬОМУ ВІДЕОЗОБРАЖЕННЯ, ЯКЕ ВИВОДИЛОСЯ НА МОНІТОР ЙОГО ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА, ПІД ЧАС ЯКОГО ЗНАХОДЯЧИСЬ ПЕРЕД ВЕБ-КАМЕРОЮ ПРАЦІВНИЦЯ ПОРНОСТУДІЇ ОГОЛИЛАСЯ, КРУПНИМ ПЛАНОМ ДЕМОНСТРУВАЛА СВОЇ СТАТЕВІ ОРГАНИ ТА ЗДІЙСНЮВАЛА МАСТУРБАЦІЙНІ ДІЇ.

У СВОЮ ЧЕРГУ ЗАЯВНИК ВКАЗАНЕ ЗОБРАЖЕННЯ ЗАПИСАВ НА КОМПАКТ-ДИСК ДЛЯ ЛАЗЕРНИХ СИСТЕМ ЗЧИТУВАННЯ, ЯКИЙ 15.11.2013 ДОБРОВІЛЬНО ВИДАВ ПРАЦІВНИКАМ МІЛІЦІЇ.

У ПОДАЛЬШОМУ ПРАЦІВНИКАМИ МІЛІЦІЇ БУЛО ЗДІЙСНЕНО ДВІ ОПЕРАТИВНІ ЗАКУПІВЛІ У ПРИМІЩЕННІ УПРАВЛІННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ГУМВС УКРАЇНИ В ХАРКІВСЬКІЙ ОБЛАСТІ НА 19,99 І 10 ДОЛАРІВ США ТА ЗАПИСАНО ВІДПОВІДНІ ДІЇ ПРАЦІВНИЦІ ПОРНОСТУДІЇ НА КОМПАКТ-ДИСКИ. ОПЕРАТИВНІ ЗАКУПІВЛІ ПРОВОДИЛИСЬ: 1) ЧЕРЕЗ САЙТ ТА 2) З ВИКОРИСТАННЯМ SKYPE.

У ПОДАЛЬШОМУ ВКАЗАНІ ДИСКИ БУЛО ПЕРЕДАНО ЕКСПЕРТУ ДЛЯ ПРОВЕДЕННЯ СУДОВО-МИСТЕЦТВОЗНАВЧОЇ ЕКСПЕРТИЗИ, ВИСНОВКАМИ ЯКОЇ БУЛО ВИЗНАНО РОЗМІЩЕНУ НА ДИСКАХ ПРОДУКЦІЮ ПОРНОГРАФІЧНОЮ [54].

Варто відмітити, що не завжди жертви добровільно беруть участь у роботі порностудій. В окремих випадках їх змушують до цього, застосовуючи психологічний або фізичний тиск, із наступним розповсюдженням графічної продукції в Інтернет. Тому викриття та припинення роботи вказаних об'єктів є дієвим інструментом протидії торгівлі людьми.

У 2009 РОЦІ УЧАСНИКИ ОРГАНІЗОВАНОЇ ЗЛОЧИННОЇ ГРУПИ ВИВЕЗЛИ ДО ПОЛЬЩІ ДЕКІЛЬКОХ ЖІНОК, ЯКИХ ПРИМУШУВАЛИ ПРАЦЮВАТИ У ПОРНОСТУДІЇ, ВСТАНОВИВШИ 12 ГОДИННИЙ РОБОЧИЙ ДЕНЬ З ДВОМА-ТРЬОМА ПЕРЕРВАМИ ПО 10-15 ХВИЛИН БЕЗ ВИХІДНИХ.

У РАМКАХ РОЗСЛІДУВАННЯ ЦІЄЇ СПРАВИ ПРАЦІВНИКАМИ УПРАВЛІННЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ У ВОЛИНСЬКІЙ ОБЛАСТІ ЗДІЙСНЮВАЛИСЯ ЗАХОДИ ПО ЗНЯТТЮ ІНФОРМАЦІЇ З КАНАЛУ ЗВ'ЯЗКУ ЗА IP-АДРЕСОЮ МЕРЕЖІ ІНТЕРНЕТ, В РЕЗУЛЬТАТІ ЯКИХ НА ДИСК ЗАФІКСОВАНО ЗОБРАЖЕННЯ ОСОБИ, КОТРА В РЕЖИМІ «ОН-ЛАЙН» (РЕАЛЬНОГО ЧАСУ), В ХОДІ СПІЛКУВАННЯ ДЕМОНСТРУВАЛА ВІДЕО-ШОУ ПОРНОГРАФІЧНОГО ХАРАКТЕРУ, ЩО ВИРАЗИЛОСЯ В ОГОЛЕННІ ТА ДЕМОНСТРАЦІЇ ПЕРЕД ВЕБ-КАМЕРОЮ ГРУДЕЙ, ГЕНІТАЛІЙ, А ТАКОЖ ЗДІЙСНЕННІ РУХІВ НАПРАВЛЕНИХ НА «МАСТУРБАЦІЮ». ЕКСПЕРТИЗА ПІДТВЕРДИЛА, ЩО ВКАЗАНІ ЗОБРАЖЕННЯ МАЛИ ОЗНАКИ ПОРНОГРАФІЇ.

ЗГОДОМ ОПЕРАТИВНИМИ ПРАЦІВНИКАМИ БУЛО ПРОВЕДЕНО ОПЕРАТИВНІ ЗАКУПІВЛІ ПОРНОГРАФІЧНОЇ ВІДЕОПРОДУКЦІЇ НА ІНТЕРНЕТ-САЙТІ. ОПЛАТА ПРОВОДИЛАСЬ ШЛЯХОМ ЗНЯТТЯ КОШТІВ З ТЕЛЕФОНУ. ФІКСАЦІЯ ЗАХОДУ ЗДІЙСНЮВАЛАСЬ ЗА ДОПОМОГОЮ ВІДЕОКАМЕРИ НА ВІДЕОКАСЕТУ, А ТАКОЖ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНОЇ ПРОГРАМИ «EATCAM WEB RECORDER PRO», КОТРА ДАЄ МОЖЛИВІСТЬ ФІКСУВАТИ ЗОБРАЖЕННЯ НА ЖОРСТКИЙ ДИСК НОУТБУКА ЧИ КОМП'ЮТЕРА. ЯК І У ПОПЕРЕДНЬОМУ ВИПАДКУ ДОКУМЕНТУВАТИ РОБОТУ ПОРНОСТУДІЇ ДОПОМАГАЛА СТОРОННЯ ОСОБА – ЗАЯВНИК, ЯКИЙ БЕЗ МЕТИ РОЗПОВСЮДЖЕННЯ, ЗАПИСАВ З ІНТЕРНЕТУ НА CD-ДИСК «ШОУ» З ПОРНОСТУДІЇ ЗА ДОПОМОГОЮ ПРОГРАМИ ВІДЕОЗАХОПЛЕННЯ, ТА В ПОДАЛЬШОМУ ПЕРЕДАВ ЙОГО ДО ПРАВООХОРОННИХ ОРГАНІВ.

У РЕЗУЛЬТАТІ ОРГАНІЗАТОРІВ ЦЬОГО ЗЛОЧИНУ БУЛО ЗАСУДЖЕНО ЯК ТОРГОВЦІВ ЛЮДЬМИ ЗА Ч. 3. СТ. 149 ТА Ч. 3. СТ. 301 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ДО ПОЗБАВЛЕННЯ ВОЛІ [55].

Наведені приклади розслідування злочинної діяльності щодо створення онлайн-порностудій не є поодинокими. Судова практика засвідчує, що з технічної точки зору під час документування їх роботи можна здійснювати:

- огляд веб-сайту;
- контроль за вчиненням злочину у формі оперативної закупівлі або спеціального слідчого експерименту із використанням апаратних та програмних засобів фіксації. З правової точки зору проведення спеціального слідчого експерименту є більш доцільним;
- тимчасовий доступ до речей і документів;
- зняття інформації з транспортних телекомунікаційних мереж;
- залучення носіїв із записами графічної продукції, створених заявником.

Під час документування роботи онлайн-порностудій для запису інформації з монітору доцільно використовувати безкоштовні програми фіксації, як от наведена EatCam Web Recorder Pro, яку можна завантажити з сайту www.eatcam.com.

Аналіз вироків, внесених до Єдиного державного реєстру судових рішень, свідчить про відсутність єдиної практики щодо кваліфікації за ст. 301 КК України дій «працівниць» порностудій.

Деякі суди виправдовують обвинувачених у виготовленні та розповсюдженні відеопродукції порнографічного характеру, наприклад Жовтневий районний суд м. Дніпропетровська у вироку від 01.03.2016 зазначив, що:

- «не може бути віднесені до предмета вказаного злочину інформація, яка не зафіксована на носіях, а передається мережами зв'язку, оскільки лише після її фіксації на матеріальних носіях (жорстких дисках комп'ютерів, оптичних дисках, картах пам'яті) вона набуває фізичної ознаки предмета злочину, передбаченого ст. 301 КК України;
- передача через канали зв'язку інформації, з використанням якої можна створити порнографічні предмети, не можна визнавати її розповсюдженням, оскільки злочинні дії передбачають операції з відповідними матеріальними об'єктами;
- стаття 301 КК України в її чинній редакції не охоплює надання доступу до порносайтів в електронних мережах, оскільки саме створення сайтів, зміст яких відображено на носіях цифрової інформації, охоплюється поняттям «виготовлення порнографічних предметів» [56].

Звертаємо увагу на те, що вищезазначений виправдувальний вирок винесений при тому, що обвинувачена визнавала свою вину.

Також, існує позиція згідно якої дії «працівниці» онлайн порностудій, які виконуючи інтимні побажання клієнтів імітують статеві акти є не створенням порнографічної відеопродукції, а наданням послуг сексуального характеру, за що передбачена адміністративна відповідальність.

Якщо коротко узагальнити вищезазначені аргументи, то на думку їх авторів зображення або інший предмет порнографічного характеру створюється лише в момент запису зображення на матеріальний носій. Натомість, в Єдиному державному реєстрі судових рішень викладено велику кількість обвинувальних вироків, якими, за аналогічних обставин, обвинувачених притягнуто до кримінальної відповідальності.

Обґрунтуванням такої позиції може бути те, що якщо певна інформація передається шляхом відеотрансляції через веб-камеру та оглядається споживачем продукції порнографічного характеру в режимі реального часу, то це може вказувати на відсутність передбаченої законом форми матеріального закріплення лише у звичайному її розумінні – на магнітній плівці чи магнітному диску, компакт-диску, переносному електронному носієві тощо.

Оскільки, все ж таки, на екран монітора споживача порнографічної послуги виводиться саме зображення, то, без будь-якого сумніву, фактично має місце форма його матеріальної фіксації в комп'ютерній мережі, в якій відбувається трансляція, хоча і на дуже незначний час. Втім, чинне законодавство не висуває вимог щодо обов'язкового проміжку часу збереження зображення, в т. ч. порнографічного характеру, на певному матеріальному носієві.

Тобто, не є принципово важливим, скільки зберігається малюнок, зарисовка з натури, натуралістична фотографія, кіно- або відеопродукція на магнітній плівці чи магнітному диску, компакт-диску, переносному електронному накопичувачеві тощо. Достатньо лише встановлення факту того, що зображення дійсно потрапило на цей матеріальний носій.

Те ж саме стосується і зображення, яке через веб-камеру одного комп'ютера транслюється на монітор іншого комп'ютера в системі загальної для них мережі. За час проходження через останню має місце запізнення сигнала, що обумовлюється не тільки законами фізики щодо швидкості його розповсюдження, а й тимчасовим збереженням зображення на серверах та у пам'яті електронних пристроїв для здійснення безперервного потоку інформації шляхом буферизації та створення тимчасових файлів.

Отже, наголосимо, що питання про проходження аудіосигнала порнографічного характеру потребує обережного та виваженого розв'язання. Пригадаємо, що відповідно до положень Закону України «Про захист суспільної моралі» від 20.11.03 р. № 1296-IV продукція порнографічного характеру в якості самостійного варіанта може мати і тільки аудіохарактеристики та передаватись крізь матеріальні носії (наприклад, слуховий апарат) [57].

## 2. МЕРЕЖНІ СХОВИЩА

### ХМАРНІ СХОВИЩА

Доступ до хмарних сховищ, як правило, забезпечується за допомогою веб-служб, які пропонують користувачам онлайнове сховище, базовий об'єм якого (5-10 Гб) надається безкоштовно, а додаткове місце – за окрему плату. Серед типових прикладів таких служб можна назвати «Dropbox», «Google Drive», «iCloud», «OneDrive», «MEGA.NZ» та багато інших.

Вони працюють аналогічно поштовим веб-провайдерам. Користувач налаштовує свій обліковий запис і має можливість доступу до нього і користування ним через Інтернет-з'єднання та веб-браузер. Дехто надає доступ через мобільні застосування і навіть пропонує доступ через соціальні мережі, такі як «Facebook», «Twitter» тощо.

Хмарні сховища можуть використовуватися торговцями людьми для зберігання, зміни, переміщення і розповсюдження будь-яких даних. Це цілком можуть бути персональні дані жертв, фотографії та навіть відеозображення.

Таке сховище може знаходитися практично будь-де у світі і залежить тільки від розташування комп'ютерного сервера, використовуваного для фізичного зберігання даних. Правопорушники можуть налаштувати контроль доступу до сховища і обмежити його або зашифрувати дані, щоб зробити доступ до них правоохоронних органів практично неможливим.

Доступ до серверів зберігання може здійснюватись через спеціальне програмне забезпечення. У контексті торгівлі людьми, вони є ідеальним середовищем для безпечного зберігання злочинних даних за межами юрисдикції або досяжності місцевих правоохоронних органів.

У ЛИПНІ 2015 РОКУ НА ГАРЯЧУ ЛІНІЮ HTTP://INTERNETBEZPEKA.ORG.UA [ , С. 102] НАДІЙШЛО ПОВІДОМЛЕННЯ ПРО РОЗМІЩЕННЯ У ХМАРНОМУ СХОВИЩІ ЗА АДРЕСОЮ HTTPS://CLOUD.MAIL.RU/PUBLIC/A503600F34BF/%D0%B2 ДИТЯЧОЇ ПОРНОГРАФІЇ. ЗА РЕЗУЛЬТАТАМИ ПРОВЕДЕНОГО АНАЛІЗУ БУЛО ВСТАНОВЛЕНО, ЩО У ДАНОМУ СХОВИЩІ ЗБЕРІГАЛОСЯ ДЕКІЛЬКА ГБ ФОТО- ТА ВІДЕОПРОДУКЦІЇ, ЯКА МІСТИТЬ ОЗНАКИ ДИТЯЧОЇ ПОРНОГРАФІЇ. НА ТЕПЕРІШНІЙ ЧАС РОБОТУ СХОВИЩА ПРИПИНЕНО ЗА ДОПОМОГОЮ АДМІНІСТРАТОРІВ РЕСУРСУ.

### PEER-TO-PEER

Peer-to-peer (P2P) – спосіб побудови комп'ютерної мережі, в основі якої стоїть мережа рівноправних вузлів. Такі мережі засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи можуть зв'язуватися безпосередньо між собою, на відміну від традиційної архітектури, де роботою мережі керує центральний вузол-сервер.

Для розповсюдження інформації за допомогою Peer-to-peer (P2P) мереж використовуються так звані трекери, що містять в собі лише загальну інформацію про відповідні файли та його роздавачів.

В зв'язку з тим, що однорангові (P2P, піринговi) мережі є зручним інструментом, за допомогою якого злочинці можуть здійснювати зберігання та обмін даними у різних формах, у тому числі відео та графічних файлів, наприклад, фотографій жертв злочину, персональних даних тощо, peer-to-peer-технології є одним із найпоширеніших інструментів, що застосовують торговці людьми.

Існують певні складнощі у доказуванні злочинного застосування веб-технологій, якщо особа використовує для розповсюдження протиправного контенту лише посилання на дані, розміщені на іншому, недосяжному для правоохоронців ресурсі. Проте як показує судова практика це не стає на заваді у притягненні особи до відповідальності, якщо усі докази зібрано належним чином.

У 2014 РОЦІ КІРОВСЬКИМ РАЙОННИМ СУДОМ М. КІРОВОГРАДА БУЛО ВИНЕСЕНО ОБВИНУВАЛЬНИЙ ВИРОК У СПРАВІ ПРО РОЗПОВСЮДЖЕННЯ ДИТЯЧОЇ ПОРНОГРАФІЇ. ПРИ ЦЬОМУ ЗАХИСНИК ЗВЕРТАВ УВАГУ СУДУ НА ТЕ, ЩО ПІДСУДНИЙ РОЗМІЩУВАВ НЕ САМІ ВІДЕОФАЙЛИ, А ЛИШЕ ПОСИЛАННЯ НА МІСЦЕ РОЗТАШУВАННЯ ВКАЗАНИХ ФАЙЛІВ. ОДНАК, СУД ДІЙШОВ ВИСНОВКУ, ЩО ПОНЯТТЯ ВІДЕОПРОДУКЦІЇ ПОРНОГРАФІЧНОГО ХАРАКТЕРУ ВКЛЮЧАЄ В СЕБЕ ГОТОВІ ПОВНОМЕТРАЖНІ, КОРОТКОМЕТРАЖНІ ВІДЕОФІЛЬМИ, НЕ ДО КІНЦЯ ЗМОНТОВАНІ ВІДЕОЗАПИСИ, ЯКІ МОЖНА ВІДТВОРИТИ ДЛЯ ПЕРЕГЛЯДУ ТА ЯКІ МАЮТЬ ПОРНОГРАФІЧНИЙ ХАРАКТЕР. В ДАНОМУ ВИПАДКУ МАЄ МІСЦЕ ГОТОВИЙ ВІДЕОЗАПИС І Є МОЖЛИВИМ ЙОГО ВІДТВОРЕННЯ. ТОЙ ФАКТ, ДЕ БЕЗПОСЕРЕДНЬО ЗНАХОДИТЬСЯ ДАНИЙ ВІДЕОЗАПИС ТА НА ЯКОМУ НОСІЇ, НЕ ВПЛИВАЄ НА НАЯВНІСТЬ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ ТА ЙОГО КВАЛІФІКАЦІЮ [59].

Корисною особливістю P2P-застосувань є те, що під час їх використання для вивантаження / завантаження певних даних відображається інформація про IP-адреси комп'ютерів, які беруть в цьому участь (рис. 47).

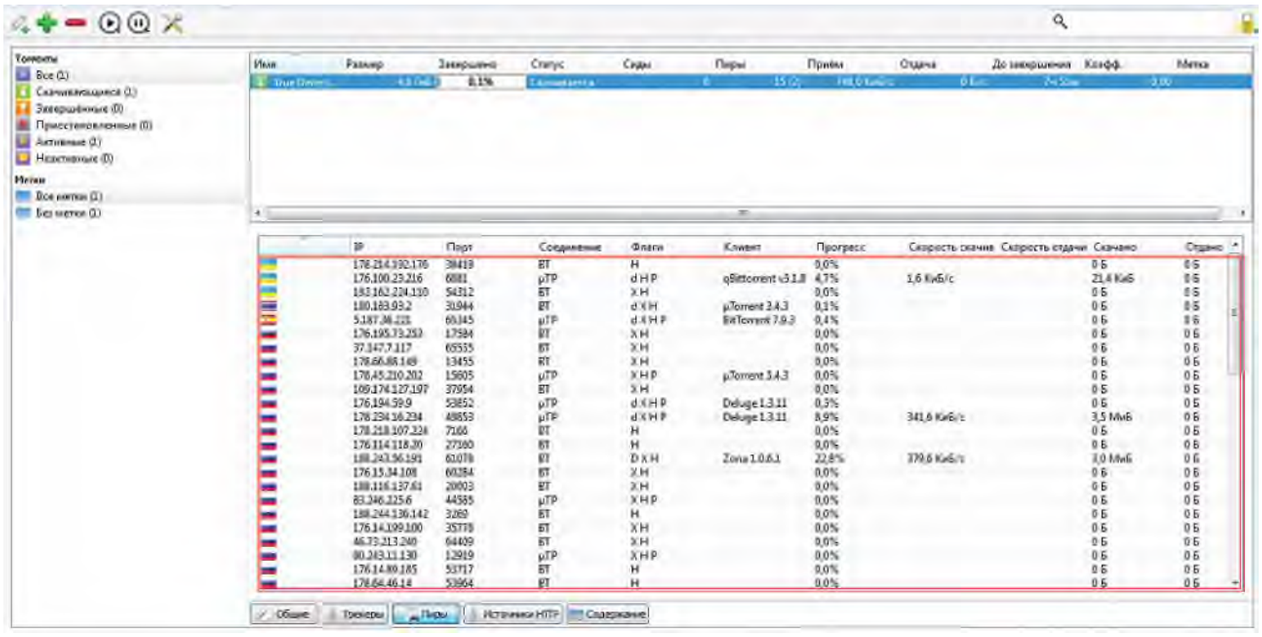


*Рис. 47. Завантаження файлу за допомогою P2P-застосування*

Вказані відомості можуть допомогти працівнику правоохоронних органів у визначенні кола правопорушників.

У 2012 РОЦІ В ЧЕРКАСЬКІЙ ОБЛАСТІ ОСОБА, ПРАГНУЧИ ШВИДКОГО ОСОБИСТОГО ЗБАГАЧЕННЯ, ШЛЯХОМ ЗБУТУ І РОЗПОВСЮДЖЕННЯ ПРОДУКЦІЇ ПОРНОГРАФІЧНОГО ЗМІСТУ, ЗАВАНТАЖИЛА З ФАЙЛООБМІННИКІВ НА ЖОРСТКИЙ ДИСК СВОГО КОМП'ЮТЕРА ФАЙЛИ, З ВІДЕО- ТА ФОТОПРОДУКЦІЄЮ ПОРНОГРАФІЧНОГО ЗМІСТУ. У ПОДАЛЬШОМУ ВЛАСНОРУЧ СТВОРЮВАЛА САЙТИ, А САМЕ: WEBCASUPER.DO.AM; SWEETWEBCAMS.MYL.RU; CAMS.MOY.SU. НА ЯКІ ЗАВАНТАЖИЛА З ЖОРСТКОГО ДИСКУ СВОГО КОМП'ЮТЕРА, ПОПЕРЕДНЬО ЗАВАНТАЖЕНІ НЕЮ ФАЙЛИ ПОРНОГРАФІЧНОГО ЗМІСТУ, У ТОМУ ЧИСЛІ ІЗ ДИТЯЧОЮ ПОРНОГРАФІЄЮ. ДЛЯ НАДХОДЖЕННЯ КОШТІВ, ОТРИМАНИХ ВНАСЛІДОК РОЗПОВСЮДЖЕННЯ ФАЙЛІВ З ВІДЕО ТА ФОТО ПРОДУКЦІЄЮ ПОРНОГРАФІЧНОГО ЗМІСТУ, ЗАРЕЄСТРУВАЛАСЬ В СИСТЕМІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ MONEY, ДЕ СТВОРИЛА ЕЛЕКТРОННИЙ РАХУНОК – ЗА НОМЕРОМ Z 103566255224. ЗА РЕЗУЛЬТАТАМИ СУДОВОГО РОЗГЛЯДУ ОСОБУ БУЛО ВИЗНАНО ВИННОЮ У ВЧИНЕННІ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТ. 301 Ч. 4 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ І ПРИЗНАЧЕНО ПОКАРАННЯ П'ЯТЬ РОКІВ ПОЗБАВЛЕННЯ ВОЛІ З КОНФІСКАЦІЄЮ ПОРНОГРАФІЧНОЇ ВІДЕОПРОДУКЦІЇ ТА МАТЕРІАЛЬНИХ НОСІЇВ КОМП'ЮТЕРНИХ ПРОГРАМ [60].

Поряд із звичайними P2P мережами існують їх закриті аналоги, які називають закритими P2P мережами (Private peer-to-peer). Такі мережі функціонують у рамках проекту DarkNet – приватної мережі, у якій використовуються свої протоколи з'єднань та шифрування збережуваної інформації. За своєю філософією мережа DarkNet є подібною до I2P-мережі. Найбільш популярними DarkNet є Freenet та RetroShare.

Вказані мережі орієнтовані на забезпечення анонімності, а тому є ідеальним середовищем для спілкування між особами, задіяними у торгівлі людьми. Водночас повільна передача інформації в таких мережах дозволяє говорити лише про їх обмежене застосування злочинним елементом.

За кордоном існують спеціально модифіковані для правоохоронних органів і захищені від несанкціонованого доступу P2P-клієнти, які приймають трансляції роздач з RSS-каналів P2P-мереж без участі в реальній передачі файлів (тобто вони отримують файли від інших пірів, але не поширюють самі). У результаті фіксуються IP-адреси пірів, які поширюють нелегальний контент.

**FTP**

**FTP (File Transfer Protocol)** – це протокол передачі даних. FTP працює за протоколом TCP, що зазвичай поставляється з операційною системою. Призначення протоколу – передача файлів між різними комп'ютерами, що працюють у мережах TCP/IP: на одному з комп'ютерів працює програма-сервер (FTP-сервер), на іншому – програма-клієнт (FTP-клієнт). Клієнтської програма надає можливість користувачеві з'єднатися з сервером і забезпечує передачу або отримання файли через FTP-протокол.

Одним із способів розміщення протиправного контенту, пов'язаного з торгівлею людьми, є використання саме FTP-серверів. На теперішній час FTP-сервери із протиправними матеріалами, як правило, розміщуються на територіях з недосконалим законодавством у сфері протидії торгівлі людьми. Доступ до таких ресурсів дозволяється «перевіреним користувачам», яких не підозрюють у зв'язках з правоохоронними органами. Для доступу користувачам надається зареєстровані на сервері ім'я та пароль. Користувачі, які користуються FTP, зазвичай, обізнані у сфері інформаційних технологій.

Користувачі, як правило, використовують FTP-клієнти, що вбудовані у браузери, при цьому стандартні браузерні клієнти дозволяють тільки завантажувати інформацію з серверів. Для запису інформації на FTP-сервери використовуються спеціальні плагіни для браузерів або стороннє програмне забезпечення.

Інколи правопорушники не встановлюють парольний захист на свої ресурси або використовують стандартні паролі. У такому випадку працівники правоохоронних органів мають змогу просканувати мережу на наявність доступних FTP-серверів та задокументувати протиправний контент.

У якості інструменту сканування можна запропонувати безкоштовну програму Network Scanner, яку можна завантажити за адресою http://lantricks.ru/download/. Для сканування мережі потрібно вказати відповідні діапазони IP-адрес та натиснути кнопку «Сканировать» (рис. 48). У програмі передбачено також пошук за ключовими словами.

Як видно з рисунку дана програма дозволяє також сканувати мережу на предмет наявності доступних ресурсів за іншими, окрім FTP, протоколами, зокрема NetBios та HTTP, тому цю програму корисно використовувати під час пошуку відкритих ресурсів у локальних (наприклад, міських) мережах на предмет наявності протиправного контенту.

Варто звернути увагу, що правопорушники можуть застосовувати компактні FTP-сервери під час несанкціонованого проникнення до комп'ютерних систем з метою вивантаження та завантаження файлів, які їх цікавлять.

За допомогою таких проникнень можуть бути скопійовані медіа-файли інтимного характеру. У майбутньому особи, які на них зображені, можуть шантажуватися аж до примушування їх до надання сексуальних послуг. Випадки подібного шантажу є особливо актуальними щодо дітей.

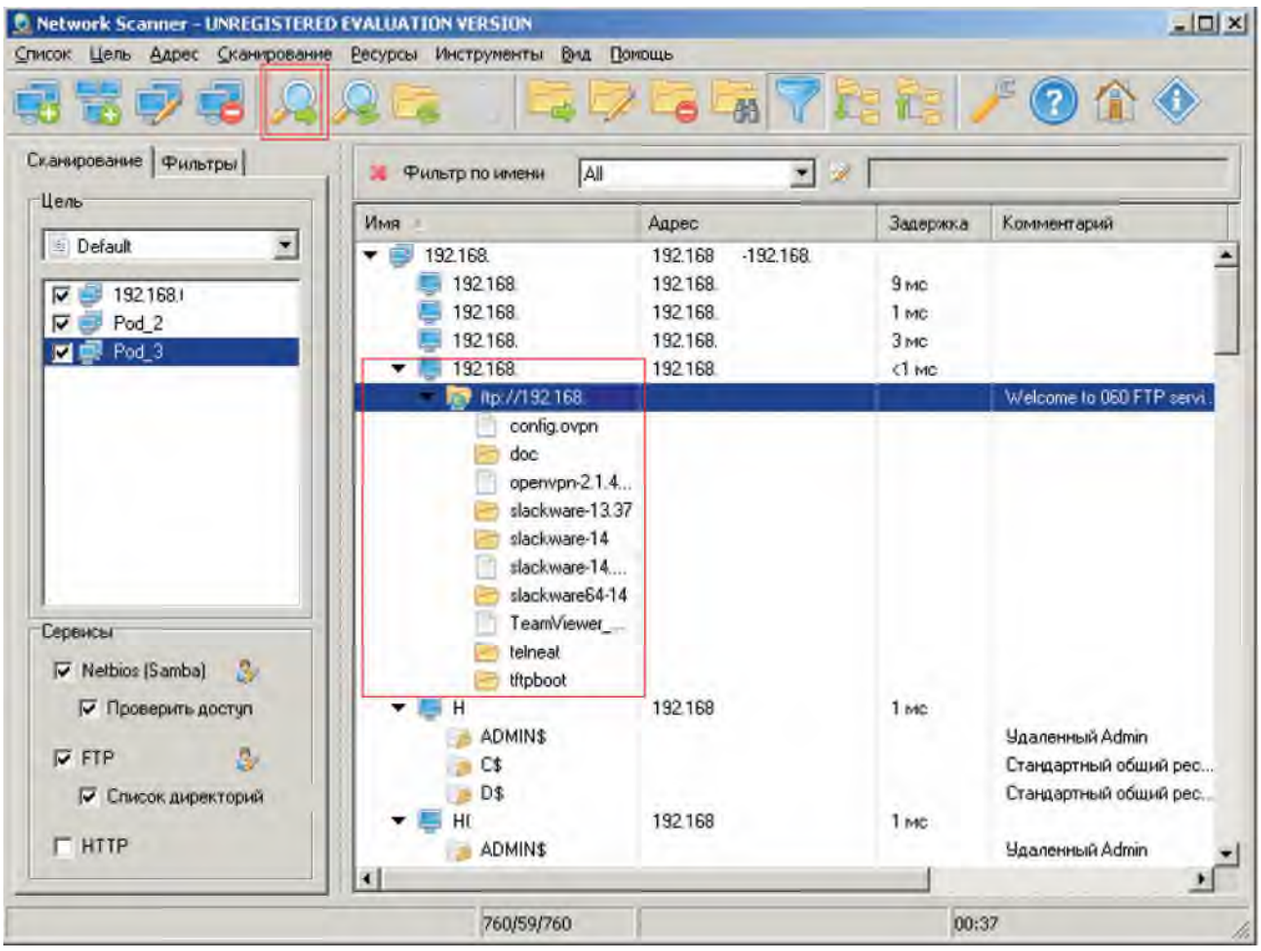



*Рис. 48. Результати сканування мережі*

### ВІДЕОХОСТИНГИ

Окрім наведених інструментів з метою розповсюдження відеоматеріалів, пов'язаних із торгівлею людьми, правопорушниками активно використовуються відохостинги – сайти, що дозволяють завантажувати і переглядати відео у браузері, наприклад через спеціальний програвач. При цьому більшість подібних сервісів не надають відео [61]. Прикладом відеохостингу є сервіси YouTube, Hulu.

Адміністратори популярних відеохостингів, як правило, прискіпливо відстежують протиправний контент, пов'язаний із торгівлею людьми, тому працівникам правоохоронних органів потрібно звертати особливу увагу на маловідомі сервіси цього типу.

Документування розміщення протиправних відеозаписів на означених ресурсах здійснюється подібно до документування роботи онлайн-порностудій шляхом огляду веб-сторінок відохостингу зі складанням відповідних актів (якщо можливості сервісу дозволяють, потрібно обов'язково вказати тривалість та кількість переглядів відеороліку), направленням одержаних матеріалів на експертне дослідження тощо.

## 3. ВЕБ-САЙТИ З НАДАННЯ ПОСЛУГ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ

Сайти, орієнтовані на вербування жертв торгівлі людьми, злочинці використовують і для їх експлуатації. Серед відповідних сайтів найбільш популярними у правопорушників є сторінки, спрямовані на:

- рекламування проституції (рис. 49) та «одруження»;
- пропозиції рабської робочої сили (як правило, безпосередньо на сайті не пропонуються, закамуфльовані під найм недорогої робочої сили);

- продаж органів (рис. 50);
- розповсюдження порнографічної продукції, у тому числі, дитячої порнографії (рис. 51).

СЛІД МАТИ НА УВАЗІ, ЩО У СХЕМАХ ТОРГІВЛІ ЛЮДЬМИ, ОСОБЛИВО З МЕТОЮ ЗАЛУЧЕННЯ ОСТАННІХ ДО ПРИМУСОВОЇ ПРАЦІ, МОЖУТЬ БУТИ ЗАЛУЧЕНІ ДІЮЧІ АБО КОЛИШНІ ПРИКОРДОННИКИ ТА ІНШІ ПРЕДСТАВНИКИ ОРГАНІВ ВЛАДИ. ТАК, НАПРИКЛАД, НАПРИКІНЦІ 2014 РОКУ НА ХАРКІВЩИНІ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ БУЛО ВИКРИТО ДІЯЛЬНІСТЬ ЗЛОЧИННОЇ ГРУПИ, ЯКА ОРГАНІЗУВАЛА КАНАЛ НЕЛЕГАЛЬНОЇ МІГРАЦІЇ ДО РОСІЇ ВИХІДЦІВ З КРАЇН СНД. ВСТАНОВЛЕНО, ЩО ВАТАЖОК ЗЛОЧИННОГО УГРУПОВАННЯ НЕОДНОРАЗОВО ОТРИМУВАВ З МОСКВИ ЗАМОВЛЕННЯ НА НЕЗАКОННЕ ПЕРЕПРАВЛЕННЯ НЕЛЕГАЛЬНИХ МІГРАНТІВ ДО РОСІЇ. ЗЛОВМИСНИКИ ОРГАНІЗОВУВАЛИ ПЕРЕТИН НЕЛЕГАЛАМИ ДЕРЖАВНОГО КОРДОНУ НА ТЕРИТОРІЮ БЄЛГОРОДСЬКОЇ ОБЛАСТІ РФ ПОЗА МЕЖАМИ ВСТАНОВЛЕНИХ ПУНКТІВ ПРОПУСКУ. У ПРОТИПРАВНІЙ ДІЯЛЬНОСТІ БРАВ УЧАСТЬ КОЛИШНІЙ ПРИКОРДОННИК, ЯКИЙ ЗАБЕЗПЕЧУВАВ НЕЛЕГАЛЬНИХ МІГРАНТІВ ПІДРОБЛЕНИМИ ДОКУМЕНТАМИ. «ПОСЛУГУ» З НЕЗАКОННОГО ПЕРЕПРАВЛЕННЯ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН ЗЛОВМИСНИКИ ОЦІНЮВАЛИ В СЕРЕДНЬОМУ ВІД 1,5 ДО 2 ТИСЯЧ ДОЛАРІВ США [62].

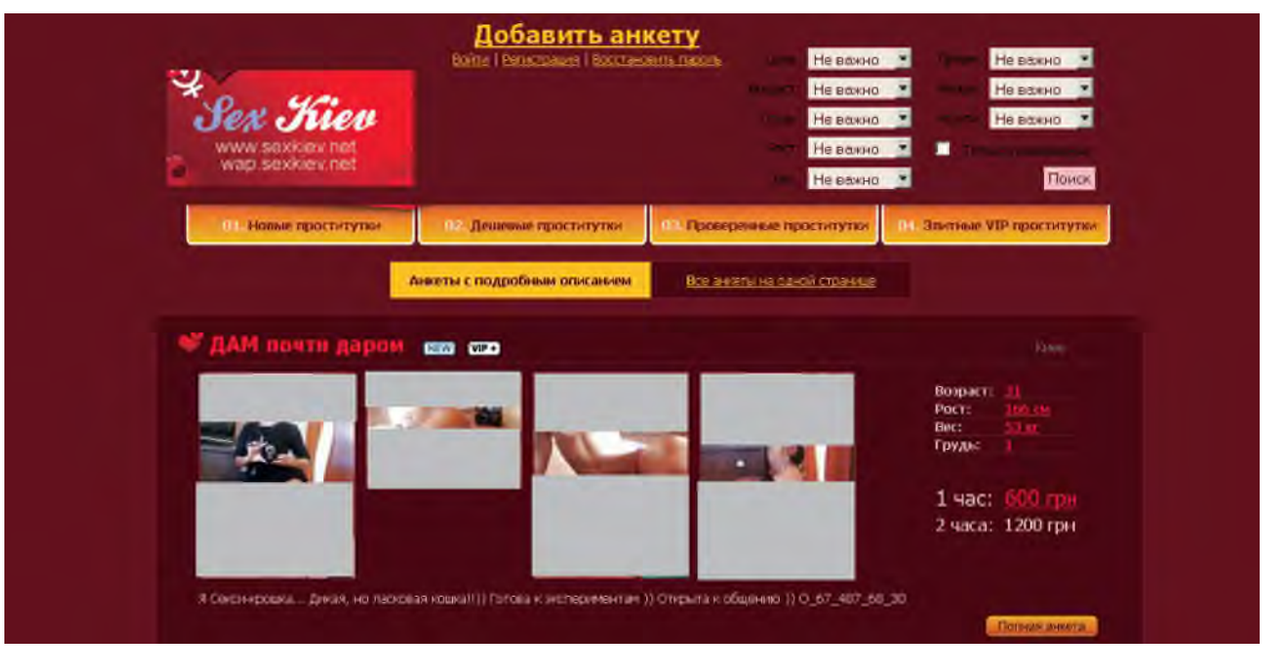



*Рис. 50. Сайт з рекламування проституції*


*Рис. 51. Сайт з рекламування продажу органів*

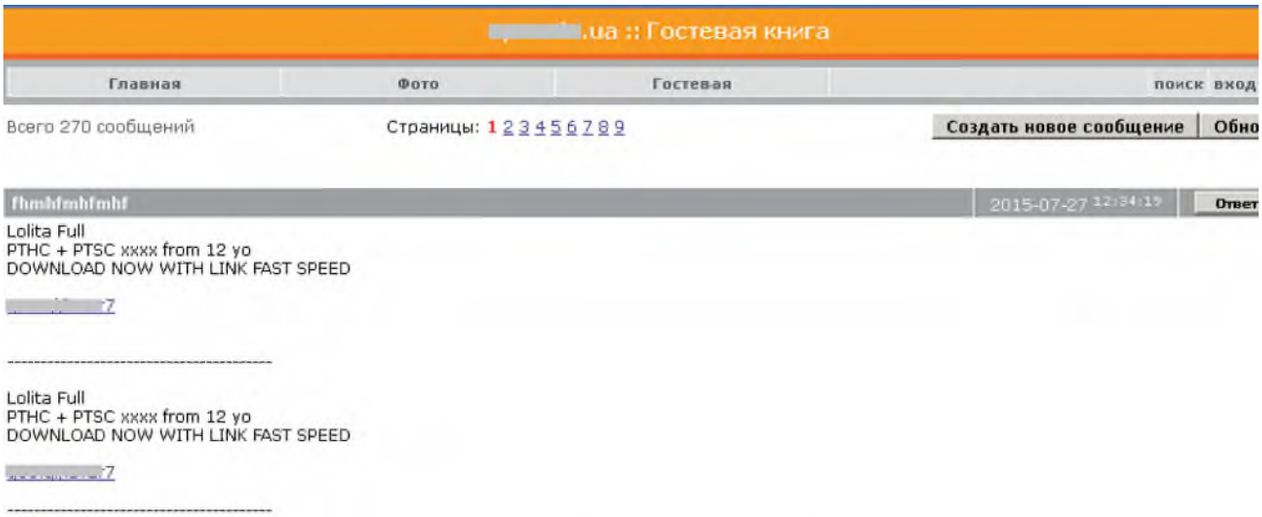



*Рис. 52. Сайт з дитячою порнографією*

Доступ до сайту із рекламування послуг повій, наприклад, надається після попереднього внесення абонентом плати. В такому випадку, анкета дівчини появляється на головній сторінці ресурсу. Оплата здебільшого здійснюється за допомогою платіжної системи Webmoney, однак інколи може застосовуватися не прямий спосіб переказу грошей, а через «погашення» ваучерів поповнення гаманця Webmoney. У такому випадку адміністратору ресурсу повідомляється код поповнення на певну суму і він відкриває доступ до анкети на сайті. Оскільки практично усі такі ресурси розміщуються на іноземних хостингових майданчиках, то документування слід розпочинати із «фінансової складової», тобто із способу оплати та подальшої легалізації коштів. Слід зазначити, що з метою конспірації, злочинці переказують гроші на 3-4 проміжних гаманця, а лише потім – на банківські карти, чи сервіси по легалізації. Є принципово важливим відслідкувати увесь ланцюг потоку коштів. Крім цього, доволі часто із інтернет-гаманців правопорушники оплачують проміжні послуги (оплату доменів, додаткового хостингу для резервних копій чи службових файлів, захисту від DDoS-атак тощо), саме по них досить часто можна ідентифікувати адміністратора ресурсу чи його співучасників.

У сайтах призначених для реклами послуг повій на території України доволі часто первинна реєстрація доменних імен відбувалася через українські компанії, що може бути додатковим джерелом інформації.

Доволі часто злочинці роблять помилку і лічильники відвідування сайту також реєструють через місцеві компанії, у такому випадку слід звернутися із запитом, щодо надання інформації про реєстранта (рис. 53).


*Рис. 53. Лічильник відвідування, зареєстрований українською компанією*

Підсумовуючи, зазначимо, що документування окреслених сайтів здійснюється по аналогії з документуванням онлайн-порностудій. Використовуються наступні слідчі та негласні слідчі (розшукові) дії (НСРД):

- огляд веб-сайту;
- контрольована та оперативна закупка;
- тимчасовий доступ до речей і документів;
- зняття інформації з транспортних телекомунікаційних мереж тощо (рис. 54).

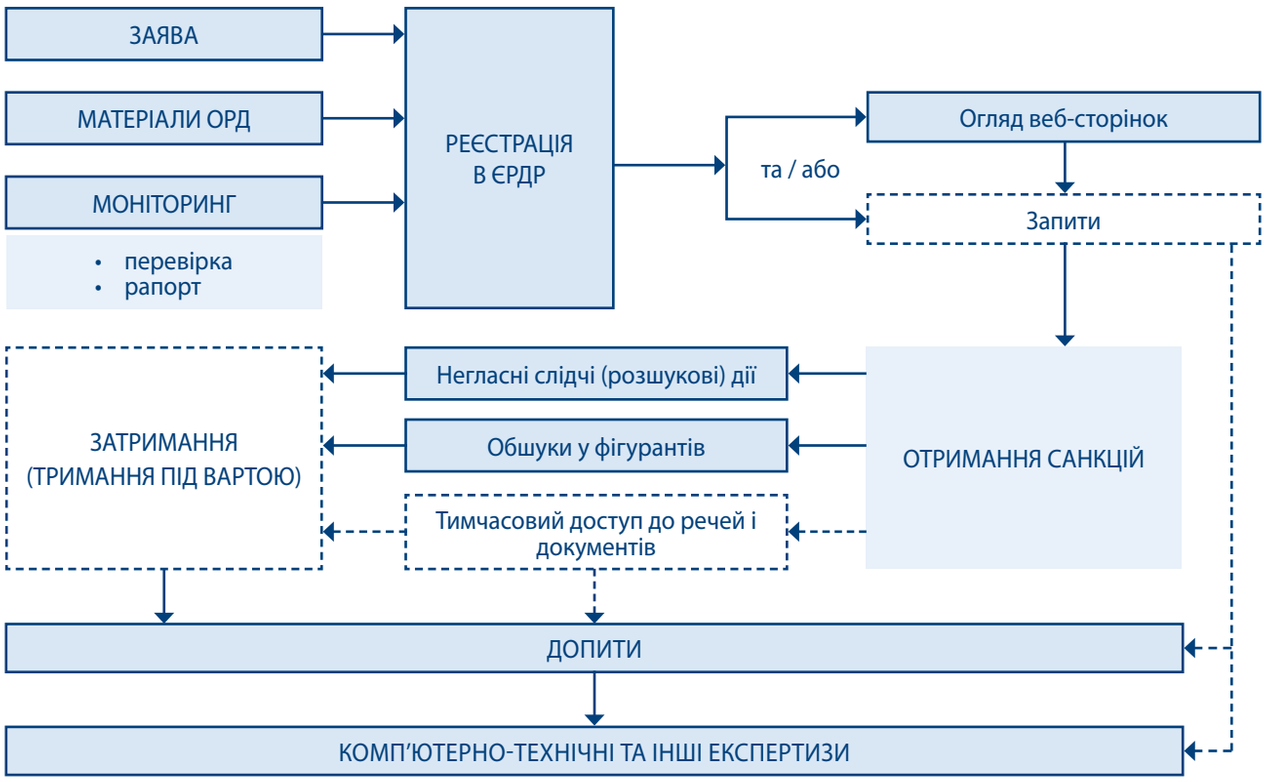



*Рис. 54. Загальний алгоритм документування*

Суцільними та пунктирними лініями на рис. 54 позначено відповідно основні та додаткові дії правоохоронних органів.

Крім того, по таких злочинах корисною може бути і допомога заявників, зокрема, щодо фіксування відповідних протиправних дій.

## МОДУЛЬ 5

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ КОМУНІКАЦІЇ, ОДЕРЖАННЯ КОШТІВ

### 1. ЕЛЕКТРОННА ПОШТА

Електронна пошта (email, e-mail) – це метод обміну цифровими повідомленнями між одним автором та одним або більше отримувачем. Сьогодні системи електронної пошти спираються на модель проміжного накопичення і передачі, а сервери електронної пошти приймають, передають, доставляють і зберігають повідомлення. Ані користувачі, ані їх комп'ютери, не повинні перебувати в режимі онлайн одночасно – їм потрібно лише ненадовго з'єднатися з поштовим сервером на час, потрібний для відправлення або прийому повідомлень.

Користуватися послугами електронної пошти можна як через Інтернет-браузер («Gmail», «Yahoo», «Hotmail», «I.ua», «Ukr.net»), так і за допомогою спеціальних поштових клієнтів. Найпопулярнішими з них є: Evolution, KMail, Mozilla Thunderbird, Netscape Mail, Outlook Express, TheBat!.

Повідомлення електронної пошти складається з двох частин:

1) *тіло повідомлення,* яке може містити текстову інформацію та інші дані, наприклад, графічні (фото/відео, аудіо (звукові)) та бінарні (програми/додатки) файли. Також цілком можна включити гіперпосилання на інші джерела, такі як веб-сайти, групи новин та ftp-сайти.

2) *заголовок повідомлення*, який містить службову інформацію, у тому числі адресу електронної пошти відправника та одну або більше адрес одержувачів. Ці дані включають технічні деталі, наприклад, хто надіслав повідомлення, за допомогою якої програми його було складено, а також через які поштові сервери пройшло повідомлення на шляху до одержувача.

Доступ до технічних заголовків електронного листа, здійснюється через меню поштового клієнта, який використовується. У заголовку міститься важлива інформація, яка може допомогти встановити відправника листа та його місцезнаходження.

Слід пам'ятати, що у заголовку можуть міститися декілька проміжних IP-адрес, через які передавався лист. При цьому IP-адреса відправника, як правило, буде *найнижчою*. Для автоматизації аналізу заголовку поштового листа можна скористатися сервісами:

http://ua.smart-ip.net/trace-email або https://www.iplocation.net/trace-email.

Якщо відправник повідомлення для його створення та відправки використовував веб-інтерфейс поштового серверу, то в цьому випадку заголовок міститиме IP-адресу поштового серверу як відправну (кінцеву). У випадку ж застосування поштових клієнтів ймовірність того, що в заголовку міститиметься IP-адреса терміналу, з якого відправлено листа, набагато збільшується.

Слід мати на увазі, що контактна особа може використовувати для відправлення електронних листів *анонімні ремейлери* – транзитні сервери електронної пошти. Ця обставина ускладнює встановлення місця знаходження контактної особи.

Тепер розглянемо на прикладі, яким чином можна дізнатися інформацію про відправника електронного листа. Для цього дослідимо фрагмент відповідного заголовку.

Received: from **[95.27.244.76]** by web132403.mail.ird.yahoo.com via HTTP; **Fri, 05 Oct 2012 16:20:46 BST**

X-Mailer: **YahooMailWebService/0.8.122.442**

References: <CAD0R7oCuUWrcfa-69c30EQA5g86zDeySQZTFX54ASaoRefVxcw@mail.gmail.com>

Message-ID: <1349450446.38373.YahooMailNeo@web132403.mail.ird.yahoo.com>

Date: Fri, 5 Oct 2012 16:20:46 +0100 (BST)

From: **Kirill Anikeev <a_stratus@yahoo.com>**

Reply-To: Kirill Anikeev <a_stratus@yahoo.com>

Ключовим в ідентифікації відправника електронного листа є частина заголовку із записом «Received: from», яка відображає IP-адресу відправника, в даному випадку це 95.27.244.76, а також час відправки: Fri, 05 Oct 2012 16:20:46 BST (формат часу), тип поштового клієнту (в даному випадку, відправка відбулася через веб-браузер) YahooMailWebService/0.8.122.442, дані щодо відправника Kirill Anikeev <a_stratus@yahoo.com>.

Встановивши IP-адресу, з якої надходили повідомлення від контактної особи, необхідно надіслати запит до провайдера телекомунікацій, який обслуговує дану адресу. У запиті необхідно вказати час з точністю

до секунди, *з обов'язковим зазначенням часового поясу*, та IP-адресу, з якої надходили повідомлення. Запит треба надсилати *до головного офісу* компанії-провайдера, тому що саме там володіють найбільш повною інформацією, викладеною у запиті.

Встановлення провайдера, якому надано у користування IP-адресу, що використовувалася контактною особою, здійснюється за допомогою сервісу Whois, шляхом звернення до так званих Інтернет-реєстратур доменних імен. Документування відповіді Whois може бути здійснено двома способами: перший – це засвідчення відповідної роздруківки у місцевого провайдера, який одночасно є реєстратором IP-адрес (LIR), другий – отримані відомості зазначаються у рапорті оперативного працівника. Правоохоронним органам потрібно одержати від провайдера максимум можливої інформації про особу, якій належить адреса. Якщо мова йде про доменне ім'я, також слід запитати інформацію про усі платіжні реквізити, які використовувались для оплати за користування доменним ім'ям.

У розглянутому прикладі одержану інформацію слід використати для формування запиту на компанію CORBINA TELECOM/Internet Network Operations (рис. 55), з метою встановлення, хто з її користувачів у заданий період часу використовував вказану IP-адресу.


*Рис. 55. Відповідь Whois-сервісу*

При дослідженні поштових платформ потрібно бути дуже уважним, тому що вони можуть містити багато цінних доказів. У якості ілюстрації, із Керівництва з питань електронних доказів можна навести реальний приклад того, як URL-посилання на файл, пов'язаний із пересиланням електронною поштою і знайдений на жорсткому диску підозрюваного, став у нагоді під час розслідування:

https://mail.google.com/mail/h/1fghjf56gshi2/?view=att&th=35hyfdfghdfgdfgwe67tid=0.1&disp=attd&realattid=f_gnt1i7j37&zw

В результаті пошуку з'ясувалося, що остання частина цього URL «realattid» означає «дійсний ідентифікатор прикріплення». Google зберігає на сервері тільки одну копію прикріпленого файлу незалежно від кількості електронних листів, які пересилали цей файл. У результаті слідчі змогли визначити, що було у прикріпленому файлі, і встановили зв'язок підозрюваного із розслідуваними подіями.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано) можна за допомогою сервісу https://www.readnotify.com/.

Для роботи із сервісом слід зареєструватися на безкоштовне пробне використання або оформити підписку. Надсилати відстежувані електронні листи можна у два способи:

- *вручну*: для цього потрібно створити електронного листа у звичній для вас програмі електронної пошти > надрукувати: «.readnotify.com» в кінці адреси електронної пошти одержувача (одержувач цього не побачить), наприклад, «drakecn@yahoo.com.readnotify.com» > надіслати електронного листа.
- *автоматично*: платні абоненти можуть встановити опціональний додаток «ActiveTracker», який автоматично додає функцію відстеження, коли під час надсилання електронних листів.

Після надсилання відстежуваного електронного листа можна зайти до свого облікового запису «ReadNotify» для перевірки статусу. Також можна одержати повідомлення про прочитання «ReadNotification» на електронну пошту, коли відстежуваного електронного листа (або документ) буде відкрито.

Існують й інші ресурси, які працюють за схожою схемою:

http://www.pointofmail.com/, http://www.confimax.com/.

**ЗАВДАННЯ**

**ПРОАНАЛІЗУВАТИ ЗАГОЛОВОК ТА ТІЛО ЛИСТА ЗІ СВОЄЇ ЕЛЕКТРОННОЇ ПОШТОВОЇ СКРИНЬКИ. ВСТАНОВИТИ МАРШРУТ ЙОГО РУХУ, ВІДОМОСТІ ПРО НАЛЕЖНІСТЬ IP-АДРЕСИ ВІДПРАВНИКА ТА ВІДОМОСТІ З ЗАГОЛОВКУ. У ЯКОСТІ ШАБЛОНУ ВЗЯТИ ІНФОРМАЦІЮ З ПРИКЛАДА**

## 2. МУЛЬТИМЕДІЙНІ ЗАСОБИ СПІЛКУВАННЯ

Рівень сучасних технологій дозволяє швидко передавати значний обсяг медіа-контенту, тому серед торговців людьми є досить популярними програмні засоби медіа-спілкування.

Одними із таких засобів є Інтернет-пейджери (Instant Messengers) – це програми, які дозволяють обмінюватися текстовими повідомленнями між комп'ютерами у реальному масштабі часу. На теперішній час найбільш часто застосовуваними для спілкування інтернет-пейджерами є ICQ, QIP, MSN, Google Talk, Pidgin, AIM, Trillian, Windows Live Messenger, Yahoo Messenger.

Для спілкування між суб'єктами торгівлі людьми та жертвами також можуть використовуватись так звані «чати». Цей термін переважно застосовується для опису будь-якої форми синхронного конференц-зв'язку, а іноді навіть асинхронного конференц-зв'язку. Отже цей термін може означати будь-яку технологію, від онлайнових чатів у реальному часі до онлайнової взаємодії з незнайомцями, обміну миттєвими повідомленнями та онлайнових форумів до повного занурення у графічне соціальне середовище.

Чати – це один з інструментів, який використовується, щоб принадити потенційних жертв торгівлі людьми. За допомогою простого чату член організованого злочинного угруповання може відповісти практично на будь-яке запитання принадженої особи.

У роботі працівника правоохоронних органів щодо попередження та розслідування випадків торгівлі людьми, які здійснюються із використанням наведених засобів медіа-спілкування, корисним може бути

застосування сервісу Simkl (simkl.org), який дозволяє використовувати проміжний сервер для відповідних підключень та фіксувати відповідні дані в онлайн-сховищі. Для окремих сервісів передбачено запис звуку.

Слід зазначити, що останнім часом торговці людьми користуються більш складними засобами спілкування, зокрема створеними на базі поширеного протоколу передачі даних VoIP. VoIP-протокол (протокол передачі голосу по Інтернету) та відео телефонія є наступним кроком розвитку Інтернет-технологій, а тому за своєю суттю більше використовується молоддю, особливо якщо цю технологію вбудовано у певні соціальні медіа і вони присутні на планшетах чи смартфонах.

Саме через це злочинні групи користуються цією технологією для спілкування з потенційними жертвами злочину, а у контексті торгівлі людьми вони також вдають із себе молодих людей, щоб вербувати і спокушати жертв.

Злочинці користуються цими формами медіа спілкування у дуже хитрий спосіб, створюючи фальшиві сайти, на яких вони спілкуються з потенційними жертвами і поглиблюють процес ґрумінгу під час розмов наодинці, обмінюючись фотографіями та застосовуючи інші техніки товаришування, доки врешті не організують зустріч зі своїми жертвами.

ДИТЯЧИЙ ҐРУМІНГ – ЦЕ НАВМИСНІ ДІЇ, СПРЯМОВАНІ НА ВСТАНОВЛЕННЯ ДРУЖНІХ ВІДНОСИН ТА ЕМОЦІЙНОГО ЗВ'ЯЗКУ З ДИТИНОЮ І ЗНИЖЕННЯ РІВНЯ ЧИННИКІВ СТРИМАННЯ ДИТИНИ З МЕТОЮ СЕКСУАЛЬНОГО НАСИЛЬСТВА НАД НЕЮ. ДИТЯЧИЙ ҐРУМІНГ МОЖЕ ВИКОРИСТОВУВАТИСЬ ДЛЯ ЗАЛУЧЕННЯ НЕПОВНОЛІТНІХ ДО ТОРГІВЛІ ДІТЬМИ, НЕЛЕГАЛЬНИХ ОБОРУДОК, ТАКИХ ЯК ДИТЯЧА ПРОСТИТУЦІЯ АБО ВИРОБНИЦТВО ДИТЯЧОЇ ПОРНОГРАФІЇ. ЦЕ ПОВЕДІНКА ХАРАКТЕРНА ДЛЯ ПЕДОФІЛІЇ.

ОНЛАЙН ҐРУМЕРИ МОЖУТЬ БУТ РОЗДІЛЕНІ НА ДВІ ГРУПИ. ДО ПЕРШОЇ НАЛЕЖАТЬ ТІ, ЯКІ «ПРАЦЮЮТЬ» ВИКЛЮЧНО ОНЛАЙН, У ТОЙ ЧАС ЯК ДРУГА ГРУПА МАЄ НА МЕТІ ВЧИНЕННЯ СЕКСУАЛЬНОГО НАСИЛЬСТВА НЕ СТІЛЬКИ В КІБЕРПРОСТОРІ ЯК У ФІЗИЧНОМУ СВІТІ. ПРАЦІВНИКИ ПОЛІЦІЇ НЕРІДКО ВИКОРИСТОВУЮТЬ ЛЕГЕНДОВАНІ ПРОФІЛІ ДІТЕЙ ДЛЯ ПРИВАБЛЮВАННЯ ПОТЕНЦІЙНИХ ПЕДОФІЛІВ. ПРИ ЦЬОМУ АНАЛІЗ ВІДПОВІДНИХ ПОЛІЦЕЙСЬКИХ ПРОФІЛІВ ЗАСВІДЧИВ, ЩО ВОНИ НЕ МІСТИЛИ СТЕРЕОТИПНИХ ОЗНАК ВРАЗЛИВИХ ДО НАСИЛЬСТВА ДІТЕЙ. ЦЕ ВКАЗУЄ НА ТЕ, ЩО БУДЬ-ЯКА ДИТИНА МОЖЕ СТАТИ ЖЕРТВОЮ ОНЛАЙН-ҐРУМІНГА [63, С. 111, 117].

У 2017 РОЦІ БРИТАНСЬКОГО ПЕДОФІЛА ПОЛА ЛЕЙТОНА (PAUL LEIGHTON) БУЛО ЗАСУДЖЕНО ДО 16 РОКІВ ПОЗБАВЛЕННЯ ВОЛІ ЗА ЗҐВАЛТУВАННЯ В РЕЖИМІ ОНЛАЙН. ВІН СТВОРИВ 30-40 НЕСПРАВЖНІХ ОБЛІКОВИХ ЗАПИСІВ FACEBOOK ДЛЯ ЗНАЙОМСТВА З ДІТЬМИ. ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ МЕРЕЖІ ЗЛОВМИСНИК СПОЧАТКУ ВМОВЛЯВ ДІТЕЙ НАДІСЛАТИ ЙОМУ ФОТОГРАФІЇ ІНТИМНОГО ХАРАКТЕРУ, ПІСЛЯ ОТРИМАННЯ ЯКИХ ШАНТАЖУВАВ ДІТЕЙ, ЗМУШУЮЧИ ЇХ ДО ВЧИНЕННЯ СЕКСУАЛЬНИХ ДІЙ НАСИЛЬНИЦЬКОГО ХАРАКТЕРУ. ТАК, 14-РІЧНОГО ХЛОПЦЯ З ФЛОРИДИ (США) ЛЕЙТОН ЗМУСИВ ЗҐВАЛТУВАТИ 12 РІЧНУ ПЛЕМІННИЦЮ, 14-РІЧНУ ДІВЧИНУ З ПІВДЕННОЇ ДАКОТИ (США) ПРИМУСИВ ДО СТАТЕВИХ АКТІВ ЗІ СВОЇМ БРАТОМ, ЯКІ ВОНИ ЗНІМАЛИ ДЛЯ ЗЛОВМИСНИКА НА ВІДЕО. В АНАЛОГІЧНІЙ СИТУАЦІЇ ОПИНИЛАСЬ І 13-РІЧНА ДІВЧИНА З ТЕННЕССІ (США). ЗАГАЛОМ ЖЕРТВАМИ СЕРІЙНОГО ПЕДОФІЛА СТАЛИ БІЛЬШЕ СТА ОСІБ З РІЗНИХ КРАЇН [64].

Ці технології доступні по всьому світу і через те, що вони переважно використовуються для спілкування «наодинці», правоохоронним органам важко виявляти таке використання і боротися з ним, якщо тільки воно не є об'єктом цілеспрямованого виявлення.

Як і у випадку інших інтернет-застосувань, злочинний елемент поєднує використання різних їх видів залежно від злочину і категорії та місця перебування потенційних жертв. Це також робиться, щоб спантеличити правоохоронні органи під час визначення їх справжніх особистих даних та місця перебування.

У практиці правоохоронних органів нерідко трапляються випадки, коли правопорушники для комунікації використовують засоби мультимедійного спілкування, зокрема Skype [65] та Viber. Встановити IP-адресу терміналу контактної особи в цьому випадку можна за допомогою програми WireShark. Основна логіка

встановлення IP-адреси абонента полягає у використанні фільтра, який буде відслідковувати мережні пакети, які надходять на локальну адресу, наприклад,

ip.src == IP-адреса and udp.srcport == номер порту and frame.len==розмір пакета.

Для відслідковування IP-адреси абонента Skype у фільтрі потрібно вказати свою IP-адресу та номер порту, який можна дізнатися у настройках Skype (Інструменти > Настройки > Додатково > З'єднання). Після чого на головній сторінці WireShark у поле Filter ввести відповідний фільтр та запустити процес перехоплення пакетів, натиснувши кнопку у вигляді плавнику. Після здійснення вказаних процедур потрібно ініціювати з'єднання з активним абонентом Skype. Якщо він використовує програму Skype, то у вікні WireShark відобразяться пакети з IP-адресою кінцевого вузла зв'язку (це може бути адреса провайдера абонента; його власна зовнішня IP-адреса; локальна адреса, у випадку роботи обох Skype-клієнтів в одній локальній мережі; адреса Microsoft, якщо абонент виходив на зв'язок через веб-клієнт тощо). Так само за допомогою WireShark можна дізнатися IP-адреси абонентів й деяких інших мультимедійних засобів спілкування, зокрема Viber [66, с. 38-39].

Слід відзначити, що аналогічним чином можна дізнатися IP-адреси користувачів програми TeamViewer.

Під час звернення до провайдера з питань приналежності IP-адреси потрібно враховувати використання операторами телекомунікацій механізму CGN (Carrier-Grade NAT) – трансляції мережних адрес. Ця технологія дозволяє оператору виділяти багатьом абонентам внутрішні локальні IP-адреси, через які вони мають змогу користуватися мережею Інтернет. При цьому взаємодія з іншими ресурсами відбувається через єдину зовнішню IP-адресу, яка належить оператору. Таким чином, одночасно користуватися однією й тією ж зовнішньою адресою можуть декілька тисяч абонентів одночасно.

У цьому випадку, запиту до провайдера про встановлення належності IP-адреси із вказівкою лише зовнішньої IP-адреси буде недостатньо. Потрібно або **вказувати у запиті додатково внутрішню IP-адресу,** яку також можна спробувати встановити описаними інструментами, або вносити у запит **декілька точних часових проміжків, протягом яких шуканий абонент користувався зовнішньою IP-адресою**.

У будь-якому випадку слід констатувати наявність проблеми для правоохоронних органів щодо визначення кінцевого абонента – користувача IP-адреси в разі застосування операторами (провайдерами) телекомунікацій механізму CGN. Вказана проблема стосується не тільки вітчизняних правоохоронних органів. На неї звертають увагу й в інших країнах та міжнародних організаціях [67].

**ЗАВДАННЯ**

**СПРОБУЙТЕ САМОСТІЙНО ВИЗНАЧИТИ IP-АДРЕСУ ВІДОМОГО КОРИСТУВАЧА TEAMVIEWER**

## 3. ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ТА БЕЗПЕЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МЕРЕЖІ

З метою уникнення відповідальності за свої дії правопорушники, задіяні у торгівлі людьми, намагаються використовувати різні технології забезпечення анонімності роботи в мережі, а також програми безпечної передачі інформації. Крім того, правопорушниками застосовуються технології вибіркового блокування доступу терміналів за їх географічним розташуванням до створених торговцями людьми мережних ресурсів.

Серед головних способів забезпечення анонімності (рис. 56) потрібно виділити застосування:

*1) проксі-серверів:*

- HTTP (дозволяють працювати з HTTP та іноді FTP протоколом);

- SOCKS 4 (працює не тільки по протоколах HTTP і FTP, але і по будь-якому іншому TCP/IP протоколу прикладного рівня);
- SOCKS 5 (вміє використовувати не тільки TCP, але і UDP з'єднання);
- CGI (скрипти, які самі завантажують віддалену веб-сторінку /відповідно відкривають IP-адресу свого сервера/ і видають її браузеру клієнта);

*2) шелів;*

*3) VPN-серверів;*

*4) Dark-net:*

- TOR;
- I2P.


*Рис. 56. Схема підключення з використанням декількох технологій забезпечення анонімності*

Анонімні проксі-сервери зазвичай використовують особи, які бажають приховати свою справжню адресу в мережі, торговці людьми тут не є виключенням. Запити в мережі при використанні такого серверу здійснюються опосередковано, від імені проксі-сервера, а не від імені комп'ютера особи, яка запитує інформацію.

Через недовіру до анонімних проксі-серверів деякі професійні зловмисники вважають за краще замінювати їх ланцюжком так званих «шелів» (комп'ютерів, на яких зловмисник знає ім'я користувача та пароль, та за посередництвом і від імені яких в подальшому може звертатися до інших комп'ютерів мережі) або використовувати комбіновано обидві технології.

Останнім часом популярним стало застосовувати VPN-сервери, за допомогою яких утворюється віртуальний захищений тунель між вузлами, який забезпечує цілісність та конфіденційність передаваної інформації. Більшість VPN-серверів є платними. Користувач цієї технології повинен встановити на своєму комп'ютері спеціальне клієнтське програмне забезпечення.

У більшості випадків віртуальна приватна мережа «VPN» приховує користувацьку IP-адресу не гірше за проксі, а іноді й краще. Вони працюють по-різному, але досягають однакового результату. По суті, «VPN» – це приватна мережа, яка використовує публічну мережу (зазвичай Інтернет) для з'єднання віддалених сайтів або користувачів. Тому, якщо користувач увійде у «VPN», то той, хто шукає користувацьку IP-адресу, зможе дійти тільки до IP-адреси мережі «VPN», але не побачить початкову IP-адресу користувача.

Поряд із звичайними проіндексованими ресурсами, в Інтернеті існує попит на приватні зони, які доступні лише обмеженим групам осіб для певних цілей. Деякі приватні зони є загальнодоступними, але знайти їх можуть тільки ті користувачі, які знають точне посилання (URL), наприклад, на віддалене хмарне сховище. А деякі зони для доступу потребують автентифікації, наприклад, закриті дошки оголошень або обліковий запис веб-пошти.

Для таких прихованих від пошуку веб-зон придумали узагальнену назву «Deep Web» (інші назви «Hidden Web», «Invisible Web», «Deepnet»).

Крім неіндексованих для пошуку сайтів, баз даних і документів існує ще декілька невидимих рівнів, які вже не доступні через звичайний браузер і які називають «Darknet». В цьому сегменті використовується структура P2P-мережі, повністю зашифрований трафік, свій адресний простір, цілком анонімні вузли. Для доступу до такої мережі потрібно встановити додаткове програмне забезпечення.

До найвідоміших мереж «Darknet» належать Freenet, The Onion Routing (Tor) Hidden Services, Invisible Internet Project (I2P).

TOR-мережа – це мережа віртуальних тунелів для забезпечення анонімності в Інтернеті, яка створюється добровільними учасниками шляхом встановлення на власний комп'ютер або сервер програм-ретрансляторів (Relays), через які і встановлюються з'єднання між клієнтом і сервером в мережі Інтернет. Спроби боротьби правоохоронних органів різних країн з учасниками TOR-мережі, наприклад, у Німеччині, із самою TOR-мережею, наприклад, у КНР, показують загальну неефективність таких спроб.

Наявність на комп'ютері підозрюваної особи програмного забезпечення на зразок TOR, разом з іншими належними та допустимими доказами може свідчити про її намагання приховати злочинну діяльність.

Звичайно, для сприйняття такої позиції у судовому засіданні доцільно скористатись допомогою спеціаліста. Так, відповідно до ст. 360 КПК України під час дослідження доказів суд має право скористатися усними консультаціями або письмовими роз'ясненнями спеціаліста, наданими на підставі його спеціальних знань. Спеціалісту можуть бути поставлені питання щодо суті наданих усних консультацій чи письмових роз'яснень. Першою ставить запитання особа, за клопотанням якої залучено спеціаліста, а потім інші особи, які беруть участь у кримінальному провадженні. Головуючий у судовому засіданні має право ставити спеціалістові запитання в будь-який час дослідження доказів.

Досліджуючи у судовому засіданні, наприклад, протокол огляду персонального комп'ютера, на якому встановлено клієнтське програмне забезпечення Tor, слід попередньо заявити клопотання про залучення спеціаліста, оскільки специфіка даної програми є невідомою широкому загалу. В якості спеціаліста, можуть залучатись викладачі факультетів інформаційних технологій та комп'ютерної інженерії вищих навчальних закладів.

Подібна до TOR-мережі є I2P – відкрита, розподілена, анонімна, самоорганізована комп'ютерна мережа, яка працює поверх загальнодоступних каналів зв'язку Інтернет.

Особливостями функціонування цієї мережі є убезпечення її користувачів від вистежування, використання унікальних ідентифікаторів замість IP-адрес, шифрування трафіку, відсутність централізованих серверів (усі користувачі здійснюють приймання та передачу інформації, тобто є і серверами, і клієнтами), застосовується протокол UDP.

Окрім згаданих технологій торговці людьми у своїй діяльності використовують і традиційні методи криптографії – шифрування передаваних повідомлень. Однією з програм, яка може використовуватися з цією метою є мобільне застосування Signal, Wire тощо, які шифрують потоковий голос та передають

його через Інтернет іншому абоненту. Користувачу не потрібно заводити окремий обліковий запис (використовується номер телефону).

Не варто забувати і про звичайні способи шифрування, які використовуються зловмисниками. Захист архівів, офісних документів, дисків тощо. Подолати такий захист швидко за умови використання зловмисником довгих ключів шифрування можна лише із застосуванням програм розподілених обчислень (http://www.rixler.com/) або, застосовуючи традиційні оперативно-розшукові заходи.

Для приховування змісту передаваної інформації правопорушниками нерідко застосовуються засоби стеганографічних перетворень (приховування однієї інформації в іншій).

## 4. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ЯКІ ЗАСТОСОВУЮТЬСЯ ДЛЯ ОДЕРЖАННЯ ТА ВІДМИВАННЯ КОШТІВ

### ЕЛЕКТРОННІ ГРОШІ ТА ІНТЕРНЕТ ОРІЄНТОВАНІ ПЛАТІЖНІ СИСТЕМИ

**Електронні гроші (e-money)** – це грошові зобов'язання емітента (юридичної особи, що здійснює випуск цінних паперів) в електронному вигляді, які розміщені на електронному пристрої та знаходяться в розпорядженні користувача. Таким пристроєм може бути мікропроцесорна картка, комп'ютер користувача, сервер системи розрахунків де централізовано зберігаються електронні гроші користувачів.

У системах, що здійснюють розрахунки в електронних грошах, банківські рахунки використовуються лише, якщо гроші вводяться та виводяться із системи. У разі емісії електронних грошей традиційні гроші користувачів зараховуються на банківський рахунок емітента. При пред'явленні електронних грошей для погашення, традиційні гроші списуються з банківського рахунка емітента і надаються пред'явнику, наприклад торговцю, який реалізував за електронні гроші товари чи послуги, або споживачу, якщо він вже не потребує такого платіжного засобу. Електронні гроші всіх відомих сьогодні систем є наперед оплаченими.

Правове визначення електронних грошей для країн ЄС міститься в Директиві 2000/46/ЄС, відповідно до якої електронні гроші – це грошова вартість, яка є вимогою до емітента і яка: (i) зберігається на електронному пристрої; (ii) випускається для одержання коштів на суму, не меншу за вартість у грошовому вираженні; (iii) приймається як засіб платежу за зобов'язаннями іншими, ніж зобов'язання емітента.

Визначення електронних грошей, наведене в Директиві 2000/46/ЄС, протягом 2001–2005 р. було імплементовано в національні законодавства усіх країн ЄС.

Головними національними нормативно-правовими актами, які регламентують обіг електронних грошей в Україні є Закон України «Про платіжні системи та переказ коштів в Україні» [68] та Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04 листопада 2010 року № 481 [69].

Згідно з цими документами:

- випуск електронних грошей може здійснювати виключно банк;
- випуск електронних грошей здійснюється шляхом їх надання користувачам або комерційним агентам в обмін на готівкові або безготівкові кошти;
- банк має право випускати електронні гроші на суму, яка не перевищує суму отриманих ним грошових коштів;
- банк, що здійснює випуск електронних грошей, зобов'язаний погашати випущені ним електронні гроші на вимогу користувача.

Із зазначеного вище випливає, що суспільні відносини у сфері випуску та обігу електронних грошей доволі чітко регламентовані законодавством і така діяльність підлягає ліцензуванню.

Виділяють два основних види електронних грошей:

1) на основі карток (card-based e-money);

2) на програмній основі (software-based electronic money).

Окрім електронних грошей у віртуальному просторі також використовуються так звані «цінності» (value), які мають різні назви, наприклад, титульні знаки, віртуальні гроші, жетони, токени, віртуальне золото або срібло, і таке інше.

Інтернет орієнтовані платіжні системи з точки зору організації бізнесу можна поділити на чотири типи:

1. Платіжні системи банківських карт (VISA, MasterCard та ін.), створені банками і процесинговими компаніями. Банк, що відкриває так званий «мерчант рахунок» для торговця, є сховищем для прийнятих через Інтернет грошових коштів і несе відповідальність за їх легальність. А координатором всього складного процесу перевірки карткових даних і гарантом транзакцій є процесинговий центр.
2. Платіжні системи електронних гаманців (Яндекс.Деньги, WebMoney, QIWI та ін.). Поєднують в собі одночасно і функції технічного провайдера при підключенні до системи, і центрального банку для самих себе, і наглядового органу, і законодавця для своїх власних грошей.
3. Платіжні системи посередників (PayPal, Moneybookers). Особлива група організацій, яка з одного боку працює з електронними гаманцями, а з іншого з реальними валютами. Приймають через Інтернет кошти від клієнтів (покупців), а після доставки товару від торговця покупцю переказують отримані кошти торговцю.
4. Універсальні платіжні системи. Працюють за всіма вищевказаними схемами [70, с. 35, 36, 38].

Останнім часом великої популярності набуває такий різновид електронних грошей, як *криптовалюта* – вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту. Функціонування системи відбувається децентралізовано в розподіленій комп'ютерній мережі [71].

Найбільш популярною криптовалютою на теперішній час є біткоїн. Алгоритм роботи цієї валюти було презентовано у 2008 році, відтоді вартість цього активу переважно зростає. У 2017 році ціна продажу одного біткоїну сягнула позначки 7500 $. На відміну від інших видів грошей біткоїн не має централізованого емітента. Так само сам обіг валюти не контролюється жодним регулятором. Для збереження цілісності системи випуску та обігу біткоїнів використовуються асиметричні криптографічні методи. Крім того, результати усіх транзакцій передаються іншим учасникам системи за технологією peer-to-peer.

Робота з криптовалютами ґрунтується на застосуванні технології Blockchain, яка передбачає генерування геш-згортки за кожною транзакцією на основі попередньої. Таким чином, кожен наступний блок містить посилання на попередній. Проаналізувавши один геш, можна подібно ланцюжку (chain) перевірити інші, згенеровані в результаті попередніх транзакцій. Так, наприклад, якщо хтось з учасників системи здійснює переведення криптовалюти з одного гаманця на інший, то генерується відповідний блок. Інформація про нього розсилається іншим учасникам системи, більша половина яких має підтвердити транзакцію, спираючись на власну базу даних попередніх транзакцій. Тільки після такого підтвердження відбувається остаточне переведення криптовалюти на інший гаманець.

Для перегляду роботи системи Blockchain можна скористатися сайтом blockchain.info (рис. 57).

Робота розподіленої системи криптовалюти забезпечується за участю так званих «майнерів», які надають свої обчислювальні потужності для вирішення складних математичних завдань. За це майнери одержують винагороду у вигляді емітованої криптовалюти та комісійних виплат.

Інші популярні криптовалюти Zcash, Эфириум, Dash працюють за схожими принципами.

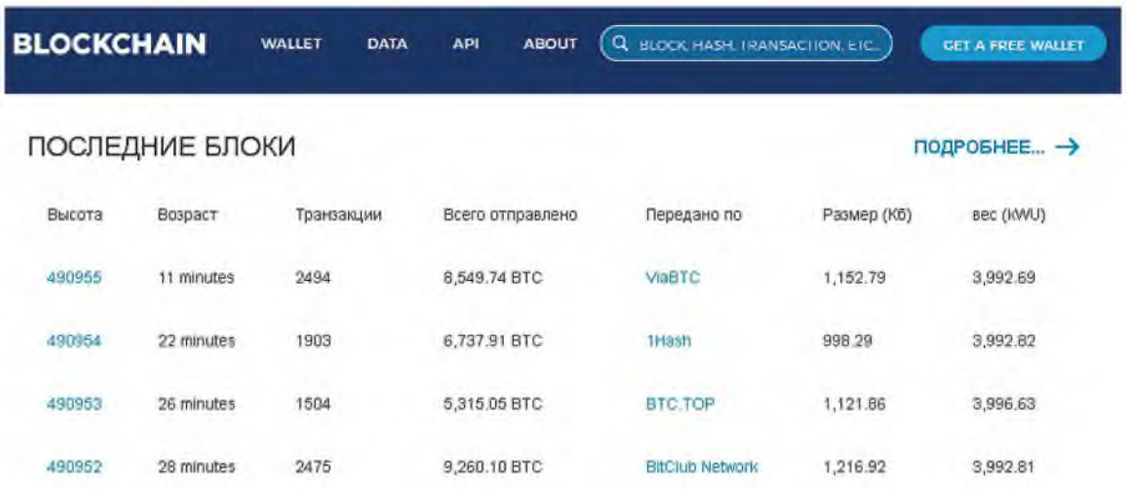



*Рис. 57. Головна сторінка сайту blockchain.info*

Як засвідчує практика на території України найпопулярнішими способами розрахунків між особами, які причетні до торгівлі людьми є використання банківських платіжних карт, а також систем онлайн-платежів WebMoney та Yandex.Деньги.

Слід зазначити, що навіть при використанні електронних платіжних систем, **банківські карти** у 90% випадків використовуються для кінцевого етапу конвертації грошей у готівку.

Незважаючи на здебільшого іменний характер банківських платіжних карток, це зовсім не зменшує долю використання їх злочинцями. В сучасних умовах, недосконалості законодавчої бази та корупції серед працівників фінансових установ, існує великий підпільний ринок із продажу платіжних карток, випущених на підставних осіб. Так, всього за 150-200 доларів США цілком можливо придбати банківську карту, емітовану на ім'я не існуючої або підставної особи, здебільшого безхатченка, чи наркозалежного. До такої карти додається мобільний телефон та можливість розрахунків онлайн, що взагалі не обмежує сферу її застосування.

У зв'язку з цим, при отриманні інформації щодо розрахунків банківською платіжною картою відразу, необхідно ідентифікувати банк-емітент (*банк, який в випустив платіжну картку*) карти та вжити заходів щодо збереження інформації, яка у подальшому може бути використана в якості доказів. Фінансову установу, яка випустила платіжний інструмент, можна визначити за допомогою перших шести цифр номера карти, так званого Bin-коду. Для цього існують бази даних, які в режимі онлайн дозволяють отримати таку інформацію (www.bindb.com, www.binlist.net, www.bins.pro, www.bindatabase.org тощо):

Оскільки будь-яка інформація щодо рахунку клієнта є банківською таємницею, то її отримання можливе лише після відповідного рішення суду. У сучасних реаліях отримання такого документу, а також його виконання банком може зайняти тривалий проміжок часу, а тому є **вкрай важливим** відразу після ідентифікації фінансової установи звернутися на її адресу із запитом про збереження усієї інформації, яка у майбутньому може **бути використана в якості доказу**. Сюди слід віднести насамперед дані щодо руху коштів, відео з камер спостереження щодо особи, яка відкривала банківський рахунок, приходила в касу за готівкою чи користувалася банкоматом тощо.

Як було зазначено, у торговців людьми користується популярністю WebMoney – електронна система миттєвих інтернет-розрахунків, середовище і технологія для ведення бізнесу та електронної комерції.

В Україні працює з 2003 року та, за ствердженням власників системи, використовується понад 2 млн. українцями. Юридично в системі відбувається передача (трансфер) майнових прав, облік яких здійснюється за допомогою спеціальних розписок – «титульних знаків», номінованих в прив'язці до різних валют і золота.

Переказ коштів можливий лише між гаманцями одного виду; обмін титульних знаків різних видів проводиться в обмінних сервісах, що не мають безпосереднього відношення до системи [72].

Номер електронного гаманця складається із букви латинського алфавіту, який вказує на його тип та 12 цифр, наприклад *Z169132036510. Один обліковий запис користувача може налічувати декілька різних гаманців, які об'єднані єдиним ідентифікатором «WMID».*

Первинну інформацію щодо власника гаманця можна одержати на офіційному веб-сайті платіжної системи, для цього у меню пошуку достатньо ввести номер гаманця або «WMID» користувача.

Одержання більш детальної інформації: даних, вказаних при реєстрації, номера мобільного телефону, історії переказів грошових коштів та IP-адрес доступу до системи, можливе лише після надсилання офіційного запиту до представництва компанії.

Після одержання такої інформації її слід уважно проаналізувати та відстежити ланцюг переказу коштів. Адже з метою конспірації, злочинці зазвичай використовують вигадані анкетні дані. Однак, як показує практика, для легалізації, отриманих коштів, вони можуть бути переказані на декілька проміжних гаманців, а потім на легітимний, який відкрито на реальні дані злочинця та пов'язано з його банківським рахунком.

Конвертувати титульні знаки WebMoney у гроші можна лише через верифіковані облікові записи, які відкриваються тільки після підтвердження особи користувача в офісі компанії із наданням документів, що посвідчують особу. Після процедури верифікації відкриваються можливості переказу коштів на банківські платіжні картки. Тут злочинці можуть діяти двома способами:

- зареєструвати та верифікувати обліковий запис WebMoney на документи підставної особи;
- скористатися послугами пунктів обміну та конвертації електронних грошей у готівку, які діють у мережі Інтернет. В такому випадку, злочинець переказує титульні знаки на гаманець обмінного пункту та вказує номер своєї платіжної карти. Протягом доби власник такого обмінного пункту із відрахуванням відсотків за свої послуги переказує кошти на банківську карту злочинця.

Прикладів використання системи WebMoney у торгівлі людьми є десятки. Так, один із сайтів з реклами послуг повій використовував вказану платіжну систему для оплати місячного абонементу із розміщення реклами (рис. 58).

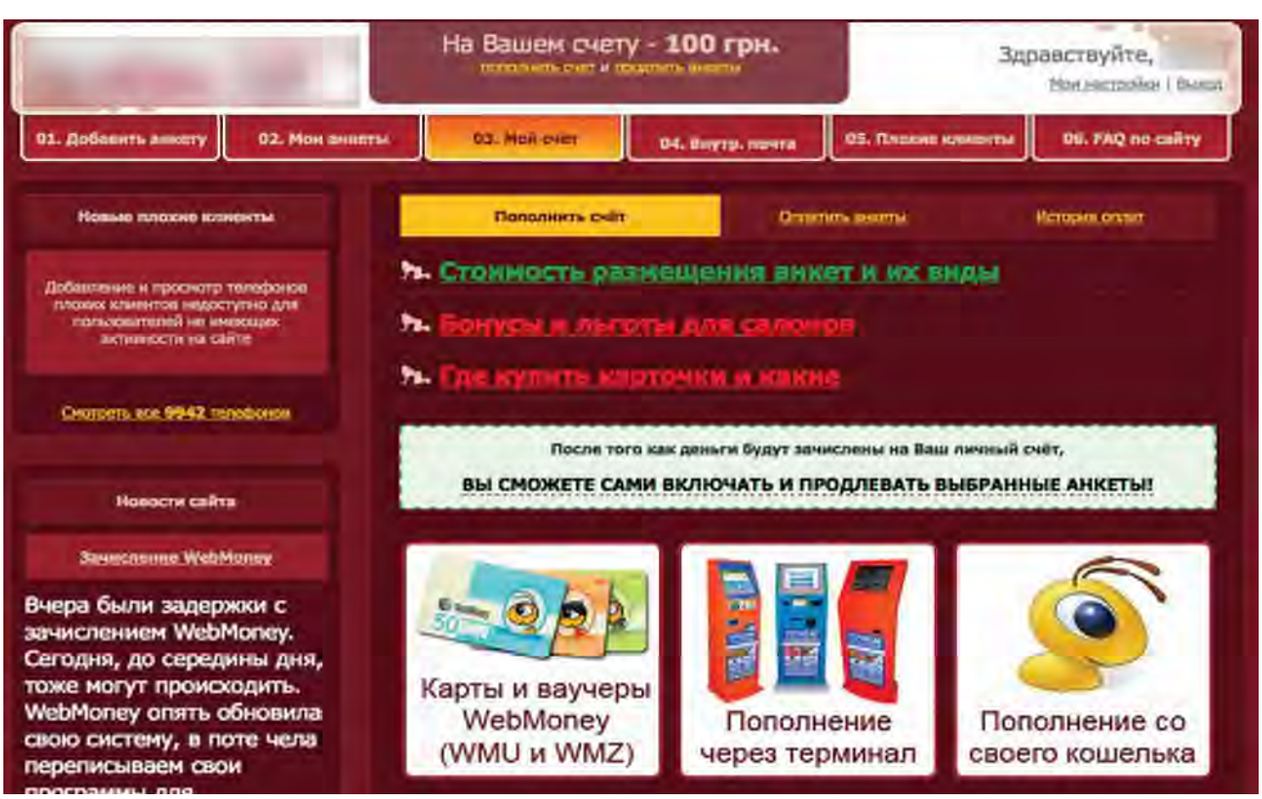



*Рис. 58. Використання WebMoney для оплати*

Доступ до сайтів трансляції відео із веб-камер здебільшого також оплачуються за допомогою електронних платіжних систем, у тому числі WebMoney. Крім цього, все ще залишається популярною вказана система Інтернет-розрахунків серед збувачів дитячої порнографії.

Процесуальний керівник та слідчий, отримавши інформацію про облікові записи електронної платіжної системи WebMoney, що використовуються злочинцями, повинні направити до суду клопотання про накладення арешту на майно.

Згідно зі ст. 170 КПК України арештом майна є тимчасове, до скасування у встановленому цим Кодексом порядку, позбавлення за ухвалою слідчого судді або суду права на відчуження, розпорядження та/або користування майном, щодо якого існує сукупність підстав чи розумних підозр вважати, що воно є доказом злочину, підлягає спеціальній конфіскації у підозрюваного, обвинуваченого, засудженого, третіх осіб, конфіскації у юридичної особи, для забезпечення цивільного позову, стягнення з юридичної особи отриманої неправомірної вигоди, можливої конфіскації майна.

Аналіз судової практики, згідно з відомостями Єдиного державного реєстру судових рішень, свідчить про численні випадки накладення арешту на майно, а саме на грошові кошти, що розташовані на рахунках/облікових записах електронної платіжної системи WEBMONEY ТОВ «ВЕБМАНІ.ЮЕЙ», за клопотаннями слідчих, погоджених з процесуальними керівниками. Водночас, в подальшому, судова практика щодо перегляду таких рішень різниться. Так, в Єдиному державному реєстрі судових рішень наявні рішення про скасування арешту на майно з підстав того, що ТОВ «ВЕБМАНІ.ЮЕЙ» забезпечує функціонування електронної системи WebMoney Transfer, яка використовується для Інтернет-разрахунків відповідними активами, які не є грошовими коштами, а фактично підтверджують право грошової вимоги користувача системи, а тому вказані Інтернет-розрахунки по суті є купівлею-продажем права вимоги в розумінні положень ст. 512, ст. 656 ЦК України, а самі облікові записи не є грошовими рахунками і не містять грошових коштів, що виключає можливість їх конфіскації та відшкодування за їх рахунок шкоди, що було метою та підставою оскаржуваного арешту [73].

На противагу вищезазначеного рішення ухвалою Апеляційного суду м. Києва від 02.02.2017, апеляційну скаргу представника власника майна – адвоката про скасування арешт на грошові кошти, що розташовані на рахунку (ідентифікаторі) електронної платіжної системи WEB MONEY (ТОВ «ВЕБМАНІ.ЮЕЙ» залишено без задоволення [74].

У скарзі адвокат зазначав, що власник облікового запису на який накладено арешт не входить до кола осіб, визначених у ч. 5, ч. 6 ст. 170 КПК України, оскільки він не є підозрюваним, обвинуваченим, засудженим, фізичною чи юридичною особою, яка в силу закону несе цивільну відповідальність за шкоду, завдану діями (бездіяльністю) підозрюваного, обвинуваченого, засудженого або неосудної особи. Також, на думку автора апеляційної скарги відсутні дані про розмір шкоди, крім того не враховано розумність та співрозмірність накладення арешту на майно, а ухвала слідчого судді не містить конкретного переліку майна, на яке накладено арешт.

Відмовляючи в задоволенні такої скарги колегія суддів зазначила, що арешт майна з підстав передбачених ч. ч. 2, 3 ст. 170 КПК України по суті являє собою форму забезпечення доказів і є самостійною правовою підставою для арешту майна поряд з забезпеченням цивільного позову та конфіскацією майна та, на відміну від двох останніх правових підстав, не вимагає оголошення підозри у кримінальному провадженні і не пов'язує особу підозрюваного з можливістю арешту такого майна.

Арешт може бути накладений у встановленому КПК порядку на рухоме чи нерухоме майно, гроші у будь-якій валюті готівкою або у безготівковій формі, в тому числі кошти та цінності, що знаходяться на банківських рахунках чи на зберіганні у банках або інших фінансових установах, видаткові операції, цінні папери, **майнові**, корпоративні права, щодо яких ухвалою чи рішенням слідчого судді, суду визначено необхідність арешту майна. Крім того, Законом допускається арешт майна з метою забезпечення збереження речових доказів.

Враховуючи викладені та інші підстави, в задоволенні апеляційної скарги адвоката відмовлено, а арешт накладений на грошові кошти, що розташовані на рахунку електронної платіжної системи WEBMONEY (ТОВ «ВЕБМАНІ.ЮЕЙ» залишено без змін.

На детальному описі платіжних систем Qiwi зупинятися не будемо, оскільки вона функціонує за схожими принципами із WebMoney. Слід лише зазначити, що вказана система розрахунків в Україні має лише маркетингові та рекламні представництва, а тому отримання буд-якої технічної інформації вимагає звернення із офіційним запитом до відповідного закордонного офісу.

**ЗАВДАННЯ**

**СТВОРІТЬ ВЛАСНИЙ ЕЛЕКТРОННИЙ ГАМАНЕЦЬ. ВСТАНОВІТЬ ВІДОМОСТІ ЩОДО ВЛАСНИКА ГАМАНЦЯ WEBMONEY ЗА ДОПОМОГОЮ ВІДОМИХ ОНЛАЙН-ЗАСОБІВ**

## ГОЛОВНІ СПОСОБИ ЛЕГАЛІЗАЦІЇ КОШТІВ

Ст. 209 Кримінального кодексу України визначає легалізацію (відмивання) доходів, одержаних злочинним шляхом, як вчинення фінансової операції чи правочину з коштами або іншим майном, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів, а також вчинення дій, спрямованих на приховання чи маскування незаконного походження таких коштів або іншого майна чи володіння ними, прав на такі кошти або майно, джерела їх походження, місцезнаходження, переміщення, зміну їх форми (перетворення), а так само набуття, володіння або використання коштів чи іншого майна, одержаних внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів.

У міжнародних нормативно-правових актах поняття легалізації («відмивання») доходів від злочинної діяльності було визначено у Віденській конвенції ООН «Про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин» від 19 грудня 1988 року, а у Страсбурзькій конвенції Ради Європи з відмивання, виявлення, вилучення та конфіскації доходів від злочинної діяльності, на відміну від Віденської конвенції, йдеться про «відмивання» грошей, отриманих не тільки від наркобізнесу, але й будь-яким злочинним шляхом [75, с. 312, 315].

Способи легалізації коштів, отриманих від торгівлі людьми, мало чим відрізняються від тих, що використовуються при наркобізнесі чи торгівлі зброєю. В усіх випадках використовуються підставні «фіктивні» фірми, через рахунки яких проходять кошти.

Використання високих інформаційних технологій в організації торгівлі людьми вносить свої корективи і у способи відмивання грошей, здебільшого розширяючи можливості злочинців у легалізації їхніх доходів. Досить поширеним є спосіб отримання незаконних доходів з-за кордону через системи грошових переказів WesternUnion, MoneyGram, які у поєднанні із системами електронних платежів є ефективним інструментом «відбілювання доходів». Так, якщо у правопорушника за кордоном є певна сума грошей, яку необхідно переказати в Україну, то на спеціалізованих форумах він може підшукати сервіс по «обналу».

Власники таких сервісів володіють розгалуженою мережею підставних осіб «дропів» у різних країнах. У попередньо-обговорений спосіб, правопорушник переказує власнику сервісу певну суму грошей, отримавши їх, останній за допомогою дропів ініціює серію грошових переказів у країну призначення через системи WesternUnion та MoneyGram (інколи у схемі беруть участь проміжна країни). Щойно гроші надходять в Україну, інша група підставних осіб, одержує перекази в банку та передає їх своєму керівнику, а той, як правило, володіючи «легальним» сервісом по конвертації електронних валют переказує їх на банківський рахунок замовника, отримавши свій відсоток від «угоди». Якщо власник сервісу з легалізації, має зв'язки серед банківських працівників, то для отримання грошових переказів можуть використовуватися лише копії паспортів «дропів», що значно спрощує схему «відмивання».

На практиці злочинці максимально автоматизували такий процес, мінімізувавши участь людини. Для цього створено спеціальні он-лайн сервіси з легалізації, в яких замовник в автоматичному режимі ініціює усі перекази у декілька кліків комп'ютерної миші.

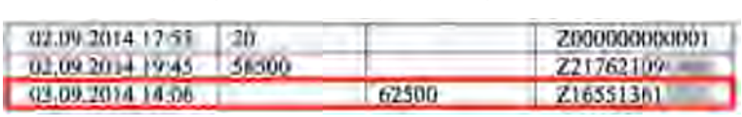
Усіх «дропів» можна розділити на два види: *обізнаних* про факт їх співучасті у відмиванні грошей і *необізнаних*, яких злочинці використовують в сліпу. Оскільки будь-який «дроп-проект», не може існувати без «грошових мулів», головним завданням для злочинців є «вербування» осіб, які потім будуть використані для отримання коштів у банках. У випадку використання так званих «обізнаних» мулів все просто – особа чітко знає, що отримає кошти від протиправної діяльності, але йде на це свідомо, очікуючи винагороду – здебільшого у процентному відношенні від «відмитої» суми.

Якщо вербуються «необізнані дропи», злочинець повинен вжити низку заходів, щоб отримати бажаних співучасників.

1. На першому етапі, як правило, створюється веб-сайт фіктивної організації, яка нібито наймає «фінансових консультантів». Тут, крім якісного дизайну, злочинці як правило купують так звані «джоб-відгуки», що є фіктивними позитивними відгуками про компанію «дроповода». Це допомагає підвищити загальний рівень довіри до фірми у майбутніх «мулів».
2. На другому етапі відбираються кандидати, які найкраще підходять до такої роботи: жінки, студенти, особи без «досвіду роботи» тощо.
3. Вербувальна бесіда. На цьому етапі злочинці проводять «онлайн-співбесіду», де майбутнім кандидатам розповідають правдиву легенду. Як правило, їм пропонують за «відсоток», нібито отримувати гроші компанії в банку та передавати представнику з руку у руки. Інколи це пояснюють тим, що компанія прагне зменшити суму податків, а тому банківські рахунки відкриваються не на юридичну особу, а на фізичну – самого «грошового мула». Легенда залежить лише від глибини уяви самого вербувальника.
4. Укладання із «грошовим мулом» трудового договору, перевірка вірності дропа за результатами тестових завдань.

«Дроп-проекти» є об'єктами торгівлі в «андерграунд ком'юніті», їх ціна може коливатися від 1000 до 50 000$.

Ще одним дієвим способом легалізації коштів, отриманих злочинним шляхом є використання мережних валютних бірж, таких як «Форекс». У такому випадку особа, яка надає послуги із легалізації коштів, є власником онлайн біржі та отримує від усіх охочих інвестиції для здійснення торгів. Однак насправді це фіктивна валютна біржа, яка немає жодного стосунку до фінансового ринку. Гроші отримуються від замовника і через деякий час повертаються йому на легітимний банківський рахунок у вигляді «виграшу» нібито від торгів на брокерській біржі. Яскравим прикладом такої схеми є легалізація коштів одним із сутенерів, власником великого сайту із реклами послуг повій (рис. 59).



| | | | |
|---|---|---|---|
| 02.09.2014 17:51 | 20 | | Z000000000001 |
| 02.09.2014 19:45 | 58500 | | Z21762109 |
| 03.09.2014 14:06 | | 62500 | Z1655136[illegible] |

*Рис. 59. Відмивання грошей через електронну біржу*

Через неперсоналізований гаманець платіжної системи WebMoney гроші переказуються на рахунок «брокера». Ця сума з відрахуванням відсотків уже через кілька днів повернеться на банківський рахунок злочинця у вигляді цілком «законного» виграшу.

Під час документування легалізації коштів, одержаних злочинним шляхом, вкрай важливою є оперативна співпраця із усіма платіжними системами та банківським установами. Представництво WesternUnion знаходиться у Латвії. У випадку виявлення підозрілих транзакцій необхідно звернутися туди із письмовим запитом щодо одержання інформації, а також проханням провести детальний фінансовий аналіз.

**ЗАВДАННЯ**

**СКЛАДІТЬ ЗАПИТ ДО ПРЕДСТАВНИЦТВА WESTERNUNION**

МОДУЛЬ 6

# ОСОБЛИВОСТІ ОГЛЯДУ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ, ВИЯВЛЕНИХ НА МІСЦІ ПОДІЇ

## 1. ОГЛЯД МІСЦЯ ПОДІЇ ЗЛОЧИНУ, ВЧИНЕНОГО З ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Згідно з ч. 1 ст. 237 КПК України огляд як слідча (розшукова) дія проводиться слідчим, прокурором з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення.

На відміну від інших слідчих (розшукових) дій проведення огляду допускається до внесення відомостей до Єдиного реєстру досудового розслідування, що передбачено ч. 3 ст. 214 КПК України. До проведення огляду електронних доказів висуваються такі ж загальні вимоги як і для проведення інших слідчих (розшукових) дій, які викладено у ст.ст. 223, 237 КПК України:

- слідчий, прокурор вживає належних заходів для забезпечення присутності під час проведення слідчої (розшукової) дії осіб, чиї права та законні інтереси можуть бути обмежені або порушені. Перед проведенням слідчої (розшукової) дії особам, які беруть у ній участь, роз'яснюються їх права і обов'язки, передбачені Кримінальним процесуальним кодексом, а також відповідальність, встановлена законом;
- проведення слідчих (розшукових) дій у нічний час (з 22 до 6 години) не допускається, за винятком невідкладних випадків, коли затримка в їх проведенні може призвести до втрати слідів кримінального правопорушення чи втечі підозрюваного;
- слідчий, прокурор зобов'язаний запросити не менше двох незаінтересованих осіб (понятих) для пред'явлення речі для впізнання, в інших випадках запрошення понятих не є обов'язковим, у той же час вони можуть бути запрошені, якщо слідчий, прокурор вважатиме це за доцільне;
- понятими не можуть бути потерпілий, родичі підозрюваного, обвинуваченого і потерпілого, працівники правоохоронних органів, а також особи, заінтересовані в результатах кримінального провадження.
- огляд житла чи іншого володіння особи здійснюється згідно з правилами КПК, передбаченими для обшуку житла чи іншого володіння особи.
- для участі в огляді може бути запрошений потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження. З метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів;
- особи, у присутності яких здійснюється огляд, при проведенні цієї слідчої (розшукової) дії мають право робити заяви, що підлягають занесенню до протоколу огляду;
- при проведенні огляду дозволяється вилучення лише речей і документів, які мають значення для кримінального провадження, та речей, вилучених з обігу. Усі вилучені речі і документи підлягають негайному огляду і опечатуванню із завіренням підписами осіб, які брали участь у проведенні огляду. У разі якщо огляд речей і документів на місці здійснити неможливо або їх огляд пов'язаний з ускладненнями, речі та документи тимчасово опечатуються і зберігаються у такому вигляді доти, доки не буде здійснено їх остаточні огляд і опечатування;

- слідчий, прокурор має право заборонити будь-якій особі залишити місце огляду до його закінчення та вчинювати будь-які дії, що заважають проведенню огляду. Невиконання цих вимог тягне за собою передбачену законом відповідальність;
- при огляді слідчий, прокурор або за їх дорученням залучений спеціаліст має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення оглянутого місця чи окремих речей, виготовляти відбитки та зліпки, оглядати і вилучати речі і документи, які мають значення для кримінального провадження. Предмети, які вилучені законом з обігу, підлягають вилученню незалежно від їх відношення до кримінального провадження. Вилучені речі та документи, що не відносяться до предметів, які вилучені законом з обігу, вважаються тимчасово вилученим майном;
- фіксація огляду відбувається у протоколі або на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії.

АНАЛІЗ ФОРМ ДОКУМЕНТУВАННЯ ПРОЦЕСУ ОГЛЯДУ ІНФОРМАЦІЇ, ЯКА НЕ МАЄ ОБМЕЖЕННЯ ДОСТУПУ ВСТАНОВЛЕНОГО ЇЇ ВОЛОДІЛЬЦЕМ ТА ЗБЕРІГАЄТЬСЯ В ЕЛЕКТРОННОМУ ВИГЛЯДІ, В РІЗНИХ РЕГІОНАХ УКРАЇНИ ЗАСВІДЧУЄ, ЩО ІСНУЮТЬ ДВА ГОЛОВНИХ ПІДХОДИ В ЦЬОМУ ПИТАННІ. ПЕРШИЙ ПОЛЯГАЄ У ВІДПОВІДНОМУ ДОКУМЕНТУВАННІ З ВИКОРИСТАННЯМ ПРОТОКОЛУ ОГЛЯДУ. У ДРУГОМУ ВИПАДКУ ПРОЦЕС ДОКУМЕНТУВАННЯ ОФОРМЛЮЄТЬСЯ ПРОТОКОЛОМ НСРД ЩОДО ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ, ДОСТУП ДО ЯКИХ НЕ ОБМЕЖУЄТЬСЯ ЇЇ ВЛАСНИКОМ, ВОЛОДІЛЬЦЕМ АБО УТРИМУВАЧЕМ АБО НЕ ПОВ'ЯЗАНИЙ З ПОДОЛАННЯМ СИСТЕМИ ЛОГІЧНОГО ЗАХИСТУ, А ТОМУ НЕ ПОТРЕБУЄ ДОЗВОЛУ СЛІДЧОГО СУДДІ (Ч. 2 СТ. 264 КПК УКРАЇНИ). РІЗНИЦЯ В ПІДХОДАХ ПОЯСНЮЄТЬСЯ СУПЕРЕЧНОСТЯМИ ЩОДО НАЛЕЖНОСТІ ІНФОРМАЦІЇ В ЕЛЕКТРОННІЙ ФОРМІ ДО МІСЦЕВОСТІ, ПРИМІЩЕННЯ, РЕЧЕЙ АБО ДОКУМЕНТІВ, ЩОДО ЯКИХ МОЖНА ЗДІЙСНЮВАТИ ОГЛЯД (Ч. 1 СТ. 237 КПК УКРАЇНИ). ВОДНОЧАС БІЛЬШІСТЬ ПРАВООХОРОННИХ ОРГАНІВ В РЕГІОНАХ ВСЕ Ж ТЯЖІЮТЬ ДО ВИКОРИСТАННЯ ПЕРШОГО ПІДХОДУ – ОФОРМЛЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПРОТОКОЛОМ ОГЛЯДУ.

ЗГІДНО ПОЗИЦІЇ ГЕНЕРАЛЬНОЇ ПРОКУРАТУРИ УКРАЇНИ З ЦЬОГО ПРИВОДУ – ФІКСАЦІЇ ІНФОРМАЦІЇ З ВІДКРИТИМ ДОСТУПОМ В МЕРЕЖІ ІНТЕРНЕТ МОЖЛИВА ШЛЯХОМ СКЛАДАННЯ ПРОТОКОЛУ ОГЛЯДУ.

Аналізуючи проведення огляду при розслідуванні злочину, пов'язаного з торгівлею людьми, вчиненого з застосуванням інформаційних технологій, слід зазначити, що у КПК України містяться поняття огляду місця події, огляду місцевості, приміщення, речей та документів.

Так, ч. 3 ст. 214 КПК України (Початок досудового розслідування) встановлено, що огляд місця події у невідкладних випадках може бути проведений до внесення відомостей до Єдиного реєстру досудових розслідувань, що здійснюється негайно після завершення огляду.

У криміналістиці місцем події називають ділянку місцевості або приміщення, у межах якого виявлені сліди вчиненого злочину, однак, враховуючи, що сліди злочину вчиненого з застосуванням інформаційних технологій знаходиться у цифровому вигляді, а огляду підлягають веб-сайти з фіксацією відеочатів зі сценами сексуального характеру, соціальні мережі, дошки оголошень, електронна пошта, чати, у слідчого або прокурора виникають питання, який саме протокол огляду складати: документу чи речового доказу.

На практиці, вищезазначена неузгодженість може призвести до того, що суд визнає недопустимим протокол огляду речового доказу, оскільки буде вважати, що мав бути складений протокол огляду документа, чи навпаки.

Трапляються випадки коли слідчі, уникаючи вказаних суперечностей, не конкретизують назву протоколу, вказуючи лише «протокол огляду», або називають його протокол огляду речового доказу – документу.

Говорячи про аргументацію використання протоколу огляду документу в описаній ситуації, слід згадати зміст ст.ст. 98-99 КПК України. У ч. 2 ст. 99 КПК України зокрема наголошується, що до документів можуть належати носії інформації (у тому числі електронні).

У той же час речовими доказами, згідно зі ст. 98 КПК України є матеріальні об'єкти, які 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, в тому числі предмети, що були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення.

Саме той факт, що речовими доказами згідно з КПК України є матеріальні об'єкти, підкреслюється прибічниками підходу про оформлення відповідної слідчої дії протоколом огляду документів. У той же час незаперечним фактом є і те, що інформація не може існувати без носія, яким може виступати поле або речовина, а відтак в окремих випадках можна стверджувати про належність цифрових носіїв до матеріальних об'єктів.

Документом, згідно зі ст. 99 КПК України є 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.

З змісту статей 98, 99 КПК України вбачається, що обидва названих джерела доказів є матеріальними об'єктами і в них є відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

До відмінностей, які розмежовують речові докази та документи, в контексті складання протоколу огляду місця події злочину, вчиненого з застосуванням інформаційних технологій слід віднести те, що речовий доказ зберігає на собі сліди кримінального правопорушення, а документ є об'єктом спеціально створеним з метою збереження інформації.

Крім того, згідно ч. 2 ст. 98 КПК України, документи є речовими доказами, якщо вони містять ознаки притаманні речовим доказам, а тому, уповноважені правоохоронні органи, оглядаючи Інтернет сторінку в мережі Інтернет, за допомогою якої відбулось вербування потерпілого від торгівлі людьми або на якій зафіксовано інформацію про одержання коштів від вчиненого злочину, з урахуванням того, що Інтернет сторінка є об'єктом спеціально створеним з метою збереження інформації і водночас зберігає на собі сліди кримінального правопорушення, мають визначитись, що саме підлягає огляду: документ-джерело доказу чи документ-речовий доказ.

Для розмежування документів-джерел доказів від документів-речових доказів можливо застосовувати такі критерії:

1) відомості, які зафіксовані у документах-речових доказах, відрізняються від інформації, шо міститься в «інших документах», за своїм процесуальним статусом;

2) доказове значення у документах-джерелах доказів має лише зміст, а їх форма має допоміжне значення. На відміну від них, документи — речові докази значимі у справі не лише за змістом, а й за своїм зовнішнім виглядом, місцем, часом їх виявлення тощо;

3) документи-джерела доказів можуть бути замінними, у той час як документи-речові докази внаслідок того, шо зміни, які відбулися з ними, пов'язані з подією злочину, не можуть бути замінені на інші, оскільки сліди, шо відобразились у них, є унікальними й існують в однині;

4) документ-джерело доказів містить у собі відомості, які складаються з опису події злочину чи фактів його вчинення за допомогою письма або інших умовних знакових кодів тощо, на відміну від документа-речового доказу, що закріплює не опис матеріальних слідів злочину чи факту його скоєння, а самі сліди злочину, які збереглися на ньому [76].

Слід зазначити, що при складання протоколу огляду особливу увагу треба звертати саме на зміст протоколу, в якому мають зазначатись: доменне ім'я, IP-адреса, характеристики технічних засобів, умови та порядок їх використання, послідовність дій тощо, оскільки саме ці складові роблять протокол належним та допустимим доказом.

## 2. ЗАГАЛЬНИЙ ОГЛЯД СТАНДАРТНИХ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Під час розслідування злочинів, пов'язаних із торгівлею людьми, працівникам правоохоронних органів часто доводиться мати справу із технічними засобами, які використовуються злочинцями у якості знарядь та засобів вчинення злочинів. Серед таких засобів найчастіше зустрічаються:

- стаціонарні персональні комп'ютери (робочі станції або сервери);
- ноутбуки та нетбуки;
- планшети;
- бортові комп'ютери автомобілів;
- телевізори із функцією SMART;
- GPS-навігатори;
- носії цифрової інформації (диски, дискети, флеш-носії тощо);
- периферійне обладнання (принтери, сканери тощо);
- мобільні комп'ютерні пристрої із функцією телефону.

Враховуючи особливості роботи із наведеними пристроями, а також відповідне апаратне та програмне забезпечення, використовуване для їх огляду, відповідний процес можна умовно розділити на чотири види:

1) огляд стандартних ЗКТ носіїв та периферійних пристроїв;
2) огляд мобільних ЗКТ:
    - із функцією телефону;
    - автомобільних пристроїв;
3) огляд побутових ЗКТ («розумних речей»);
4) гляд інших ЗКТ.

Перед проведенням відповідного огляду важливо правильно підібрати інструментарій оглядача. При цьому слід пам'ятати, що швидкий розвиток технологій, а також велика кількість умов, які виникають під час огляду ЗКТ, з чисто практичної точки зору унеможливлюють так звану сертифікацію відповідних апаратних та/або програмних засобів. Це підтверджується і правозастосовною практикою провідних західних країн . В Україні така сертифікація також не проводиться, зважаючи на її недоречність. Так само в процесі огляду потрібно намагатися уникати використання програм, наявних у системі, що підлягає огляду, адже потім буде складно підтвердити правильність їх роботи.

Тому, враховуючи українське законодавство, видається правильним акцентувати увагу на двох важливих аспектах. По-перше, використовувані засоби мають бути з відповідною відкритою ліцензією або такими, що перебувають на балансі правоохоронного органу, аби можна було у будь-який час перевірити коректність їх роботи. По-друге, якщо використовується відкрите програмне забезпечення, наприклад, Live-CD під керуванням Linux, то відповідну копію із геш-сумою диску потрібно долучити у якості додатка до протоколу огляду.

Основні інструменти, які можуть знадобитися працівнику правоохоронних органів для огляду ЗКТ, є наступними: портативний комп'ютер з автономним джерелом живлення; привод CD-ROM (DVD-ROM); викрутки та інший інструмент; комплекти запасних батарей; диски з операційними системами та іншими програмними засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду, блокувач жорсткого диску та/або набір дублікаторів, польовий комплект експерта криміналіста тощо.

Взагалі, перелік інструментарію залежить від конкретної ситуації. У цьому сенсі, в процесі його підбору, вельми корисними стають регулярно оновлювані каталоги криміналістичних програмних та апаратно-програмних засобів. Наприклад, перелік криміналістичного програмного забезпечення, протестованого Американським інститутом стандартизації (NIST), можна зайти за адресою http://www.cftt.nist.gov.

Після підготовки відповідного інструментарію, який можна вважати підготовчим етапом огляду, проведення інших підготовчих заходів, працівники правоохоронного органу переходять до безпосередньо збирання даних на місці події. З урахуванням вивчення сучасної зарубіжної та вітчизняної практики і критичного осмислення даного матеріалу сам алгоритм огляду ЗКТ у загальному вигляді можна представити як на рис. 60.

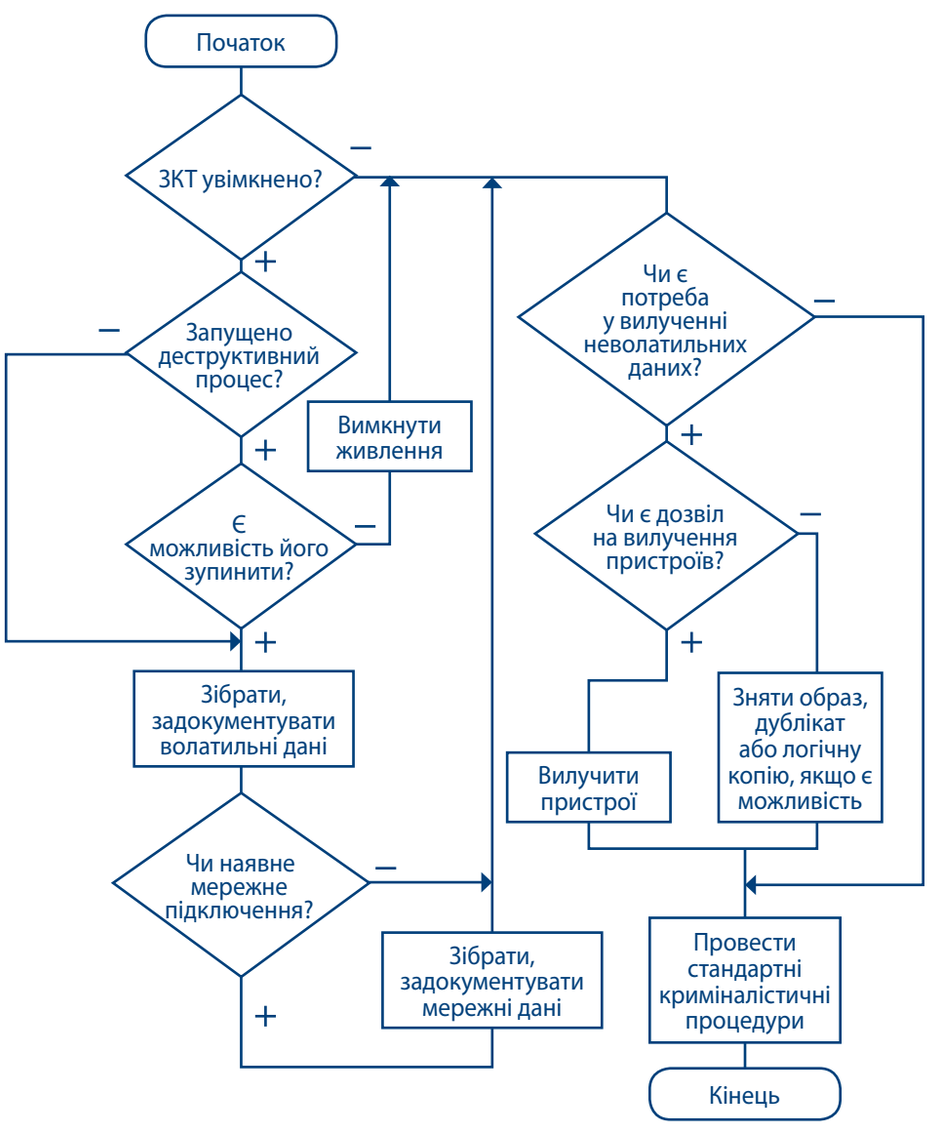



*Рис. 60. Загальний алгоритм техніки огляду ЗКТ*

Коментуючи окремі елементи цього алгоритму, потрібно зауважити, що на сьогодні в Україні практично не відбувається збирання та документування нестійких волатильних даних (зберігаються в енергозалежних запам'ятовувальних пристроях: оперативній пам'яті, кеші, регістрах), хоча саме волатильні дані часто містять ключі до різних криптоконтейнерів, останні повідомлення у мережі та відкриті документи тощо. Так само потрібно звернути увагу на мережні технології віддаленого зберігання даних (хмари, термінали тощо).

Щодо копіювання неволатильних даних, то на теперішній час в світі застосовується три головних способи одержання копій цифрових носіїв, що містять слідову інформацію:

1) створення образу відповідного носія;

2) створення дублікату носія;

3) логічне копіювання окремих даних.

Перший спосіб є більш повільним, водночас за його допомогою працівник правоохоронних органів одразу одержує готовий для дослідження програмними засобами матеріал, який можна достатньо легко тиражувати для здійснення розподіленого дослідження декількома фахівцями одночасно.

У будь-якому випадку для убезпечення електронних доказів рекомендується робити дві копії цифрового носія, одна з яких є контрольною (еталонною) та зберігається на випадок втрати або пошкодження іншої – робочої копії цифрового носія. Вилучені пристрої та носії потрібно належним чином зберігати та досліджувати. Наприклад, для дослідження мобільних пристроїв потрібно використовувати клітку Фарадея.

Перед зняттям копії більшості цифрових носіїв потрібно одержати геш-значення для вихідного носія інформації (джерела) за алгоритмом SHA-1, SHA-2 або SHA-3. Підрахунок гешу за допомогою алгоритму MD5 проводити не рекомендується, враховуючи можливості знаходження колізій з прийнятною обчислювальною складністю, що неодноразово демонструвалися дослідниками для цього алгоритму.

Слід пам'ятати, що особливості зберігання даних на окремих носіях (флеш-карти, SSD-вінчестери), а також вирівнювання ступеню їх зношеності, призводять до того, що посекторне геш-значення такого носія може не збігатися при наступному підрахунку. У цьому випадку можна говорити лише про можливість підтвердження геш-значеннями так званих «логічних» структур даних, наприклад, окремих файлів тощо.

Перед одержанням дублікату цифрового носія інформації (джерела) потрібно простерилізувати носій, на який будуть копіюватися відповідні дані (приймач). Цей носій, по перше, має бути за ємністю більшим від джерела, по друге, перед створенням дублікату його потрібно заздалегідь стерилізувати, тобто заповнити усі сектори нулями. Окремі дослідники пропонують лише частково стерилізувати носій вже після копіювання даних в частині, що незайнята скопійованими даними. Під час огляду стандартних ЗКТ провести процес стерилізації в операційній системі Windows можна, наприклад, за допомогою X-ways Forensics (Winhex). У Linux аналогічна процедура може бути виконана командами:

```
fdisk –l                # перегляд інформації про носії;
dd if=/dev/zero of=/dev/sd[a-z] bs 2048          # заповнення нулями відповідного носія;
killall -USR1 dd          # перевірка стану роботи процесу dd (вводиться в іншому терміналі).
```

Підтвердити перед понятими, що диск є дійсно стерилізованим, можна:

1) в операційній системі Windows за допомогою підрахунку контрольної суми (Cheksum – логічна сума за допомогою операції «або») в програмі X-ways Forensics (Winhex);

2) у Linux з використанням команди пошуку ненульових значень:

```
grep -a –v '0' /dev/sd[a-z]
# у квадратних дужках вказано обрання відповідної літери для диску приймача [77].
```

У загальному вигляді вилучені зразки комп'ютерної техніки передаються на дослідження експерту.

Базовими нормативно-правовими актами щодо проведення таких експертиз є Закон України «Про судову експертизу» від 25.02.1994 [78], Інструкція про призначення та проведення судових експертиз та експертних досліджень, а також Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджені Наказом Міністерства юстиції України № 53/5 від 08.10.1998 [79].

Для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій). Для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення.

СЛІД ПАМ'ЯТАТИ, ЩО ПРАВОПОРУШНИКИ НЕРІДКО ВДАЮТЬСЯ ДО ПРИХОВУВАННЯ СВОЄЇ ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ НЕ ЛИШЕ В КІБЕРПРОСТОРІ, АЛЕ Й В РЕАЛЬНОМУ СЕРЕДОВИЩІ. ЗОКРЕМА НОСІЇ З ВІДПОВІДНИМ ПРОТИПРАВНИМ КОНТЕНТОМ МОЖУТЬ ЗБЕРІГАТИСЯ В СТОРОННІХ РЕЧАХ (ІГРАШКАХ, КЛЮЧАХ, ПОДОВЖУВАЧАХ ТОЩО), А ТАКОЖ ПЕРИФЕРІЙНИХ ПРИСТРОЯХ (КЛАВІАТУРІ, МИШІ ТОЩО). ВКАЗАНІ ОСОБЛИВОСТІ СЛІД ВРАХОВУВАТИ ПІД ЧАС ЗДІЙСНЕННЯ ОГЛЯДУ ТА ПРИЙНЯТТЯ РІШЕННЯ ПРО ВИЛУЧЕННЯ ТИХ АБО ІНШИХ ПЕРДМЕТІВ.

Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду. Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація 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) в галузі комп'ютерної техніки.

ПРИБЛИЗНИЙ ПЕРЕЛІК ЗАПИТАНЬ ДЛЯ ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ:

1. ЧИ ВСТАНОВЛЕНО НА КОМП'ЮТЕРІ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБМІНУ МИТТЄВИМИ ІНТЕРНЕТ-ПОВІДОМЛЕННЯМИ (ICQ, SKYPE, VIBER, JABBER ТОЩО), А ТАКОЖ ПОВІДОМЛЕННЯМИ ЕЛЕКТРОННОЇ ПОШТИ, ЯКЩО ТАК, ТО ПРОШУ ЗАФІКСУВАТИ ЇХ ІСТОРІЮ?
2. ЯКИМИ Є МЕРЕЖНІ НАЛАШТУВАННЯ КОМП'ЮТЕРА (ЙОГО IP-АДРЕСА, ДОМЕННЕ ІМ'Я, МЕРЕЖНЕ МАРКУВАННЯ)?
3. ЯКА ІСТОРІЯ ВІДВІДУВАННЯ ВЕБ-САЙТІВ ІЗ ВКАЗАНОГО КОМП'ЮТЕРА?
4. ЧИ ЗДІЙСНЮВАВСЯ ДОСТУП З ДОСЛІДЖУВАНОГО КОМП'ЮТЕРА ДО ІНТЕРНЕТ-САЙТУ WWW._____.UA?
5. ЧИ ВСТАНОВЛЕНО НА КОМП'ЮТЕРІ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАВАНТАЖЕННЯ ФАЙЛІВ ЧЕРЕЗ ПІРИНГОВІ МЕРЕЖІ, ЯКЩО ТАК, ТО ЗАФІКСУВАТИ ЙОГО ІСТОРІЮ?
6. ДО ЯКИХ ОБЛІКОВИХ ЗАПИСІВ, ЯКИХ СОЦІАЛЬНИХ МЕРЕЖ ЧИ САЙТІВ ЗДІЙСНЮВАВ ДОСТУП КОРИСТУВАЧ (КОРИСТУВАЧІ) ВКАЗАНОГО КОМП'ЮТЕРА?
7. ЧИ ЗДІЙСНЮВАЛАСЯ АВТОРИЗАЦІЯ КОРИСТУВАЧІВ ІЗ ВКАЗАНОГО КОМП'ЮТЕРА НА ІНТЕРНЕТ-САЙТІ WWW._____.UA, ЯКЩО ТАК, ТО КОЛИ І З ВИКОРИСТАННЯМ ЯКОГО (ЯКИХ) ОБЛІКОВИХ ЗАПИСІВ?
8. ЧИ МІСТИТЬСЯ НА КОМП'ЮТЕРІ ІНФОРМАЦІЯ ЩОДО КЛЮЧОВИХ СЛІВ «_____»,«_____»,«_____», ЯКЩО ТАК, ТО ЯКИЙ ЇЇ ЗМІСТ?
9. ЯКОЮ Є НАЗВА ОБЛІКОВОГО ЗАПИСУ КОРИСТУВАЧА ВКАЗАНОГО КОМП'ЮТЕРА?
10. 10. ЧИ МІСТИТЬСЯ НА ЖОРСТКИХ ДИСКАХ ВКАЗАНОГО КОМП'ЮТЕРА ПРОДУКЦІЯ ПОРНОГРАФІЧНОГО ХАРАКТЕРУ, У ТОМУ ЧИСЛІ ВИГОТОВЛЕНА ЗА УЧАСТЮ ДІТЕЙ?

В окремих випадках слідчий або оперативний працівник за його дорученням може самостійно провести огляд засобів комп'ютерної техніки зі складанням протоколу огляду речей. У загальному вигляді такий огляд з урахуванням певних міркувань [80] можна представити так:

1. Аналіз даних, одержаних з оперативних запам'ятовуючих областей, в тому числі буферу обміну
2. Аналіз залишкових слідів в елементах ОС, які вказують на дані, що оброблювались системою:
   *2.1. дослідження використовуваного програмного забезпечення;*
   *2.2. дослідження елементів системних файлів;*
   *2.3. дослідження та перевірка назв і реквізитів ярликів;*
   *2.4. дослідження файлів історій відповідних програмних засобів;*
   *2.5. дослідження налаштувань Інтернет-браузерів;*
   *2.6. дослідження атрибутів та метаданих файлів, що викликали інтерес під час перевірки.*
3. Аналіз безпосередньо файлів з даними, шляхом контекстного пошуку за ключовими фразами:
   *3.1. дослідження файлів, які зберігаються на цифрових носіях, зокрема:*
      *3.1.1. пошук прихованих та зашифрованих даних;*
      *3.1.2. пошук та перевірка тимчасових файлів;*
      *3.1.3. аналіз специфічних даних, передбачених структурою файлової системи, наприклад, альтернативних потоків даних;*
      *3.1.4. аналіз файлів, що пов'язані з мережною активністю;*
   *3.2. відновлення з послідуючим аналізом видалених файлів, в тому числі:*
      *3.2.1. дослідження залишків файлів в кластерах;*
      *3.2.2. перевірка вільного простору носіїв інформації;*
      *3.2.3. перевірка файлів підкачки, якщо вони мають місце.*

Для аналізу зображень, які завантажено з мережних ресурсів, асоційованих із торговцями людьми, до проведення відповідної експертизи працівникам правоохоронних органів можна застосовувати відповідні сервіси, наприклад, безкоштовний сервіс imageforensic.org.

Завантаживши до нього відповідне зображення можна оперативно дізнатися важливі дані про нього (рис. 61), які можуть вказати на особу автора зображення, дату його створення, програмне забезпечення, яке використовувалося для редагування, тощо.


*Рис. 61. Фрагмент звіту про результати аналізу зображення*

На теперішній час в правоохоронних органах існує серйозна проблема проведення експертних досліджень електронних доказів у розумні строки. Недостатня кількість експертів, які мають право проводити комп'ютерно-технічні експертизи, сприяє створенню кількамісячних, а у деяких випадках кількарічних черг на проведення означеного виду експертиз. З урахуванням наведеного вбачається доречним розширення практики дослідження відповідних електронних доказів безпосередньо слідчим із залученням спеціаліста (за необхідності) з подальшим оформленням проведеного дослідження протоколом огляду. Така практика вже існує в регіонах, проте вона все ще не є поширеною, зважаючи на недостатні знання слідчих (у переважній більшості) в сфері інформаційних технологій.

**ЗАВДАННЯ**

**ОЗНАЙОМТЕСЬ ІЗ НАВЕДЕНИМ ПРОГРАМНИМИ ЗАСОБАМИ. ЗДІЙСНІТЬ ОГЛЯД ВЛАСНОГО КОМП'ЮТЕРА ІЗ ПОШУКОМ ІНФОРМАЦІЇ ЗА КЛЮЧОВИМИ СЛОВАМИ. ЗАВАНТАЖТЕ ІЗ СОЦІАЛЬНОЇ МЕРЕЖІ ФОТОГРАФІЮ БУДЬ-ЯКОЇ ОСОБИ. СПРОБУЙТЕ ВСТАНОВИТИ ВІДОМОСТІ ПРО ЇЇ МІСЦЕ СТВОРЕННЯ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЯКЕ ДЛЯ ЦЬОГО ЗАСТОСОВУВАЛОСЬ**

## 3. ПОШУК І ВИЛУЧЕННЯ КОМП'ЮТЕРНИХ ДАНИХ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

З огляду на важливість отримання волатильних або енергозалежних даних розглянемо цей процес більш детально. Якщо на місці огляду виявлено включені ЗКТ, то необхідно провести вилучення даних в режимі реального часу. Раніше в такій ситуації радили «витягнути шнур живлення із розетки», але вимикання живлення може призвести до втрати цінних для розслідування енергозалежних (волатильних) даних, розірвання віддалених з'єднань, блокування тимчасово розшифрованих і відкритих файлів, тому доцільно проводити збір даних в режимі реального часу.

Оскільки імовірність зміни і навіть перезапису джерел доказів дуже висока. то спеціаліст з криміналістичного аналізу «живих» даних або слідчий повинні мати:

- достатній рівень технічних знань і умінь;
- знання і досвід правильного застосування алгоритмів пошуку і вилучення із мінімальним впливом на систему;
- спеціальний набір перевірених криміналістичних інструментів.

Дуже важливим у процедурі пошуку і вилученн комп'ютерних даних в режимі реального часу є фіксація часу здійснення своїх дій. Якщо на місці огляду немає спеціаліста, то іноді буде кращим знеструмити систему і втратити енергозалежні дані, ніж спотворити джерела доказів, намагаючись їх вилучити із системи без відповідного досвіду і навичок.

### ЕНЕРГОЗАЛЕЖНІ ДАНІ

Під терміном «енергозалежні дані» розуміються *цифрові дані, щодо яких існує дуже висока ймовірність того, що в короткий проміжок часу вони будуть видалені, перезаписані або змінені внаслідок людського або автоматичного втручання.*

Енергозалежні дані дуже нестійкі у часі, і якщо їх не зберегти правильно і швидко, то вони можуть бути втрачені. В сучасних комп'ютерних системах дані часто зберігаються і обробляються не на самому пристрої, а в інших місцях (наприклад, хмарні сховища), доступ до яких регулюється законодавством тієї країни, де вони фізично розташовані.

Розрізняють такі види енергозалежних даних:

1. *Енергозалежні дані комп'ютерної системи*, наприклад, відкриті мережні з'єднання, запущені процеси, кеш ARP[1] і кеш DNS[2].
2. *Тимчасові дані*, які самі по собі не є енергозалежними, але доступ до них можна отримати тільки на місці огляду, наприклад зашифровані томи і віддалені ресурси. Якщо не отримати до них доступ під час огляду, то вони можуть стати недоступними, зміненими або видаленими.

У енергозалежній пам'яті можуть знаходитися такі дані:

- процеси, що виконуються;
- сервіси, які запущені;
- системна інформація;
- дані про користувачів, які знаходяться в системі;
- логічні порти, що відкриті і прослуховуються;
- кеш ARP (протокол визначення адреси);
- кеш DNS (доменна системи імен);
- інформація про застосування, що автоматично запускаються;
- інформація з реєстру, яка  не записана на диск;
- незбережені документи;
- бінарні процеси і сервіси, в тому числі шкідливі програми, які зберігаються тільки в пам'яті.

Для збереження енергозалежних даних правоохоронним органам потрібно:

- визначити, вилучити, описати і сфотографувати кожен пристрій, що містить енергозалежні дані;
- ізолювати підозрюваних та інших сторонніх осіб від ЗКТ і не допустити, щоб вони змінили або знищили докази;
- спостерігати за складовими ЗКТ і запобігати будь-який автоматичній зміні або знищенню доказів.

## ФІЗИЧНИЙ ДОСТУП

В процесі огляду часто складно визначити стан живлення комп'ютера (включений/виключений). Нижче наведено кілька додаткових порад на цей випадок:

- сфотографуйте комп'ютер, щоб зафіксувати його стан;
- прислухайтеся і придивіться до системи, щоб визначити, чи включений комп'ютер: це можна дізнатися по звуку працюючого вентилятора або обертів дисків, по палаючим світлодіодним індикаторам;
- посовайте мишкою, але не натискайте на кнопки;
- подивіться, чи виводиться на екран заставка або запит на введення логіна для входу в систему;
- сфотографуйте екран, щоб зафіксувати його стан після ваших маніпуляцій.

Із Керівництва з питань електронних доказів можна запропонувати початковий алгоритм огляду комп'ютера (рис. 62).

[1] Протокол визначення адреси (Address Resolution Protocol, скор. ARP) – загальноприйняті правила і стандарти перетворення IP-адреси на адресу конкретного пристрою, за рахунок чого повідомлення в мережі направляються туди, куди потрібно.

[2] Доменна система імен (Domain Name System, скор. DNS) – база даних, за допомогою якої доменні імена перетворюються в IP-адресу.

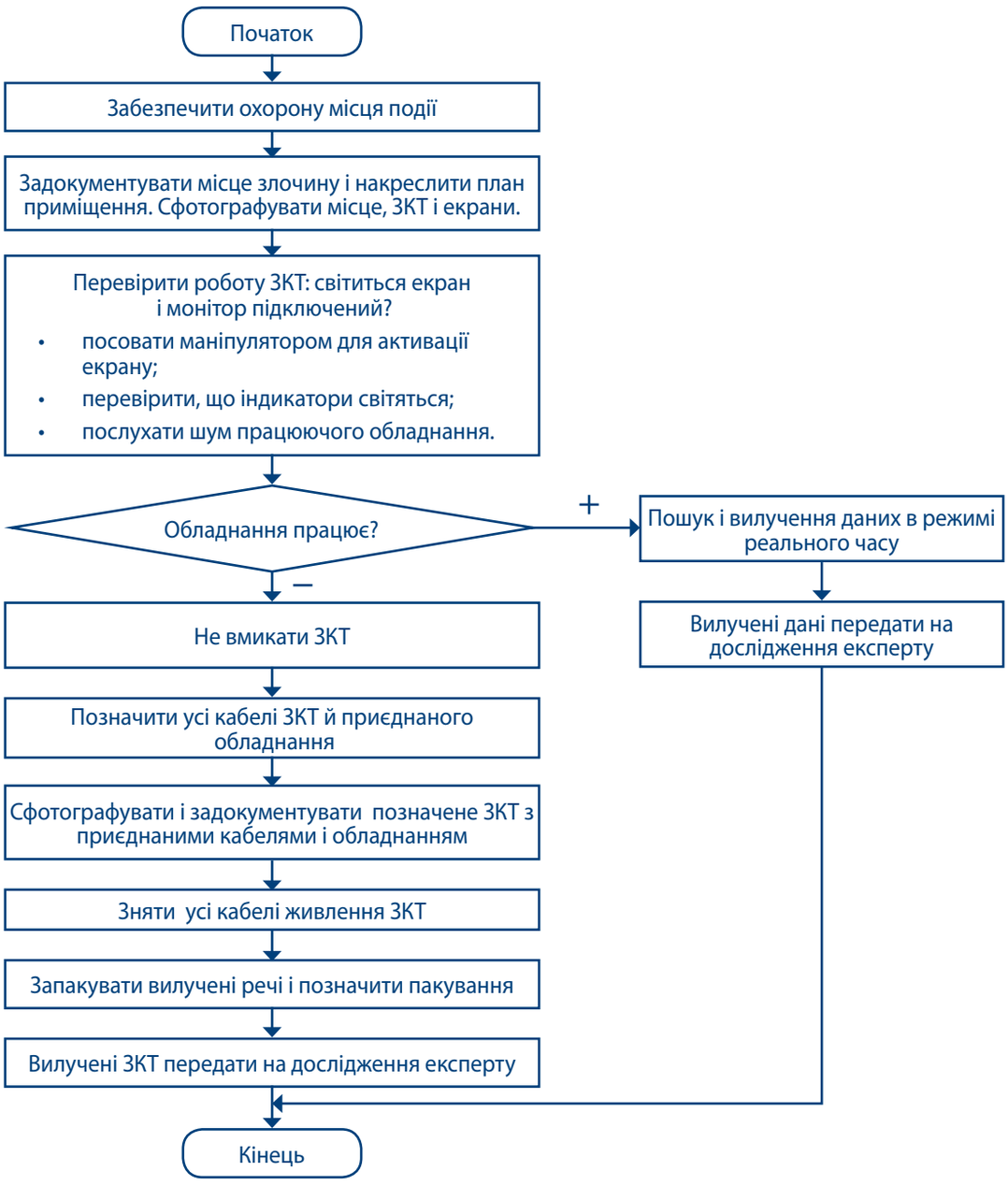



*Рис. 62. Початковий алгоритм огляду комп'ютера*

Якщо виявилося, що комп'ютер включений і на екрані видна заставка, то необхідно:

- спостерігати, що відбувається з екраном під час руху мишки;
- якщо заставка зникла і ви отримали доступ до системи без паролю, то можна переходити до наступних кроків пошуку і вилучення даних в режимі реального часу (за умови, що у вас є необхідні знання та повноваження);
- якщо система вимагає введення пароля, то опитайте володільця системи; перевірте, чи відображається на екрані підказка паролю; пошукайте папірці з паролем або інші об'єкти, які допоможуть дізнатися пароль.
- якщо вдалося отримати пароль, то увійдіть в систему і переходьте до наступних кроків;
- якщо не вдалося отримати пароль, то існують спеціальні техніки отримання доступу до оперативної пам'яті через інтерфейси FireWire, Thunderbolt або шляхом «холодного перезавантаження» («cold boot»);
- у будь-якому випадку необхідно сфотографувати екран, щоб зафіксувати його стан.

Якщо комп'ютер увімкнений, але на екрані немає заставки/запиту на введення пароля або ж вдалося отримати пароль, то потрібно час від часу рухати мишкою (щоб не допустити активації заставки/блокування екрану) і візуально шукати ознаки:

- знищення даних: слова «delete» («знищити»), «format» («форматувати»), «remove» («видалити»), «copy» («копіювати»), «move» («перемістити»), «cut» («вирізати») або «wipe» («стерти»);
- шифрування;
- входу в систему з віддаленого комп'ютера або пристрою;
- використання хмарних сервісів;
- активного або нерозірваного сеансу спілкування з іншими користувачами або комп'ютерами (це може бути вікно чату або програми для обміну миттєвими повідомленнями);
- роботи камери або веб-камери;
- включених віртуальних машин (можливо в повноекранному режимі).

У будь-якому випадку сфотографуйте екран, щоб зафіксувати його стан.

При зборі комп'ютерних даних в режимі реального часу зміни в системі неминучі, проте потрібно намагатися отримати якомога більше енергозалежних даних, залишивши при цьому якомога менше слідів. Важливе значення має також і те, в якому порядку здійснюється збір даних, тому необхідно ретельно обміркувати відповідний план дій, де рекомендується застосовувати методи, в основі яких лежить ступінь енергозалежності даних. Для цього доцільно використовувати вже готові сценарії збору даних в режимі реального часу, які можна адаптувати для кожного окремого випадку розслідування, наприклад, флеш-накопичувач Microsoft COFEE (поширюється через Інтерпол) містить такі сценарії.

В Табл. 5 [81] наведений перелік інструментів для збору енергозалежних даних.

*Таблиця 5. Перелік інструментів для збору енергозалежних даних*

| Енергозалежний фрагмент | Інструменти Windows | Інструменти Linux |
|---|---|---|
| Зміст оперативної пам'яті (RAM) | Dumpit, Winen, Mdd | dd, fmem |
| Таблиця маршрутизації, кеш ARP, статистика ядра | Route PRINT, arp -a, netstat | netstat -r -n, route, arp -a |
| Кеш DNS | Ipconfig / displaydns | rndc dumpdb (if installed) |
| Списки процесів | PsList, ListDLLs, CurrProcess, tasklist | ps -ef, lsof |
| Активні мережні з'єднання (сокети) | netstat –a | netstat -a, ifconfig |
| Програми/сервіси, що використовують мережні з'єднання | sc queryex, netstat -ab | netstat -tunp |
| Відкриті файли | Handle, PsFile, Openfiles, net file | lsof, fuser |
| Загальні мережні ресурси | Net share, Dumpsec | showmount -e, showmount -a smbclient -L |
| Відкриті порти | OpenPorts, ports, netstat -an | netstat -an, lsof |
| Авторизовані користувачі | Psloggedon, whoami, ntlast, netusers /l | w, who -T, last |
| Шифрована файлова система | Manage-bde (Bitlocker), efsinfo (EFS) | mount -v, ls /media |
| Тимчасово приєднані файлові системи | Fsinfo, reg (Mounted Devices) | mount -v, ls /media |

| Енергозалежний фрагмент | Інструменти Windows | Інструменти Linux |
|---|---|---|
| Віддалена авторизація та контроль даних | psloglist | /etc/syslog.conf Port UDP 514 |
| Фізична конфігурація, топологія мережі | Systeminfo, msinfo32, ipconfig /all | ifconfig -a netstat -in |
| Носії пам'яті | reg (Mounted Devices), Net share, netstat -a | mount -v, ls /media |
| Системний годинник (для синхронізації з сервісами точного часу) | time /T, date /T, uptime | time, date, uptime |
| Змінні оточення | cmd /c set | env, set |
| Буфер обміну | Pclip | |
| Дані, що зберігаються на дисках | FTK Imager, EnCase, Tableau Imager | Dc3dd, ewfacquire, Guymager |

Різноманітні інструменти збору енергозалежних даних для ОС Windows містяться у безкоштовних пакетах:

- Sysinternals, https://docs.microsoft.com/uk-ua/sysinternals/;
- LiveGator (http://orionforensics.com/w_en_page/livegator.php);
- Redline (https://www.fireeye.com/services/freeware/redline.html);
- Win-UFO (http://www.caine-live.net/page2/page2.html);
- DART (http://na.mirror.garr.it/mirrors/deft/dart/DART_v2-2014.7z);
- OSForensics (http://www.osforensics.com/download.html),

а для ОС Linux у спеціальних Live-DVD дистрибутивах:

- Caine Live-DVD with Win-UFO, http://www.caine-live.net/;
- DEFT Live-DVD with DART, http://www.deftlinux.net//.

При виборі програм вилучення живих комп'ютерних даних необхідно враховувати наступне:

- віддавати перевагу програмам із мінімальним розміром файлів;
- програми повинні мати власні виконувані файли і не використовувати файли системи, що оглядається;
- вибирати програми із сценаріями автоматизації;
- бажано, щоб програми мали функцію сортування даних;
- програми повинні збирати виключно енергозалежні дані.

Зібрані енергозалежні дані слід зберігати на підготовлених стерилізованих (усі сектори перед форматуванням заповнюються нулями) зовнішніх носіях. При підготовці програм і пристроїв, які будуть використовуватися для вилучення живих комп'ютерних даних, доцільно виконати наступне:

- підготувати носії з достатнім місцем для запису даних в декількох форматах, наприклад, NTFS, EXT4;
- бути готовим працювати з різними операційними системами, наприклад, Windows, Mac і Linux;
- перевірити наявність працездатного носія із довіреними програмами збору живих даних та обчислити і зафіксувати для цих програм геш-значення за алгоритмом SHA-1 або SHA-2.

**ШИФРУВАННЯ**

При зборі комп'ютерних даних в режимі реального часу дуже важливим аспектом є недопущення активації шифрування даних або виявлення вже запущених процесів шифрування.

Доцільно почати огляд із пошуку видимих ознак використання шифрувальних програм, а саме наявності іконок шифрувального програмного забезпечення на панелі завдань або на робочому столі. До найбільш розповсюджених можна віднести програми Microsoft Bitlocker, Truecrypt, VeraCrypt, Steganos, GnuPG.

Ознаки шифрувальної програми можуть проявитися в запущених процесах, діалогових вікнах програм, реєстрах (наприклад, в реєстрі змонтованих пристроїв, встановлених програм або пов'язаних файлових розширень), а також у провіднику Windows (рис. 63).


*Рис. 63. Диск в провіднику Windows, зашифрований за допомогою програми Microsoft Bitlocker*

Для Microsoft Bitlocker інформацію про змонтовані зашифровані диски можна отримати за допомогою введення наступної команди із командного рядка з правами адміністратора:

> manage-BDE -status

При виявленні ознак шифрування рекомендується виконати наступні дії:

- при виявленні процесу монтування зашифрованих дисків або контейнерів скопіюйте їх в режимі реального часу поки є доступ до системи;
- якщо в Bitlocker відбувається монтування зашифрованого тому, то збережіть 48-значний ключ відновлення за допомогою команди:

> manage-BDE -protectors -get <volume name>

і після цього скопіюйте файли;

- при виявленні в системі зашифрованих, але не змонтованих, томів або сховищ спробуйте дізнайтеся у підозрюваного пароль або ключ відновлення і порядок розшифрування;
- якщо підозрюваний надав необхідну інформацію, розшифруйте дані і скопіюйте їх;
- передбачте, щоб включення заставки/енергозберігаючого режиму або низький заряд батареї не завадив зберегти зашифровані файли.

Успіх розшифрування залежить не тільки від знання паролю, а і наявності вбудованих в пристрій апаратних криптографічних модулів, наприклад, чіпу TPM (Trusted Platform Module), для яких потрібні додаткові файли ключів, що можуть зберігатися як в самій системі, так і на зовнішніх носіях (наприклад, в USB-ключі). Тому важливо зібрати всі джерела доказів, виявлених на місці огляду.

При використанні функції повного шифрування диска в TrueCrypt і VeraCrypt жорсткий диск може виявитися розділеним на дві частини з двома окремими паролями. Перша частина не містить ніякої важливої інформації і може бути відкрита під тиском, а друга частина є прихованою із важливою для користувача інформацією.

## ВІДДАЛЕНИЙ ДОСТУП

Разом із фіксацією енергозалежних даних працюючого комп'ютеру перевіряється наявність віддаленого доступу, при якому данні фізично зберігаються в інших віддалених місцях. Наприклад, в організаціях дані користувача можуть розміщуватися (зберігатися) централізовано на одному загальному сервері, який забезпечує роботу всіх робочих станцій мережі. Зазвичай зупинити сервер великої організації і вилучити обладнання не представляється можливим внаслідок операційних обмежень або цивільно-правових ризиків. Як правило, дозвіл на обшук поширюється тільки на ті дані, які належать підозрюваному або до яких у нього є доступ, тому слідчий не має відповідних повноважень вилучити дані з усього сервера або загальної мережі.

У таких випадках для отримання доступу до інформації організації рекомендується під час обшуку організувати зустріч з її керівником, представниками юридичного та IT-департаменту, де обговорити детальний план співпраці між усіма сторонами процесу.

Комп'ютерні мережі в будинках/квартирах або в офісах малих/середніх компаній, як правило, складаються з декількох індивідуальних комп'ютерів, загального сервера, який містить: бази даних бухгалтерського програмного забезпечення, настройки мережних ресурсів, домашні каталоги користувачів, і іноді є поштові сервери. У подібній ситуації потрібно налагодити співпрацю із відповідальним за комп'ютерну інфраструктуру організації (якщо він не перейшов в статус підозрюваного).

Інформацію про конфігурацію мережі можна отримати із списків контролю доступу (ACL) або набору правил безпеки[3] маршрутизатора і брандмауера. Для цього потрібно знати логіни і паролі та через адміністративний доступ подивитися відповідні настройки конфігурації. Також конфігурацію мережі можна встановити за допомогою мережних утиліт Live-DVD криміналістичних дистрибутивів. Не зайвим буде намалювати схему мережної інфраструктури, що допоможе побачити зв'язки між досліджуваним комп'ютером і іншою мережею.

Ознаками віддаленого зберігання даних є:

- каталоги спільного доступ на інших комп'ютерах мережі;
- підключені мережні диски з сервера;
- електронні листи зберігаються на поштових серверах IMAP або Exchange Server);
- використовуються хмарні сервіси і хмарні сховища.

Каталоги зі спільним доступом  і підключені мережні диски можна подивитися через провідник Windows або безкоштовні інструменти ShareEnum від Sysinternals. При їх наявності потрібно створити образ (точна копія із видаленими файлами і зарезервованим простором) диску пам'яті віддаленого пристрою.

Факт віддаленого розташування електронних повідомлень на сервері IMAP[4] або Exchange Server, можна встановити шляхом аналізу параметрів облікових записів відповідних поштових клієнтів. Дані облікових записів POP3 (а іноді і облікових записів IMAP) зберігаються на комп'ютері користувача, не є енергозалежними та не вимагають вилучення в режимі реального часу. Якщо листи  на комп'ютері користувача відсутні, то можна спробувати їх завантажити безпосередньо із сервера Exchange Server або попросити про це хостинг-провайдера облікового запису.

## ХМАРНІ ТЕХНОЛОГІЇ

Важливою особливістю хмарних сервісів є те, що дані зберігаються на віддаленому сервері і часто навіть самому постачальнику хмарного сервісу не просто визначити їх конкретне місце розташування. Хмарні сервіси можуть замінити практично будь-який елемент корпоративної IT-інфраструктури – від текстових редакторів і бухгалтерських програм до повної заміни всіх робочих станцій.

[3] Правила, що регулюють безпеку мережі і діапазон її використання

[4] Протокол доступу до електронної пошти (Internet Message Access Protocol, скор. IMAP)

Це означає, що в деяких випадках з офісного комп'ютера не вийде вилучити інформацію, оскільки він є «тонким клієнтом», тобто не має власного жорсткого диску пам'яті і використовує ресурси віртуальної машини хмари. У цій ситуації є свої переваги: технічно процес копіювання віртуальної машини провайдера хмарного сервісу дуже простий, але можуть виникнути складнощі із отриманням дозволом на вилучення даних – це залежить від відповідного законодавства країни, де розміщуються дані. Крім того, може бути непросто довести, що процедура отримання даних не порушує законодавство запитуючої сторони.

Ще одна проблема полягає в тому, що дані можуть бути безповоротно втрачені, коли підозрюваний створив віртуальну машину спеціально для вчинення злочину, а після видалив її.

Якщо при огляді комп'ютеру, який має з'єднання із мережею, виникли підозри у використанні хмарних сервісів, то доцільно виконати наступні рекомендації:

- здійсніть пошук ярликів відомих сервісів хмарних технологій на панелі завдань;
- перевірте у настроюваннях системи встановлені програми хмарних сервісів;
- перегляньте назви хмарних сервісів в списку запущених процесів;
- здійсніть пошук загальних каталогів і підключених мережних дисків;
- за допомогою аналізатора протоколів пошукайте в мережі пакети хмарних сервісів;
- перевірте список відкритих портів на предмет підозрілої активності;
- скопіюйте всі дані із віддалених ресурсів незалежно від наявності можливої встановленої синхронізації даних із жорстким диском комп'ютера.

Після завершення вилучення енергозалежних і тимчасових даних потрібно:

- вийняти кабель живлення із пристрою (не із розетки, оскільки може бути встановлено джерело безперебійного живлення) і записати час, коли це було зроблено;
- при наявності підключених змінних носіїв пам'яті вийняти їх, запакувати і підписати;
- фізично від'єднати модем.
- у портативного комп'ютеру вийняти акумуляторну батарею живлення (іноді у відсіку DVD-приводу встановлюють додаткову батарею).

## ВІДДАЛЕНЕ АДМІНІСТРУВАННЯ

Віддалені мережні ресурси організації можуть управлятися зовнішніми компаніями-підрядниками як українськими, та і закордонними. В такому випадку важливим є налагодити співпрацю з віддаленим системним адміністратором. Якщо немає можливості оперативного виїзду до компанії-підрядника, то можна спробувати встановити віддалений контакт із керівництвом компанії-підрядника для обговорення можливості юридично обґрунтованого залучення до співпраці їх системного адміністратора (якщо він не є підозрюваним).

В даному випадку «співпраця» не означає зобов'язання адміністратора збирати докази. Доступ адміністратора до системи повинен бути мінімальним, а пошук і вилучення доказів є завданням слідчих. Співпраця з боку адміністратора обмежується тим, що він надає інформацію про інфраструктуру і права доступу до певних ділянок сервера, комп'ютера або функцій програмного забезпечення.

У великих закордонних компаніях, що надають послуги віддаленого адміністрування мережними ресурсами, можуть бути встановлені системи e-discovery (системи виявлення електронних даних), тому є сенс, у випадку згоди на співпрацю, запитати про наявність такої системи і її віддаленого використання, що дозволить здійснити прихований віддалений пошук і доступ до отримання даних (в тому числі і енергозалежних) підозрюваного.

## 4. ОГЛЯД МОБІЛЬНИХ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ ІЗ ФУНКЦІЄЮ ТЕЛЕФОНУ

Враховуючи широке використання засобів мобільного зв'язку і можливостей мобільних телефонів по зберіганню та обробці інформації все більш важливим завданням для правоохоронних органів стає аналіз вмісту мобільних телефонів тих осіб, які підозрюються у вчиненні кримінальних правопорушень. Дійсно, адже сучасний мобільний телефон – це фактично маленький комп'ютер, який об'єднує в собі багато різних функцій, серед яких:

- телефонна та адресна книги;
- щоденник зі списком зустрічей і справ;
- пристрій для обміну повідомленнями (SMS, MMS, E-mail);
- записна книжка;
- диктофон;
- фотоапарат та відеокамера;
- програвач мультимедіа
- і багато інших функцій, включаючи власне здійснення та отримання дзвінків.

Усі перераховані вище дані можуть містити або орієнтуючу інформацію для правоохоронних органів, або доказову інформацію та сліди, що можуть бути проаналізовані за наявності відповідного інструментарію.

Непоодинокими є випадки, коли за допомогою аналітичної обробки даних з мобільних пристроїв вдавалося розкривати неочевидні злочини або злочини минулих років, кількість яких з кожним роком невпинно збільшується.

Слід також зауважити, що зроблені за допомогою сучасних мобільних пристроїв (наприклад, iPhone) фотографії з працюючим функціоналом GPS нерідко містять в собі інформацію про координати місця фотографування, що дозволяє в окремих випадках з'ясувати місцезнаходження шуканої особи.

Більше того у практиці правоохоронних органів траплялися випадки, коли за локалізацією даних з мобільних апаратів вдавалося знаходити викрадене майно, відшукувати безвісти зниклих дітей.

Усе це дає підстави говорити про існуючу потребу більш інтенсивного використання спеціалізованого програмного забезпечення для аналізу інформації з мобільних пристроїв правоохоронними органами України.

Серед таких програм варто відзначити Mobile Phone Examiner Plus (MPE+), яка легко інтегрується з Forensic Toolkit (FTK), «Мобильный Криминалист» від розробника ЗАТ «Оксиджен Софтвер», яка дозволяє серед іншого відновлювати окремі видалені повідомлення, MOBILedit! від розробника COMPELSON Labs, криміналістичний програмний продукт XRY шведської компанії Micro Systemation.

Здебільшого названі програмні продукти використовують у своїй діяльності експертні служби, але є потреба у їх засвоєнні не лише спеціалістами вузького профілю, але й більшістю слідчих та оперативних працівників [82].

Огляд мобільних ЗКТ має свої особливості. Найбільш складним елементом у цьому процесі є зняття дампу даних мобільного пристрою, оскільки для цього потрібно мати спеціальні права доступу до нього. Дамп, як правило, знімається програмним шляхом, проте окремі апаратно-програмні комплекси дозволяють проводити зняття фізичного дампу пристроїв безпосередньо з відповідних чіпів (наприклад, UFED, XRY). В окремих випадках корисну допомогу в дослідженні мобільних пристроїв можуть надати фахівці Європолу.

Вказана співпраця здійснюється в рамках Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 [83], ратифікованою відповідним Законом України

№ 2129-VIII від 12.07.2017. Серед іншого згідно зі ст. 18 вказаної Угоди Україна і Європол пропонують одна одному надання підтримки у створенні та функціонуванні спільних слідчих груп.

У рамках протидії торгівлі людьми може виникнути потреба в огляді мобільних пристроїв як жертв злочину, так і суб'єктів його вчинення. У рамках кримінального провадження результати огляду можна оформити протоколом огляду речей. Для огляду бажано залучити спеціаліста.

**ЗАВДАННЯ**

**1) ЗАПИШІТЬ ВСЮ МОЖЛИВУ ІНФОРМАЦІЮ ПРО МЕРЕЖУ, ЯКУ ВИКОРИСТОВУЄ МП;**

**2) ВСТАНОВІТЬ ГРУПУ ТЕЛЕФОННИХ НОМЕРІВ, ЯКИМ ВЛАСНИК ТЕЛЕФОНУВАВ ЗА ОСТАННІЙ ТИЖДЕНЬ;**

**3) ВСТАНОВІТЬ ВСІ КОНТАКТИ, ТЕЛЕФОНИ В ЯКИХ ПОЧИНАЮТЬСЯ НА КОМБІНАЦІЮ ЦИФР 095;**

**4) ВИКОРИСТОВУЮЧИ ПОШУК, ЗНАЙДІТЬ ВСІ ФАЙЛИ, ЯКІ МІСТЯТЬ СЛОВА «ПОРНО, ІНТИМ, ХХХ»;**

**5) ВСТАНОВІТЬ, ЯКІ САЙТИ У МЕРЕЖІ ІНТЕРНЕТ ВІДВІДУВАВ ВЛАСНИК ЗА ОСТАННІЙ МІСЯЦЬ;**

**6) ПРОАНАЛІЗУЙТЕ ВСІ ДОКУМЕНТИ У ФОРМАТІ .TXT;**

**7) ЗНАЙДІТЬ ВСЮ МОЖЛИВУ ІНФОРМАЦІЮ ПРО АБОНЕНТІВ, ЯКІ МАЮТЬ РОДИННІ ЗВ'ЯЗКИ З ВЛАСНИКОМ (ВИКОРИСТОВУЙТЕ КЛЮЧОВІ СЛОВА ТИПУ «БАТЬКО, БРАТ, СЕСТРА» ТОЩО);**

**8) ВСТАНОВІТЬ 10 ОСТАННІХ ДІЙ, ЩО БУЛИ ВИКОНАНІ З ТЕЛЕФОНОМ (ДЗВІНКИ, SMS ТОЩО);**

**9) ЗНАЙДІТЬ ВСІ SMS-ПОВІДОМЛЕННЯ, ЩО БУЛИ ВИДАЛЕНІ З ТЕЛЕФОНУ;**

**10) ЗНАЙДІТЬ ТА ПРОАНАЛІЗУЙТЕ СПИСОК ЗАВДАНЬ, ЯКІ ПЕРЕД СОБОЮ СТАВИВ ВЛАСНИК ТЕЛЕФОНУ;**

**11) ВИЗНАЧТЕ АДРЕСИ (ЯКЩО МОЖЛИВО) ОСІБ В КОНТАКТАХ, ТЕЛЕФОНИ ЯКИХ МІСТЯТЬ КОМБІНАЦІЮ ЦИФР 837;**

**12) ЗНАЙДІТЬ ВСІ ВІДЕОФАЙЛИ, ЩО ЗБЕРЕЖЕНІ У ТЕЛЕФОНІ.**

Одним з джерел доказової інформації можуть бути автомобільні засоби комп'ютерної техніки. Для їх дослідження використовується спеціальне програмне забезпечення, наприклад, **iVe** (https://www.berla.co/ive.html).

Правоохоронні органи США дослідження бортових комп'ютерів автомобілів часто здійснюють за допомогою спеціального програмного забезпечення, одержаного у рамках взаємодії з компаніями Дженерал Моторс, Додж та Форд.

Професійні зловмисники нерідко для приховування своєї діяльності застосовують засоби шифрування. Відтак на вилучених правоохоронцями пристроях можуть міститися зашифровані дані.

Процес їх **розшифрування** може бути доволі складним та тривалим. Для ефективного вирішення означеного завдання працівникам правоохоронних органів слід звернути увагу на наступне:

- у перші хвилини після оголошення обшуку, користуючись розгубленістю фігурантів, найлегше одержати від них відомості про облікові записи та паролі доступу;
- для формування словника, з якого підбиратимуться паролі доступу, потрібно створити профіль відповідної особи, з урахуванням якого скласти Словник 1. Для формування такого профілю та словника може стати в нагоді програма CUPP (github.com/Mebus/cupp). Словник 2 складається з проіндексованих слів текстових документів, які зберігаються на вилучених під час обшуку засобах комп'ютерної техніки.

**МОДУЛЬ 7**

# МЕТОДИ І ФОРМИ ВЗАЄМОДІЇ ПРАВООХОРОННИХ ОРГАНІВ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

## 1. ВЗАЄМОДІЯ ПРАВООХОРОННИХ ОРГАНІВ НА НАЦІОНАЛЬНОМУ РІВНІ

З теоретичної точки зору, на національному рівні взаємодія правоохоронних органів поділяється на такі види:

- координація діяльності правоохоронних органів;
- взаємодія слідчого та оперативних підрозділів;
- взаємодія прокурора із слідчим;
- взаємодія слідчого (органів дізнання) з експертами, фахівцями у відповідних галузях знань (наукове забезпечення);
- взаємодія слідчого з іншими міжнародними та громадськими організаціями [84].

Розглядаючи дане питання, слід відмітити, що взаємодія правоохоронних органів на національному рівні під час розслідування злочинів пов'язаних з торгівлею людьми має свої особливості лише в частині суб'єктного складу, натомість форми і методи такої взаємодії відображені в КПК України, а саме в статтях щодо повноважень і обов'язків сторони обвинувачення, законах та підзаконних нормативно-правових актів, як то наприклад Закон України «Про оперативно-розшукову діяльність», Інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні».

Отже суб'єктами взаємодії виступають: 1) державні органи: Генеральна прокуратура, регіональні та місцеві прокуратури, МВС України, де головні завдання з протидії торгівлі людьми із використанням високих технологій виконують підрозділи боротьби зі злочинами, пов'язаними з торгівлею людьми, підрозділи боротьби з кіберзлочинністю та слідчі підрозділи; Служба безпеки України (зокрема Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки); Державна служба спеціального зв'язку та захисту інформації України (Державний центр захисту інформаційно-телекомунікаційних систем, зокрема команда CERT-UA); структури інформаційної безпеки органів влади; 2) приватні структури: приватні юридичні та фізичні особи, які професійно займаються протидією торгівлі людьми; провайдери (оператори) телекомунікацій, громадські організації.

Оскільки найбільш часто у кримінальних провадженнях, пов'язаних з торгівлею людьми, внутрішня взаємодія відбувається між оперативним працівником та слідчим наведемо орієнтовний алгоритм такої взаємодії:

1. Усна заява особи про вчинення кримінального правопорушення відповідно до вимог наказу МВС від 06.11.2015 № 1377 заноситься працівником поліції до протоколу усної заяви (повідомлення) про кримінальні правопорушення, який підписують заявник та посадова особа, яка прийняла

заяву. Письмова заява, подана безпосередньо заявником, або повідомлення, які надійшли телефонним зв'язком, реєструються в черговій частині в ЄО та негайно надаються керівникові органу досудового розслідування, про що інформується начальник територіального органу поліції. Усі заяви і повідомлення про вчинені кримінальні правопорушення та інші події реєструються цілодобово в чергових частинах поліції. Потерпілому, особою, яка прийняла заяву про вчинення кримінального правопорушення, вручається пам'ятка про процесуальні права та обов'язки відповідно до вимог ст. 55 КПК України. Після резолюції керівника органу досудового розслідування відомості про кримінальне правопорушення слідчим вносяться до ЄРДР, після чого розпочинається досудове розслідування відповідно до вимог ст. 214 КПК України. Керівником органу досудового розслідування згідно з вимогами ст. 39 визначає слідчого (слідчих), який здійснюватиме досудове розслідування.

2. Повідомлення слідчим відповідно до вимог ст. 60 КПК України потерпілої (потерпілого) про реєстрацію заяви у ЄРДР.
3. Повідомлення слідчим відповідно до вимог ч. 6 ст. 214 КПК України прокурора про початок досудового розслідування.
4. Створення на підставі ст. 39 КПК України слідчої групи (за необхідності).
5. Складання детального узгодженого з оперативними підрозділами плану проведення слідчих (розшукових) дій з визначенням конкретних строків та виконавців відповідно до наказу МВС від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні».
6. Допит потерпілої (потерпілого) з дотриманням вимог ст. 224 КПК України про обставини вчинення протиправних дій.
7. У разі необхідності процесуальним керівником (прокурором) на підставі ст. 241 КПК України виноситься постанова про проведення освідування потерпілого(-ої), під час якого встановлюється стан його здоров'я; у тому числі наявність ознак застосування до нього фізичного насильства; при сексуальній експлуатації; ознак тривалого неконтрольованого інтимного життя та його наслідків. За результатами слідчої дії складається протокол.
8. За наявності підстав (наявності виписок з історії хвороби (у випадку лікування жінки після повернення з місця експлуатації від венеричних чи інших захворювань сечостатевої системи, здійснення абортів, провокації передчасних пологів тощо) відповідно до статей 242-245 КПК України слідчим, прокурором виноситься постанова, слідчим суддею, судом доручення про проведення судово-медичної експертизи.
9. За наявності підстав відповідно до статей 242-245 КПК України проводиться судово-психологічна експертиза потерпілого (потерпілої) з метою встановлення його психологічного стану в умовах експлуатації, дослідження перебування в уразливому стані тощо.
10. У рамках досудового розслідування кримінального провадження слідчий на підставі ст. 40 КПК України направляє начальникові підрозділу боротьби зі злочинами, пов'язаними з торгівлею людьми, доручення з метою встановлення особи, яка причетна до торгівлі людьми, а також встановлення осіб, які можуть підтвердити факт вербування, переміщення, передачі (одержання) людини з метою експлуатації.
11. Після виконання доручення слідчий надає запити до інформаційно-аналітичних підрозділів поліції, реєстраційної служби, психоневрологічного диспансеру та збирає на особу (потенційного підозрюваного) інші характеризуючі дані.
12. Підготовка слідчим, прокурором відповідно до вимог глави 21 КПК України клопотань про проведення необхідних негласних слідчих (розшукових) дій, у випадках, передбачених

кримінально-процесуальним законодавством погодження їх з прокурором та спрямування їх на розгляд слідчому судді. Зокрема, на практиці найчастіше проводиться аудіо-, відео контроль особи згідно з вимогами ст. 260 КПК України, зняття інформації з транспортних телекомунікаційних мереж згідно з вимогами ст. 263 КПК України, зняття інформації з електронних інформаційних систем згідно з вимогами ст. 264 КПК України, спостереження за особою, річчю згідно з вимогами ст. 269 КПК України, контроль за вчиненням злочину згідно з вимогами ст. 271 КПК України. Клопотання та ухвала слідчого судді мають гриф «таємно» та зберігаються в режимно-секретному органі.

13. Надання доручення оперативним працівникам відповідно до положень п. 3 ч. 2 ст. 40 КПК України щодо проведення необхідних негласних слідчих (розшукових) дій. Доручення має гриф «таємно», зберігається в режимно-секретному органі.

14. Проведення детальних допитів свідків протиправних дій щодо потерпілого згідно з вимогами статей 224-226 КПК України (це можуть бути як члени родини і знайомі потерпілої (го); працівники фірми, які були задіяні у вербуванні; працівників паспортної, міграційної, митної служби, які мають інформацію щодо факту перетину кордону потерпілою(им); осіб, які користувалися послугами потерпілого (ої), у т.ч. інтимного характеру, що вимушено надавав потерпілий (а); працівників медичних закладів, до яких зверталася за допомогою потерпіла(ий) та інших).

15. Слідчим відповідно до вимог глави 15 КПК України на підставі ухвали слідчого судді, суду здійснюється тимчасовий доступ до речей і документів:

    - які свідчать про оформлення виїзних документів;
    - оригіналів друкованих видань або їх копій, у яких розміщувалися рекламні оголошення щодо надання підприємством (особою) відповідних послуг;
    - якими підтверджується факт звернення потерпілої особи до даного підприємства (особи) та взяття з його боку зобов'язань надати певні послуги (такі документи можуть знаходитись як на підприємстві (у певної особи), так і у потерпілого);
    - які знаходяться в касах аеропортів, залізничних вокзалів; відділів віз та реєстрації, паспортної, реєстраційної та міграційної роботи ОВС (куди надходить інформація із консульств України щодо осіб, які, перебуваючи за кордоном, втратили паспорт і потребують підтвердження їхньої особи); підрозділах охорони державного кордону (щодо затримання потерпілих під час нелегального перетину кордон чи даних щодо факту перетину кордону) та ін.;
    - які підтверджують наявність (відсутність) майна трафікерів, на яке в подальшому можливо накласти арешт;
    - даних з Укртелекому, інших установ зв'язку, а також операторів стільникового зв'язку про вхідні та вихідні дзвінки з телефонних апаратів, власниками яких є особи, які є потенційними підозрюваними у вчиненні правопорушення; банківських установ щодо отримання документів, які свідчать про спосіб та порядок передачі та отримання грошових коштів, отриманих злочинним шляхом, за системою переказів «Western Union», банківськими переказами та ін.

16. Складання протоколу затримання підозрюваного згідно з вимогами ст. 208 КПК України. Зазначення в протоколі часу фактичного затримання особи. Повідомлення про затримання близьких родичів, членів сім'ї чи інших осіб за вибором затриманого.

17. Внесення слідчим відомостей про затримання підозрюваного до ЄРДР.

18. Залучення згідно з вимогами ст. 48 КПК України захисника підозрюваного.

19. Допит слідчим, прокурором з дотриманням вимог ст. 224 КПК України, у необхідних випадках – слідчим суддею з дотриманням вимог ст. 225 КПК України особи як підозрюваного за участю захисника.

20. Оголошення особі на підставі статей 276-278 КПК України узгодженого з прокурором повідомлення про підозру у вчинені кримінального правопорушення, передбаченого ст. 149 КК України.
21. Внесення слідчим згідно з вимогами ст. 278 КПК України відомостей про підозру до ЄРДР.
22. Підготовка слідчим відповідно до вимог ст. 184 КПК України клопотання про застосування запобіжного заходу, узгодження його з прокурором та направлення до слідчого судді для розгляду. Вручення копії клопотання з відповідними додатками підозрюваному та його захиснику не менш ніж за 3 години до початку розгляду клопотання в суді.
23. Підготовка слідчим (за погодженням з прокурором), прокурором на підставі ст. 171 КПК України клопотання із відповідними додатками про арешт майна підозрюваного та направлення його до слідчого судді для розгляду відповідно до вимог статей 172, 173 КПК України.
24. Підготовка слідчим за погодженням з прокурором або прокурором згідно з вимогами ст. 234 КПК України клопотання із відповідними додатками про проведення обшуків за місцем реєстрації та мешкання підозрюваного та направлення їх для погодження прокурору. Отримання ухвали слідчого судді про дозвіл на обшук відповідно до ст. 235 КПК України.

Отже, ефективне розслідування торгівлі людьми не можливе без організації взаємодії слідчих з іншими підрозділами органів Національної поліції України, зокрема підрозділами боротьби зі злочинами, пов'язаними з торгівлею людьми Національної поліції України. Взаємодія слідчих з оперативними підрозділами повинна здійснюватись у відповідності з вимогами «Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні», затвердженої наказом МВС України № 575 від 07.07.2017 року.

Крім того, у рамках здійснення взаємодії важливо налагодити співпрацю не лише з державними та міжнародними органами, але й з громадськими організаціями, які ведуть роботу щодо протидії торгівлі людьми.

Зі службами безпеки державних органів, приватними юридичними та фізичними особами, які професійно займаються протидією торгівлі людьми, правоохоронні органи співпрацюють, як правило, шляхом обміну інформацією.

**Серед приватних підприємств найбільш плідною є взаємодія із провайдерами (операторами) телекомунікацій.**

Відповідно до п. 4 ст. 39 Закону України «Про телекомунікації» від 18.11.2003 [85] оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

Крім того, у 2010 р. в рамках боротьби з дитячою порнографією п. 2 ст. 39 Закону України «Про телекомунікації» було доповнено важливою нормою, згідно з якою оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента в порядку, встановленому законом.

Таким чином, на законодавчому рівні закріплено **обов'язок оператора (провайдера телекомунікацій)** не тільки щодо **реєстрації мережної активності** своїх клієнтів, але й щодо **збереження такої інформації** протягом певного періоду часу. Для одержання такої інформації потрібне судове рішення.

Відповідно до ст. 6 Директиви ЄС інформація про з'єднання абонентів має зберігатися не менше 6 місяців і не більше 2 років з дня з'єднання [86].

Структуру та вимоги до систем перехоплення, встановлених у провайдерів телекомунікацій, можна знайти у нормативному документі «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги», затвердженому спільним наказом Служби безпеки України та Адміністрації Держспецзв'язку від 13.02.2014 № 48/75 [87].

**ЗАВДАННЯ**

**СКЛАДІТЬ ЗАПИТ ДО ПРОВАЙДЕРА ТЕЛЕКОМУНІКАЦІЙ ЩОДО НАДАННЯ ІНФОРМАЦІЇ ПРО ВЛАСНИКА МЕРЕЖНОГО РЕСУРСУ**

## 2. МІЖНАРОДНА ВЗАЄМОДІЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

### ЗАГАЛЬНИЙ ПОРЯДОК МІЖНАРОДНОЇ ВЗАЄМОДІЇ

Однією з головних проблем у виявлені та припинені злочинів, пов'язаних із торгівлею людьми, є їх транснаціональний характер. Адже аналіз практики свідчить про те, що часто потерпілі, свідки й обвинувачені потенційно можуть бути представниками різних держав. Така ситуація може ускладнюватися з огляду на те, що ці злочини виходять за межі однієї держави. Їх фігуранти можуть бути затримані, заарештовані за межами юрисдикції України, що спричиняє необхідність використання процедур видачі після, можливо, міжнародного ордера на арешт.

Міжнародні експерти виділяють також інші проблемні питання у протидії торгівлі людьми: надзвичайно велика латентність злочинів, використання трафікерами прогалин в роботі поліції, кордони між країнами походження, транзиту і призначення живого товару, викриття і затримання лише рядових виконавців злочинного ланцюга, передування торгівлі людьми економічних, соціальних та екологічних проблем, спричинених військовими, релігійними та іншими конфліктами. Під час активного виявлення злочинів, зокрема внаслідок попереднього збирання оперативних даних, оперативні підрозділи, потребують отримання інформації з інших юрисдикцій.

Отримання такої інформації на даний час відбувається в двох найбільш розповсюджених формах, а саме:

- міжнародно-правової допомоги, а саме проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою шляхом надання відповіді на запит про надання правової допомоги у кримінальному провадженні;
- обміну відомостями оперативно-розшукового характеру, реагування на повідомлення та запити правоохоронних органів іноземних держав шляхом співробітництва центрального бюро Інтерполу в Україні з Генеральним секретаріатом Інтерполу та правоохоронними органами зарубіжних держав під час здійснення діяльності, пов'язаної із попередженням, розкриттям та розслідуванням злочинів, які мають транснаціональний характер або виходять за межі України.

### МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Міжнародна взаємодія у кримінальних провадженнях, як правило, здійснюється через органи прокуратури.

Головними нормативно-правовими актами, на підставі яких здійснюється взаємодія органів прокуратури з іноземними юрисдикціями з питань оперативно-розшукової діяльності та досудового слідства є:

- Конституція України;

- міжнародні договори, ратифіковані Верховною Радою України у встановленому законом порядку;
- Кримінальний процесуальний кодекс України від 13.04.2012;
- Закон України «Про міжнародні договори України» від 29.06.2004;
- Закон України «Про прокуратуру» від 14.10.2014.

Відповідні міжнародні угоди про взаємну допомогу у кримінальних справах можуть бути багатосторонніми, як от Європейська конвенція про взаємну допомогу у кримінальних справах 1959 року із додатковими протоколами, Конвенція про правову допомогу і правові відносини у цивільних, сімейних та кримінальних справах 1993 року із додатковим протоколом або двосторонніми.

Найбільш сприятливою ситуацією для здійснення міжнародної взаємодії є наявність взаємно ратифікованої двосторонньої угоди про правову допомогу у сфері здійснення кримінального провадження. На теперішній час в Україні є чинними більше сорока таких договорів. Серед останніх документів цього виду можна виділити:

- Договір між Україною та Урядом Малайзії про взаємну правову допомогу в кримінальних справах від 04.08.2016, ратифікований Законом України № 1902-VIII від 22.02.2017;
- Договір між Україною та Демократичною Соціалістичною Республікою Шри-Ланка про взаємну правову допомогу у кримінальних справах від 25.06.2016, ратифікований Законом України № 1750-VIII від 16.11.2016.

Крім наведених країн відповідні договори укладено з Республікою Сенегал, Об'єднаними Арабськими Еміратами, Сирійською Арабською Республікою, Арабською Республікою Єгипет, Ісламською Республікою Іран, Республікою Панама, Корейською Народно-Демократичною Республікою, Республікою Куба, Республікою Індія, Федеративною Республікою Бразилія, Соціалістичною Республікою В'єтнам, США, Канадою, Монголією, Латвійською Республікою, Естонською Республікою, Республікою Грузія, Республікою Молдова, Литовською Республікою, Республікою Польща, Китайською Народною Республікою тощо.

Якщо міжнародного договору на даний момент нема, то відповідна взаємодія здійснюється через Міністерство закордонних справ. При цьому саме звернення формує Генеральна прокуратура України.

У будь-якому випадку, працівнику прокуратури перед ініціюванням міжнародної взаємодії слід проконсультуватися з працівниками Департаменту міжнародно-правового співробітництва Генеральної прокуратури України.

Основним відомчим нормативним актом в галузі міжнародної правової допомоги у кримінальному провадженні є наказ Генеральної прокуратури України від 18.09.2015 № 223 (зі змінами, внесеними наказом Генеральної прокуратури України від 16.01.2017 № 6) «Про організацію роботи органів прокуратури України у галузі міжнародного співробітництва».

Питання правової допомоги також безпосередньо регламентують накази Генерального прокурора України від 16.11.1998 № 27 «Про забезпечення виконання органами прокуратури України «Угоди між Генеральною прокуратурою України і Міністерством юстиції Республіки Польща на виконання статті 3 Договору між Україною і Республікою Польща про правову допомогу та правові відносини у цивільних і кримінальних справах від 24 травня 1993 року» та від 19 липня 2010 року № 42 «Про забезпечення виконання органами прокуратури України «Угоди між Генеральною прокуратурою України та Генеральною прокуратурою Республіки Молдова на виконання статті 3 Договору між Україною і Республікою Молдова про правову допомогу та правові відносини у цивільних і кримінальних справах від 13 грудня 1993 року».

За загальним правилом, встановленим ст. 545 КПК України, зносини з питань правової допомоги у кримінальному провадженні здійснюються через центральні органи України, а саме: Генеральну прокуратуру України (під час досудового розслідування) та Міністерство юстиції України (під час судового провадження).

Порядок направлення запитів українськими компетентними органами чітко визначено ст.ст. 548 та 551 КПК України.

Суд, прокурор або слідчий за погодженням з прокурором надсилає до уповноваженого (центрального) органу України запит про міжнародну правову допомогу у кримінальному провадженні, яке він здійснює.

Закон також передбачає використання сучасних засобів зв'язку для прискореної передачі запитів. Зокрема, ч. 4 ст. 548 КПК України визначає можливість надіслання запиту за кордон у невідкладних випадках електронним, факсимільним або іншим засобом зв'язку. У разі використання таких сучасних комунікаційних можливостей закон зобов'язує уповноважений (центральний) орган надіслати оригінал запиту поштою не пізніше трьох днів з моменту його передання іншим засобом зв'язку.

Зміст та форма запиту про міжнародну правову допомогу повинні відповідати загальним вимогам, встановленим ст. 552 КПК України, а також міжнародному договору України, що застосовується у конкретному випадку. Запит може бути складений у формі доручення. Запит і долучені до нього документи складаються у письмовій формі, засвідчуються підписом уповноваженої особи та печаткою відповідного органу.

Загальний опис фабули має бути простим і стислим, але достатнім з юридичної точки зору для отримання допомоги.

Доцільно відзначити, що спеціальними міжнародними Конвенціями передбачено право запитуваних країн направляти запити про виявлення коштів, одержаних злочинним шляхом. Зокрема, відповідно до статті 17 Конвенції про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, 1990 року кожна Сторона на умовах, викладених у цій статті, уживає заходів, необхідних для визначення, у відповідь на запит іншої Сторони, чи має або контролює фізична чи юридична особа, яка є суб'єктом кримінального розслідування, один чи більше рахунків будь-якого виду в будь-якому банку, розташованому на її території, і, якщо так, надає інформацію про визначені рахунки. Незважаючи на вказане положення, практика свідчить про інше. Іноземними компетентними органами такі доручення відкладаються як другорядні та виконуються неохоче. За таких обставин саме правоохоронні органи України як ініціатори запитів зобов'язані виявити майно, рахунки, вказати реквізити і запросити точні процесуальні дії з метою належного виконання міжнародного доручення [88].

У СЕРПНІ 2017 РОКУ ПРАЦІВНИКИ ДЕПАРТАМЕНТУ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ, ПОВ'ЯЗАНИМИ З ТОРГІВЛЕЮ ЛЮДЬМИ, СПІЛЬНО З ПРАЦІВНИКАМИ ГОЛОВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ІВАНО-ФРАНКІВСЬКІЙ ОБЛАСТІ, ДЕПАРТАМЕНТОМ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ДПС УКРАЇНИ ТА ЗА СПРИЯННЯМ ПРИКОРДОННОЇ ВАРТИ ПОЛЬСЬКОЇ РЕСПУБЛІКИ, НАЦІОНАЛЬНОГО АГЕНТСТВА ПРОТИДІЇ ЗЛОЧИННОСТІ ВЕЛИКОЇ БРИТАНІЇ, ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ ЛИТОВСЬКОЇ РЕСПУБЛІКИ ТА СЛУЖБИ ФІНАНСОВОЇ РОЗВІДКИ «WESTERN UNION», ПРИПИНИЛИ ДІЯЛЬНІСТЬ ТРАНСНАЦІОНАЛЬНОГО КАНАЛУ ТОРГІВЛІ ЛЮДЬМИ.

У МЕЖАХ ДОСУДОВОГО РОЗСЛІДУВАННЯ, РОЗПОЧАТОГО ЗА СТ. 149 КК УКРАЇНИ, ПРАВООХОРОНЦІ ВИКРИЛИ ДІЯЛЬНІСТЬ ЗЛОЧИННОЇ ГРУПИ, ЩО НАЛІЧУВАЛА БІЛЬШЕ 10 ОСІБ, СЕРЕД ЯКИХ ГРОМАДЯНИ ПОЛЬЩІ, ЛИТВИ ТА УКРАЇНИ. У РЕЗУЛЬТАТІ ПРОВЕДЕННЯ СПЛАНОВАНОЇ СПЕЦОПЕРАЦІЇ ЗАТРИМАНО 4 ОСІБ, З ЯКИХ 3 – ІНОЗЕМЦІ.

ЗЛОВМИСНИКИ ОРГАНІЗУВАЛИ ТА НАЛАГОДИЛИ ЧІТКО СПЛАНОВАНУ СХЕМУ, ЗА ЯКОЮ ВЕРБУВАЛИ ТА НЕЗАКОННО ПЕРЕМІЩУВАЛИ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНЦІВ ДО ВЕЛИКОЇ БРИТАНІЇ. ОПЕРАТИВНИКИ ПОЛІЦІЇ ВСТАНОВИЛИ, ЩО ЗА ЦІЄЮ СХЕМОЮ ЗЛОВМИСНИКИ ПЕРЕПРАВИЛИ ДО БРИТАНІЇ БЛИЗЬКО 20 УКРАЇНЦІВ. ОБІЦЯЮЧИ РОБОТУ ЗА КОРДОНОМ, УЧАСНИКИ ЗЛОЧИННОЇ ГРУПИ ВТЯГУВАЛИ У БОРГОВУ КАБАЛУ ПОТЕРПІЛИХ. НЕЗАКОННО ПЕРЕТНУВШИ ДЕРЖАВНИЙ КОРДОН, ГРОМАДЯНИ УКРАЇНИ, ЧЕРЕЗ НЕВИЗНАЧЕНИЙ СТАТУС ТА БОРГ, ПОТРАПЛЯЛИ У ЗАЛЕЖНІСТЬ РОБОТОДАВЦІВ, ДЕ ПРАЦЮВАЛИ ПОНАД НОРМИ. ЗАРОБІТНА ПЛАТА ЗАЛИШАЛАСЬ МІЗЕРНОЮ, ТОЖ ВОНИ НЕ МАЛИ МОЖЛИВОСТІ ПОВЕРНУТИСЯ ДОДОМУ ЧЕРЕЗ БРАК КОШТІВ І НЕЛЕГАЛЬНЕ СТАНОВИЩЕ.

ПОЛІЦЕЙСЬКІ ВСТАНОВИЛИ, ЩО ПРОТЯГОМ 2014-1017 РОКІВ, ЙМОВІРНИМИ ПОТЕРПІЛИМИ ВІД ЦЬОГО ЗЛОЧИННОГО ТРАФІКУ СТАЛИ БІЛЬШЕ НІЖ 30 ГРОМАДЯН УКРАЇНИ. ПРАВООХОРОНЦІ ПРОВЕЛИ ШІСТЬ САНКЦІОНОВАНИХ ОБШУКІВ ЗА МІСЦЕМ ПРОЖИВАННЯ ЗЛОВМИСНИКІВ А ТАКОЖ У ЇХ АВТОТРАНСПОРТІ. ЗА РЕЗУЛЬТАТОМ, ВИЛУЧЕНО ЧОРНОВІ ЗАПИСИ, ДОКУМЕНТИ УКРАЇНЦІВ ТА ТЕЛЕФОННІ ЗАПИСНИКИ ІЗ НОМЕРАМИ ТЕЛЕФОНІВ ПОСІБНИКІВ ЗА КОРДОНОМ ТА ПОТЕРПІЛИХ. КРІМ ТОГО, ВИЛУЧЕНО СПИСКИ ПОТЕНЦІЙНИХ ПОТЕРПІЛИХ, ЯКИХ БУЛО БІЛЬШЕ 200 ОСІБ.

Відомості, які містяться в матеріалах, отриманих у результаті виконання дій, передбачених у запиті про міжнародне співробітництво, органами іноземної держави та за процедурою, передбаченою законодавством запитуваної держави, не потребують легалізації і визнаються судом допустимими, якщо під час їх отримання не було порушено засади справедливого судочинства, права людини і основоположні свободи.

Слід пам'ятати, що відповідно до ч. 2 ст. 84 КПК України процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів, а згідно п. 2 ч. 2 ст. 99 КПК України до документів належать матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України.

## ІНТЕРПОЛ

Співробітництво органів внутрішніх справ України з правоохоронними органами іноземних держав із питань обміну відомостями оперативно-розшукового характеру з метою запобігання транснаціональним злочинам та їх розкриття, а також реагування на повідомлення та запити правоохоронних органів іноземних держав здійснюється лише через структурні підрозділи апарату МВС за напрямами оперативно-службової діяльності, Управління міжнародних зв'язків та Робочий апарат Укрбюро Інтерполу.

Проекти Генерального Секретаріату Інтерполу спрямовані на:

- збирання, вивчення й аналізування інформації про певний вид транснаціональної злочинності, пов'язаної з торгівлею людьми (характер злочинних груп, їх учасники тощо);
- установлення осіб, причетних до протиправної діяльності, пов'язаної з торгівлею людьми;
- ідентифікацію членів організованих злочинних груп, пов'язаних із торгівлею людьми, дослідження їх ієрархічної структури, сфер, способів та наслідків учинення злочинів;
- підготування узагальнених звітів для розповсюдження серед правоохоронних органів держав-учасниць проектів;
- систематизування даних щодо злочинних угруповань, пов'язаних із торгівлею людьми, та їх членів;
- надання допомоги країнам-учасницям Інтерполу щодо обміну інформацією з питань розслідування кримінальних проваджень, пов'язаних із торгівлею людьми;
- налагодження безпосередніх контактів між Національними центральними бюро Інтерполу та правоохоронними органами, що є учасниками конкретного проекту.

Порядок направлення запитів до Укрбюро Інтерполу, їх типову форму й зміст регламентує Інструкція про порядок використання правоохоронними органами можливостей Національного центрального бюро Інтерполу в Україні у попередженні, розкритті та розслідуванні кримінальних правопорушень [89].

Відповідно до цієї Інструкції, запити та інші документи, що надсилаються до Укрбюро Інтерполу, повинні мати такі реквізити: назва органу, його повна адреса, телефон, телетайп або факс, вихідний номер і номер посилання (за наявності), прізвище й телефон виконавця. Крім цього, запити та інші документи мають бути оформлені лише в друкованому вигляді, містити підписи керівників органу. Прізвища, імена іноземних

громадян, назви закордонних фірм, підприємств, організацій або установ, за наявності їх написання мовою запитуваної країни, відтворюються в оригіналі. Слід пам'ятати, що Укрбюро Інтерполу відмовляє повністю або частково стосовно виконання запитів, які:

- не стосуються компетенції Інтерполу;
- пов'язані з кримінальними правопорушеннями політичного, військового, релігійного чи расового характеру;
- можуть призвести до порушення суверенітету й безпеки України, законодавства України чи держави, до якої надсилають запит, прав людини;
- оформлені з порушенням вимог Інструкції про порядок використання правоохоронними органами можливостей Національного центрального бюро Інтерполу в Україні у попередженні, розкритті та розслідуванні кримінальних правопорушень;
- надійшли від фізичних осіб.

Про відмову у виконанні запиту із зазначенням причин Укрбюро Інтерполу інформує ініціатора письмово.

Перевірка з використанням каналів і можливостей Укрбюро Інтерполу може здійснюватися стосовно будь-яких діянь, визначених кримінальним законодавством як кримінальні правопорушення, крім тих, що мають військовий, політичний, релігійний чи расовий характер.

Аналіз практики свідчить, що транснаціональна злочинність, пов'язана з торгівлею людьми, може використовувати різні схеми господарської діяльності.

Так, під час проведення оперативно-розшукових заходів і слідчих (розшукових) дій щодо розкриття кримінальних правопорушень, пов'язаних із господарською діяльністю, через Укрбюро Інтерполу можна одержати з Генерального Секретаріату або Національного центрального бюро Інтерполу в зарубіжних країнах таку інформацію:

- офіційні назви комерційних структур та інших юридичних осіб – суб'єктів господарської діяльності, розташованих за кордоном;
- дата їх реєстрації у відповідних державних органах, юридична адреса, номери телефонів та інших телекомунікаційних засобів;
- прізвища й імена керівників таких структур;
- головні напрями діяльності;
- розміри статутного капіталу;
- відомості про припинення діяльності;
- відомості кримінального характеру стосовно їх керівників та інших працівників.

Крім того, можливе отримання з окремих країн інформації про угоди, укладені українськими резидентами з іноземними юридичними та фізичними особами або за їх участі, а також наслідки їх виконання. Відомості про відкриття фізичними особами, у тому числі громадянами України, та юридичними особами фінансових рахунків у зарубіжних банках, а також рух коштів ними, становлять зазвичай банківську чи комерційну таємницю. Тому іноземні правоохоронні органи їх можуть надавати лише після розгляду офіційного звернення Генеральної прокуратури України верховним органом юстиції (прокуратури) запитуваної держави в порядку надання правової допомоги в кримінальному проваджені.

До запитів, за потреби, додають копії контрактів та інших документів, що стосуються справи або матеріалів перевірки. За необхідності перевірки іноземних фірм, філіалів, спільних підприємств та інших об'єктів господарської діяльності, зареєстрованих за кордоном, у запиті додатково зазначають назву такої структури, юридичну (або фактичну) адресу, телефони, факси, конкретні запитання, на які передбачається одержати відповідь.

Якщо підозрювану особу встановлено, у запитах до Укрбюро Інтерполу зазначають:

- прізвище, ім'я, по батькові та повну дату народження підозрюваної особи, її громадянство та місце проживання;
- номер кримінального (оперативно-розшукового) провадження, матеріалу перевірки й орган, у провадженні якого вона перебуває;
- дані документів, що ідентифікують особу (паспорт, посвідчення водія тощо);
- обставини, якими викликана необхідність звернення до Національного центрального бюро;
- перелік заходів, що потрібно реалізувати.

Однією з важливих функцій Інтерполу є міжнародний розшук осіб, які вчинили злочини, пов'язані з торгівлею людьми. Його здійснюють відповідно до міжнародних договорів, Статуту Організації та рішень Генеральної Асамблеї Інтерполу, національного законодавства держав-членів Інтерполу.

У межах міжнародного розшуку правоохоронні органи України мають можливість ініціювати проведення розшукових заходів на території однієї, декількох або всіх держав-учасниць Інтерполу, ініціювати публікацію міжнародного повідомлення Інтерполу, розмістити в банках даних Генерального секретаріату Інтерполу інформацію щодо розшукуваних або інших осіб, у том числі громадян України, які не перебувають у розшуку, але є членами організованої злочинної групи або схильні до вчинення тяжких злочинів, зокрема тих, що пов'язані з торгівлею людьми на території різних держав.

ВІДПОВІДНО ДО СТАТТІ 84 ПРАВИЛ ІНТЕРПОЛУ З ОБРОБКИ ДАНИХ, ЗАТВЕРДЖЕНИХ РЕЗОЛЮЦІЄЮ 80-Ї СЕСІЇ ГЕНЕРАЛЬНОЇ АСАМБЛЕЇ ІНТЕРПОЛУ AO-2011-KE8-07 ПУБЛІКАЦІЮ ЦИРКУЛЯРНОГО РОЗШУКОВОГО ПОВІДОМЛЕННЯ ПРО МІЖНАРОДНИЙ РОЗШУК ОСОБИ З МЕТОЮ ЇЇ АРЕШТУ ТА ПОДАЛЬШОЇ ЕКСТРАДИЦІЇ МАС БУТИ ПОГОДЖЕНО З ЦЕНТРАЛЬНИМ ОРГАНОМ ЩОДО ВИДАЧІ (ЕКСТРАДИЦІЇ), ТОБТО ГЕНЕРАЛЬНОЮ ПРОКУРАТУРОЮ УКРАЇНИ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ, ПІД ЧАС СУДОВОГО РОЗГЛЯДУ.

ТОМУ, ҐЕНЕРАЛЬНОМУ СЕКРЕТАРІАТУ ІНТЕРПОЛУ МАЮТЬ БУТИ НАДАНІ ЧІТКІ ТА ПРЯМІ ГАРАНТІЇ, ЩО ТИМЧАСОВИЙ АРЕШТ І ВИДАЧУ (ЕКСТРАДИЦІЮ) ОСОБИ БУДЕ ЗАПИТАНО У ВИПАДКУ ЇЇ АРЕШТУ (ЗАТРИМАННЯ) НА ТЕРИТОРІЇ КРАЇН-ЧЛЕНІВ МОКП-ІНТЕРПОЛ У ПОРЯДКУ, ПЕРЕДБАЧЕНОМУ ЧИННИМ ЗАКОНОДАВСТВОМ, ДВОСТОРОННІМИ ТА БАГАТОСТОРОННІМИ ДОГОВОРАМИ.

ВКАЗАНА ПОЗИЦІЯ БЮРО ІНТЕРПОЛУ ПОЯСНЮЄТЬСЯ ТИМ, ЩО СТ. 573 КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ ЦЕНТРАЛЬНИЙ ОРГАН УКРАЇНИ МАЄ ПРАВО ВІДМОВИТИ В НАПРАВЛЕННІ ЗАПИТУ ДО ІНОЗЕМНОЇ ДЕРЖАВИ, ЯКЩО ІСНУЮТЬ ПЕРЕДБАЧЕНІ ЦИМ КОДЕКСОМ АБО МІЖНАРОДНИМ ДОГОВОРОМ УКРАЇНИ ОБСТАВИНИ, ЯКІ МОЖУТЬ ПЕРЕШКОДЖАТИ ВИДАЧІ.

ТОМУ, ІНТЕРПОЛ, ПРИ ОГОЛОШЕННЯ ОСОБИ У МІЖНАРОДНИЙ РОЗШУК ПРОСИТЬ ПОВІДОМЛЯТИ ЧИ БУДЕ ГЕНЕРАЛЬНА ПРОКУРАТУРА УКРАЇНИ НАПРАВЛЯТИ ЗАПИТ ПРО ВИДАЧУ (ЕКСТРАДИЦІЮ) ПЕВНОЇ ОСОБИ У ВИПАДКУ ЙОГО АРЕШТУ (ЗАТРИМАННЯ) НА ТЕРИТОРІЇ КРАЇНИ-ЧЛЕНА МОКП-ІНТЕРПОЛ.

Одним із пріоритетних напрямів діяльності Міжнародної організації кримінальної поліції – Інтерполу є протидія злочинам, пов'язаним із торгівлею людьми. Для забезпечення ефективної реалізації функцій організації в структурі директорату з окремих видів злочинів Генерального Секретаріату створено відділ протидії злочинам, пов'язаним із торгівлею людьми, завданнями якого є:

- координування співробітництва правоохоронних органів держав-членів Інтерполу в справах щодо злочинів, пов'язаних із торгівлею людьми з метою сексуальної, трудової експлуатації, розповсюдження дитячої порнографії, організування незаконної міграції;

- створення та забезпечення функціонування спеціалізованих банків даних щодо осіб, причетних до торгівлі людьми;ведення банку даних порнографічних зображень неповнолітніх;
- ідентифікація потерпілих у справах про транснаціональні злочини, пов'язані зі створенням і розповсюдженням дитячої порнографії;
- запровадження й реалізація аналітичних проектів у сфері торгівлі людьми;
- організація та проведення міжнародних науково-практичних заходів із проблем протидії торгівлі людьми (конференцій, тренінгів, оперативних зустрічей тощо).

Банк даних порнографічних зображень неповнолітніх містить більше 500 тис. зображень. Метою його запровадження є допомога правоохоронним органам різних держав у здійсненні ідентифікації неповнолітніх, яких використовували під час створення дитячої порнографії, а також виявлення та припинення кримінальних правопорушень, пов'язаних із систематичною сексуальною експлуатацією дітей. Доступ до зазначеного банку даних надається правоохоронним органам за умови їх активної участі в його наповненні.

Аналітичні проекти з питань торгівлі людьми реалізовує Генеральний Секретаріат за участі держав-учасниць Інтерполу, яких стосується зазначена проблема. Так, наприклад, у межах проекту «Червоні шляхи» («Redroutes») здійснювався аналіз інформації з усіх держав Європи, Центральної, та Південно-Східної Азії й Близького Сходу. Метою цього проекту був моніторинг ситуації щодо торгівлі жінками з країн Східної Європи та пострадянських держав Азії. Зокрема, він передбачав вивчення статистичної інформації про країни-походження та країни-призначення жертв торгівлі людьми, маршрути, характеристики організованих злочинних груп, залучених до цього виду злочинного бізнесу, розподіл за віковими й іншими характеристиками постраждалих та підозрюваних. Крім того, у межах проекту було створено відповідний банк даних постраждалих і підозрюваних у злочинах, пов'язаних із торгівлею людьми.

Генеральний Секретаріат Інтерполу також може організовувати проведення оперативних зустрічей працівників правоохоронних органів різних держав-учасниць Інтерполу, залучених до розслідування кримінальних правопорушень, пов'язаних із торгівлею людьми [90, с. 202-209].

## ІНШІ ФОРМИ ВЗАЄМОДІЇ

Окрім взаємодії у протидії торгівлі людьми через Інтерпол існують й інші шляхи співпраці. Так, згідно з Конвенцією «Про кіберзлочинність» щодо взаємодії правоохоронних органів у боротьбі з високотехнологічною злочинністю створено цілодобову мережу для здійснення контактів з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Зміст такої допомоги наведено на рис. 64 [91, с. 648].

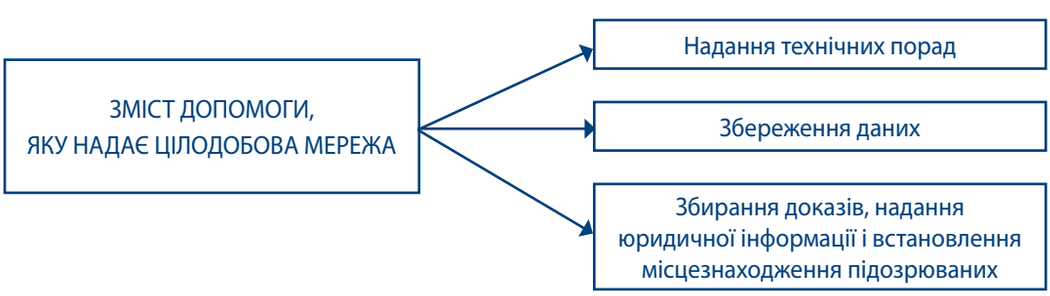



*Рис. 64. Структурна схема допомоги, яку надає цілодобова контактна мережа у боротьбі з кіберзлочинністю*

Також варто відзначити взаємодію безпосередньо між правоохоронними органами різних країн. Так, у рамках взаємодії із правоохоронними органами США працівникам правоохоронних органів України

корисно домовитись про спільне використання автоматизованих систем. Одним з відповідних ресурсів, який містить інформацію про IP-адреси, з яких здійснюється розповсюдження дитячої порнографії, в режимі реального часу із вказівкою країни та міста розповсюдження є icaccops.com (рис. 65).

| IP | All Networks | Location | FOI | Last Seen (UTC) |
|---|---|---|---|---|
| 193 8.69 | B | UA, 26, Zaporozhye | 99340 | 20.03.2017 |
| 77.5 186 | B | UA, 26, Zaporozhye | 85827 | 20.03.2017 |
| 91.1 .246 | B | UA, 26, Zaporozhye | 76222 | 19.03.2017 |
| 77.5 138 | B | UA, 26, Zaporozhye | 72321 | 20.03.2017 |
| 46.2 5.79 | B E | UA, 26, Zaporozhye | 59671 | 18.03.2017 |
| 89.2 103 | B | UA, 26, Zaporozhye | 57168 | 17.03.2017 |
| 194 .9 | B | UA, 26, Zaporozhye | 56474 | 19.03.2017 |

*Рис. 65. Сервіс ICACCOPS*

Для реєстрації на цьому ресурсі використовується форма за адресою https://www.icaccops.com/users/login.aspx (рис. 66).

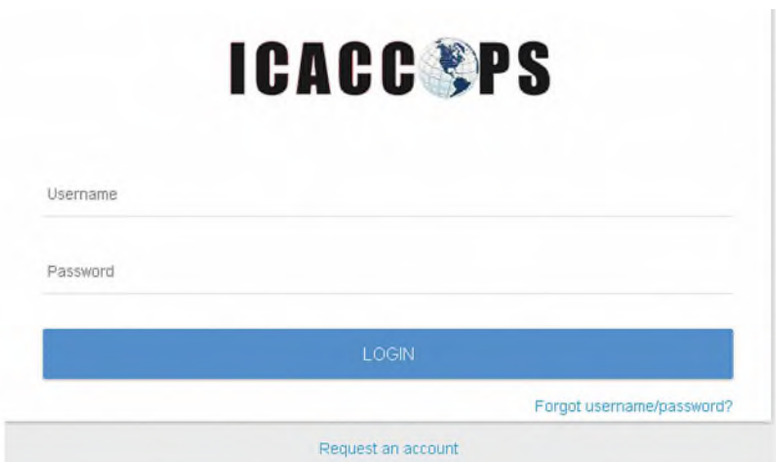



*Рис. 66. Форма реєстрації*

У рамках дослідження інституту міжнародної взаємодії правоохоронних органів під час протидії торгівлі людьми слід відзначити роль ОБСЄ з удосконалення цієї діяльності. Діяльність ОБСЄ у напрямку протидії міжнародному трафіку здійснюється на підставі Плану дій по боротьбі з торгівлею людьми, затвердженому 55 закордонними міністрами на Маастрихтській Раді Міністрів у грудні 2003 року. Зазначений документ має на меті забезпечити країни-учасниці Організації необхідним інструментарієм, що сприятиме виконанню ними функцій з ліквідації каналів вербування та переміщення осіб за кордон з метою експлуатації.

План дій запроваджує всебічний підхід до проблеми та передбачає низку заходів з протидії цій сучасній формі рабства на національному та міжнародному рівнях у сферах попередження, виявлення та припинення кримінальних правопорушень цієї спрямованості.

**План дій також охоплює низку зобов'язань та рекомендацій для реалізації на національному рівні:**

- впровадження національних механізмів переадресації постраждалих;
- призначення національних координаторів та доповідачів;
- розробка національних планів та програм протидії міжнародному трафіку;
- передбачення національним законодавством кримінальної відповідальності за торгівлю людьми;

- забезпечення захисту та надання притулку жертвам;
- забезпечення створення спеціалізованих підрозділів правоохоронних органів з протидії торгівлі людьми як у країнах походження, так і в країнах призначення.

Реалізація Організацією положень зазначеного документу в Україні здійснюється через Офіс Координатора проектів ОБСЄ в Україні, який надає допомогу уряду України у впровадженні національної стратегії боротьби з торгівлею людьми на політичному рівні, у сфері попередження, активізації переслідування та криміналізації цього кримінального правопорушення, надання допомоги постраждалим та дослідження проблеми торгівлі людьми.

Надаючи підтримку зусиллям України у попередженні цих грубих порушень прав людини, Координатор проектів ОБСЄ в Україні проводить низку заходів для підвищення рівня обізнаності та розуміння ризиків і наслідків торгівлі людьми серед працівників органів державної влади, потенційних жертв торгівлі людьми та неурядових організацій. З цією метою у посольствах та консульствах іноземних держав в Україні розповсюджуються інформаційно-довідкові матеріали із зазначених питання, впроваджуються проекти, надається підтримка неурядовим організаціям у роботі «гарячих ліній», їх працівники разом з представниками державних установ та засобів масової інформації залучаються до участі у відповідних тренінгах.

Крім того, Координатор проектів ОБСЄ в Україні активно сприяє органам державної влади України у формуванні національного законодавства та урядових програм з протидії торгівлі людьми.

З метою підвищення професіоналізму та результативності органів внутрішніх справ на даному напрямку оперативно-службової діяльності Координатор проектів ОБСЄ в Україні надає технічну допомогу та організовує, у співпраці з українськими партнерами, регулярні тренінги та семінари, робочі зустрічі з представниками поліцейських відомств іноземних держав з метою обміну позитивним досвідом та налагодження взаємодії. Офіс також активно співпрацює з МВС України на напрямку фінансування перекладів клопотань про надання міжнародної правової допомоги у кримінальних провадженнях та матеріалів, що надходять за результатами їх виконання з-за кордону.

Також у рамках здійснення міжнародної взаємодії важливо налагодити співпрацю не лише з державними та міжнародними органами, але й з громадськими організаціями, які ведуть роботу щодо протидії торгівлі людьми.

Як відомо, жертви торгівлі людьми неохоче йдуть на контакт з представниками правоохоронних органів. Тому зв'язуючим ланцюгом між правоохоронними органами та постраждалими від даного виду злочинів можуть стати саме такі організації. Необхідно прагнути до того, аби взаєморозуміння між правоохоронними підрозділами та такими організаціями було на високому рівні. Це дозволить в постійному режимі одержувати оперативно значущу інформацію про жертв торгівлі людьми, які потрапили в поле зору таких організацій, а також про діяльність відповідних злочинних угруповань.

Така інформація, як правило, фіксується шляхом проведення опитувань представників цих організацій, а також жертв торгівлі людьми, яким вони надають відповідну допомогу. Дана інформація дозволяє правоохоронним підрозділам почати відповідну перевірку шляхом провадження оперативно-розшукових заходів, слідчих і негласних (розшукових) дій [92, с. 69-70].

Слід наголосити, що без згоди жертви торгівлі людьми відомості про неї правоохоронцям не розголошуються. При цьому інформація про сам факт вчинення злочину є орієнтуючою для посилення уваги правоохоронних органів до потенційних правопорушників.

**ЗАВДАННЯ**

**З ВИКОРИСТАННЯМ СЛУЖБОВОЇ ЕЛЕКТРОННОЇ ПОШТИ ЗАРЕЄСТРУЙТЕСЯ НА САЙТІ HTTPS://ICACCOPS.COM/**

# КОМПЛЕКСНА ВПРАВА

**З метою комплексного опрацювання набутих навичок та засвоєння матеріалів курсу слухачам потрібно вирішити завдання комплексної вправи та продемонструвати результати їх виконання.**

Для вирішення комплексної вправи пропонується розділити групу слухачів на дві команди: 1) слідчі та 2) оперативні працівники.

На першому етапі обом командам надається фабула та завдання комплексної вправи, після чого вони у взаємодії приступають до її виконання. Час на виконання завдань визначається у кожному випадку окремо, залежно від їх складності.

По завершенні виконання завдань оцінюється якість роботи кожної з команд. Критерії оцінювання (за п'ятибальною шкалою кожний): повнота та аргументованість відповідей; робота в команді; дотримання вимог чинного законодавства. Після оцінювання команд вони змінюють свій статус, одержують нову фабулу та завдання і продовжують їх виконання. Так два раунди. По закінченні вправи підбиваються підсумки.

Слухачі повинні засвоїти, що кожний злочин залишає в навколишньому середовищі певні сліди. Вони є носіями інформації, на основі якої можна встановити обставини злочину і осіб, які його вчинили. У випадку наявності електронних слідів існують спеціальні процедури їх виявлення та фіксації.

Вирішуючи завдання комплексної вправи, потрібно звертати увагу на:

- види слідів, які можливо зафіксувати за результатами використання правопорушниками тих чи інших інформаційних технологій;
- вибір тактики дій з документування виявленого кримінального правопорушення;
- порядок роботи у складі слідчо-оперативної групи;
- особливості застосування інформаційних технологій та документального закріплення цього процесу під час слідчих та негласних слідчих (розшукових) дій;
- порядок взаємодії зі спеціалістами та експертами;
- заходи забезпечення інформаційної безпеки правоохоронних органів під час провадження службової діяльності;
- зрозумілості задокументованих даних для прокуратури та суду.

## ФАБУЛА 1

Від британських правоохоронних органів (Центр боротьби з дитячою експлуатацією) отримано відомості про групу громадян України, які підозрюються в участі у торгівлі людьми та інших тяжких злочинах.

За оперативною інформацією вони користуються веб-сайтами «Facebook» та «ВК», щоб переконати сім'ї (особливо з малими дітьми) з країн пострадянського простору поїхати в Україну, де батьки зможуть отримати роботу, а потім залучають їхніх дітей до сексуальної експлуатації, зокрема участі у статевих актах та потоковому відео цих актів наживо з трансляцією через Інтернет.

Поширення матеріалів з дитячою порнографією відбувається через P2P програми: «Emule» та «Edonkey», спілкування з іншими співучасниками за межами України через «Skype» та «Viber». Також відома адреса сайту, з якого здійснюється онлайн-трансляція у приват-чатах з дітьми.

# КОМПЛЕКСНА ВПРАВА

Правопорушники регулярно спілкуються за допомогою засобів стільникового зв'язку як із жертвами злочину, так і між собою.

Попередньо встановлено особи двох правопорушників – мешканців Дніпропетровської області, які є активними користувачами соціальних мереж (відомі їх облікові записи) та спеціалізованих форумів з обговорення дитячої порнографії. Оперативні дані також свідчать, що у Київській області злочинці орендують помешкання, в якому проживають дві родини з сусідньої країни з малими дітьми.

? *Визначити порядок дій правоохоронних органів України. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.*

## ФАБУЛА 2

Під час ініціативного пошуку на закритих форумах в мережі Інтернет оперативним працівником було виявлено оголошення з пропозицією купівлі «рабів» з України. У якості контактів для спілкування було залишено назву електронної пошти та номер ICQ.

У рамках перевірки оперативної інформації було встановлено, що особи, які надали таке оголошення, входять до складу злочинного угруповання, яке переважно діє на території Донецької та Луганської областей, що є тимчасово непідконтрольними державним органам України. Злочинці мають спільників у Запорізькій та Харківській областях, а також дотримуються правил конспірації.

У рамках дослідження переписки на форумі було встановлено, що можливий організатор злочинного угруповання має прізвисько «Арсен», є громадянином України та регулярно виїжджає до східних країн (зокрема Туреччини) з метою укладання протиправних угод з торгівлі людьми.

Також у результаті аналізу записів форуму оперативний працівник обґрунтовано припустив, що організатор злочинного угруповання та дівчина з ніком «Люсьен» перебувають у близьких стосунках.

За результатом вивчення профілю «Люсьен» стали відомі її ймовірний рік народження та назва контакту в «Skype».

? *Яким чином має діяти оперативний працівник, слідчий? Визначити порядок дій правоохоронних органів у даній ситуації. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.*

## ФАБУЛА 3

Від однієї з міжнародних громадських організацій в правоохоронні органи України надійшло повідомлення, що до них звернувся по допомогу чоловік на території Польщі з проханням доправити його в Україну.

Вказана особа повідомила, що його та ще дванадцять осіб (7 жінок та 5 чоловіків) шляхом обману вивезли на територію Польщі з України.

## КОМПЛЕКСНА ВПРАВА

Особисто йому запропонували добре оплачувану роботу у Данії на одній із ферм та навіть перерахували аванс у вигляді ста доларів США через систему Webmoney. Пропозицію із роботою він знайшов на сайті оголошень. Усю переписку із «роботодавцем» вів за допомогою електронної пошти.

Під час перебування у Польщі до вказаного чоловіка та інших осіб застосовували психологічне та фізичне насильство, жінок примушували до надання сексуальних послуг, а чоловіків до роботи на якійсь фермі. Одним із способів залякування стало те, що чоловіка, який найбільше пручався вивезли у невідомому напрямку та через місяць привезли назад до бази злочинців без однієї нирки.

Чоловік також повідомив, що один з охоронців постійно грався в онлайн-ігри та назвав його псевдонім у цих іграх.

Під час нічного перевезення з одного місця до іншого чоловікові, який звернувся по допомогу до міжнародної організації, вдалося втекти. Де їх тримали йому не відомо. Надалі він повернувся в Україну.

? *Визначити порядок дій правоохоронних органів у даній ситуації. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.*

### ФАБУЛА 4

Під час досудового слідства по кримінальному провадженню, внесеному до Єдиного реєстру досудових розслідувань за статтею 149 КК України (Торгівля людьми або інша незаконна угода щодо людини), встановлено, що громадянин України Петров Петро Петрович за безпосередньою змовою з громадянином Чехії, дані останнього слідству не відомі, займаються злочинною діяльністю, спрямованою на сексуальну експлуатацію жінок з метою отримання прибутку.

З цією метою Петров на сайті «Робота» в мережі Інтернет розмістив оголошення про нібито легальне працевлаштування в Чехії молодих жінок в якості офіціанток в ресторанах та нічних клубах, пропонуючи високу заробітну плату та привабливі умови, заздалегідь вводячи в оману майбутніх потерпілих відносно дійсного характеру їх діяльності.

Також слідством встановлено, що Петров для зв'язку зі своїм закордонним спільником використовує особистий мобільний телефон з номером 067-300-30-30, IMEI 300200200300200.

За місцем свого проживання м. Київ, вулиця Борщагівська, 10, кв. 22 зберігає ноутбук LENOVO, який також використовує для зв'язку через мережу Інтернет та накопичує інформацію про завербованих потерпілих, їхні борги за організацію поїздки та виготовлені документи.

Під час досудового слідства встановлено, що Петров проводить зустрічі з майбутніми потерпілими в приміщенні ресторанного комплексу «Багратіон», розташованому в м. Києві, вулиця Теремківська, 2/178, де обговорює з ними організацію поїздки, отримання закордонного паспорту, відкриття віз, умови роботи та оплати праці.

Під час вербування потерпілих для правдоподібності своїх злочинних намірів, Петров пред'являє останнім недійсні запрошення від чеської фірми на нібито легальне працевлаштування, зазначені

## КОМПЛЕКСНА ВПРАВА

запрошення він отримує від свого спільника через міжнародне поштове відправлення в установі поштового зв'язку «Укрпошта» в м. Києві, вулиця Грінченка, 52/34.

У разі коли завербована особа є неповнолітньою, Петров за місцем свого проживання самостійно підроблює закордонний паспорт на її прізвище, а також займається виготовленням підроблених штампів та печаток з текстом різних регіонів Державної міграційної служби.

Також слідством встановлено, що грошові кошти за доставлених жінок та відсотки від примусової сексуальної експлуатації потерпілих Петров отримує у відділенні банку в м. Києві, вулиця Грушевського, 31/12, які переказує на його ім'я спільник з Чехії за допомогою міжнародної платіжної системи Western Union.

? *Визначити порядок дій правоохоронних органів у даній ситуації. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.*

# ДОДАТОК А

## ТЕРМІНОЛОГІЯ

| | |
|---|---|
| **IP-АДРЕСА** | ідентифікатор (унікальний числовий номер) мережного рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP |
| **АНАЛІЗАТОР ПРОТОКОЛІВ** | спеціалізовані програмні або апаратні модулі для мереж, які за допомогою певних процедур збирають весь або частину трафіку мережі для подальшого аналізу |
| **БАНЕР** | частина WEB-сторінки, в якій, зазвичай, розміщено рекламу |
| **ВЕБ-СЕРВЕР** | сервер, призначений для відображення інформації в мережі Інтернет |
| **ГЛОБАЛЬНІ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ** | іноземні та міжнародні мережі передачі даних, у тому числі мережа Інтернет |
| **ДАНІ** | інформація в електронному вигляді, яка створюється, зберігається та передається з використанням глобальних мереж |
| **ДОМЕН** | частина адресного простору в мережі Інтернет, призначена для ідентифікації комп'ютера або групи комп'ютерів. Домени поділяються на піддомени або домени нижчих рівнів |
| **ДОМЕННЕ ІМ'Я** | буквено-цифровий вираз, що ідентифікує будь-який комп'ютер абонента у мережі Інтернет |
| **КОМП'ЮТЕР** | пристрій для обробки даних |
| **ЛОГ-ФАЙЛ** | файл пртоколювання дій програми |
| **ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ** | нефізичні компоненти комп'ютерної системи та кібер-інфраструткури |
| **ПРОКСІ-СЕРВЕР** | сервер (комп'ютерна система або програма) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережних сервісів |
| **СЕРВЕР** | сукупність апаратних і програмних засобів, призначених для обслуговування інформаційних запитів комп'ютерів абонентів у мережах передачі даних |
| **СЕРВЕР СИСТЕМИ ДОМЕННИХ ІМЕН** | сукупність апаратних і програмних засобів, які забезпечують розподіл запитів комп'ютерів абонентів |
| **СЕСІЯ** | час активного з'єднання |
| **ФЕЙК** | несправжні систематизовані відомості |
| **ФОРУМ** | інтернет-ресурс, популярний вид спілкування в Інтернеті, за визначеними темами |
| **ХОСТИНГ** | надання послуг з розміщення мережних ресурсів |

# ДОДАТОК Б

## КОРИСНІ ПОСИЛАННЯ

| | |
|---|---|
| МЕРЕЖНІ СХОВИЩА | https://www.dropbox.com<br>https://yadi.sk, https://drive.google.com<br>https://mega.co.nz<br>http://www.ge.tt |
| ПЕРЕЛІК ІСНУЮЧИХ БЕЗКОШТОВНИХ VPN-МЕРЕЖ | http://www.makeuseof.com/tag/7-completely-free-vpn-services-protect-privacy |
| ПОШУК ВИДАЛЕНИХ СТОРІНОК | http://www.cachedpages.com/<br>http://www.archive.org/ |
| ПОШУК ЗАВАНТАЖЕНЬ З ВИЗНАЧЕНОЇ IP-АДРЕСИ | https://iknowwhatyoudownload.com/ru/peer/ |
| ПОШУК ЗА РІЗНИМИ УСТАНОВЧИМИ ДАНИМИ | http://www.nomer.org<br>http://www.yasni.ru<br>http://www.radaris.com<br>http://lookup.com<br>https://www.imena.ua/blog/ukraine-database/<br>http://osintframework.com/<br>https://youcontrol.com.ua<br>http://findmobil.info/ |
| ПОШУК ЗОБРАЖЕННЯ ОСОБИ | http://www.facesaerch.com<br>http://www.tofinder.ru/index.php<br>https://images.google.com/imghp?tbm=isch&tbs=itp:fface&gws_rd=ssl |
| ПОШУК ЗА ЗОБРАЖЕННЯМ | http://www.findbyface.com/<br>https://findface.ru/ |
| ПОШУК ЗОБРАЖЕНЬ (КОПІЙ) | http://images.google.com<br>http://images.search.yahoo.com<br>http://www.tineye.com |
| ПОШУК КОНТАКТІВ «ПЕРВОИСКАТЕЛЬ» | http://pervoiskatel.ru |
| ПОШУК ЛЮДЕЙ ЗА ПРІЗВИЩЕМ В СОЦІАЛЬНИХ МЕРЕЖАХ | http://socpoisk.com<br>http://www.ph4.ru/service_socsearch.ph4?a=social |
| ПОШУК ПО ОНЛАЙН ЩОДЕННИКАХ | http://www.liveinternet.ru<br>http://www.livejournal.com<br>http://tumblr.com |
| ПОШУК ПО ПРОФІЛЯХ GOOGLE+ | http://google.com/profiles |

| | |
|---|---|
| ПОШУК ПО СЕРВІСАХ ОБМІНУ ФОТОГРАФІЯМИ І ВІДЕОЗАПИСАМИ | http://www.youtube.com<br>http://rutube.ru<br>http://instagram.com<br>http://flickr.com<br>http://picasa.google.com |
| ПОШУК СЕРЕД ОСІБ, ЯКІ ПОСТУПАЛИ У ВИЩІ НАВЧАЛЬНІ ЗАКЛАДИ УКРАЇНИ | http://vstup.info |
| СЕРВІСИ ДЛЯ ЗБИРАННЯ ІНФОРМАЦІЇ ПРО ЕЛЕКТРОННІ РЕСУРСИ ЗА АДРЕСАМИ | http://robtex.com,<br>http://he.net<br>http://facebook.com, http://plus.google.com, http://myspace.com |
| СОЦІАЛЬНІ МЕРЕЖІ | http://facebook.com<br>http://plus.google.com<br>http://myspace.com |
| ЯНДЕКС.ПОШУК ЛЮДЕЙ В СОЦІАЛЬНИХ МЕРЕЖАХ (ВКОНТАКТЕ, FACEBOOK, TWITTER, GOOGLEPLUS, МОЙКРУГ, LIVEJOURNAL, ЯРУ) | http://people.yandex.ru |
| WEB-АРХІВИ | http://archive.is/<br>http://archive.org/ |
| ПОШУК РОЗТАШУВАННЯ ТОЧОК ДОСТУПУ WI-FI ЗА MAC-АДРЕСОЮ АБО НАЗВОЮ (ДЛЯ ПОШУКУ ПОТРІБНО ЗАРЕЄСТРУВАТИСЬ) | https://www.wigle.net/ |
| ФІШІНГОВІ САЙТИ | https://ema.com.ua/report-an-incident/black-list/ |
| ФОРУМ ІЗ ОБГОВОРЕННЯМИ РІЗНИХ ПРОТИПРАВНИХ ТЕХНІК (У ТОМУ ЧИСЛІ ЗЛАМАНІ БАЗИ) | http://phreaker.pro/ |

# ДОДАТОК В

## ЗРАЗКИ ДОКУМЕНТІВ

### ЗАПИТ НА ВСТАНОВЛЕННЯ ІНФОРМАЦІЇ ПРО КОРИСТУВАЧА IP-АДРЕСИ

**[реквізити підрозділу]**

_____ 20_ року № _____

На № _____ від _____

Директору _____ філії

ПАТ «Укртелеком»

_____

**Шановний _____!**

У зв'язку з виконанням окремого доручення слідчого № _____ від 201_ року по кримінальному провадженню № _____ від 201_ року, відкритого за ознаками злочину, передбаченого ч. 4 ст. 301 Кримінального кодексу України, на підставі ст. 23 Закону України «Про Національну поліцію», ст. 41 Кримінального процесуального кодексу України прошу Вас надіслати на адресу Управління / Відділу відомості щодо абонентів (у тому числі номери телефонів та IMEI мобільних терміналів), які для з'єднання з глобальною мережею Інтернет використовували наступні IP-адреси:

1. _____ – __.__.20__ о 22:55:13;
2. _____ – __.__.20__ о 18:01:06;
3. _____ – __.__.20__ о 12:59:08;
4. _____ – __.__.20__ о 19:30:03;
5. _____ – __.__.20__ об 11:51:33.

Враховуючи вкрай обмежений термін на проведення заходів, прошу сприяння у наданні зазначеної інформації в якомога стислий строк.

**З повагою,**

**начальник управління / відділу** _____

Вик. _____ _._.

тел. ___-__-__

т. м. 0_____

## ПРОТОКОЛ ОГЛЯДУ ВЕБ-СТОРІНКИ

### ПРОТОКОЛ ОГЛЯДУ

м. _____ ___ _____ 20__ року

Огляд розпочато о/об __ год. __ хв.

Огляд закінчено о/об __ год. __ хв.

Оперуповноважений *посада звання П.І.Б.* у приміщенні *назва приміщення*, розташованого за адресою: *адреса* з дотриманням вимог статей 104, 105, 106, 234, 237, 223 КПК України, за дорученням слідчого *дані слідчого* по кримінальному провадженню № _____, порушеного за ознаками злочину, передбаченого ч.__ ст. ___ КК України, щодо невстановлених осіб, які *коротка фабула* провів огляд Інтернет-сторінки, яка розміщена за адресою: http://_____.

Огляд проводився у приміщенні, при змішаному освітленні, в ясну погоду.

У РЕЗУЛЬТАТІ ОГЛЯДУ ВСТАНОВЛЕНО:

Огляд проводився із використанням комп'ютеру *назва та склад комп'ютера*, під'єднаного до мережі Інтернет, операційна система *назва*, Інтернет-браузер *назва версії* __.

З метою огляду зазначеного сайту, в адресний рядок браузера назва було введено URL адресу http://_____ та натиснута клавіша «Enter», у результаті чого завантажилася сторінка Інтернет *«Назва сторінки»*.

Під час огляду встановлено наступне:

_____

На цьому огляд сторінки закінчено.

Копія оглянутої сторінки була збережена у вигляді файла на жорсткий диск комп'ютеру, використовуваного для огляду, у тому вигляді, як вона була виявлена.

Протокол огляду склав:

**Оперуповноважений**

_____ _____

## ЗАПИТ ПРО ВЛАСНИКА ЕЛЕКТРОННОГО ГАМАНЦЯ

**[реквізити підрозділу]**

_____ 20_ року № _____

На № _____ від _____

**ТОВ «ДМ-Україна»**

вул. Марії Раскової, 11, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який зареєстрував та використовує Інтернет-гаманець з ідентифікатором WMID _____, вказати номер телефону, використаний клієнтом під час реєстрації, ідентифікуючі дані комп'ютера, програмне забезпечення та IP-адреси, за допомогою яких здійснювався доступ до системи управління вказаним обліковим записом, надати виписку операцій по його гаманцям, а у разі здійснення операцій із переведення коштів до фінансово-кредитних установ, прошу зазначити реквізити відповідних рахунків.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

**Начальник управління / відділу** _____

Вик. _____ _._.

тел. ___-__-__

т. м. 0_____

## ЗАПИТ ПРО ВЛАСНИКА ЕЛЕКТРОННОЇ ПОШТОВОЇ АДРЕСИ

**[реквізити підрозділу]**

_____ 20_ року № _____

На № _____ від _____

**ТОВ «Реєстратор»**

вул. Богомольця, 1, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який зареєстрував та використовує електронну поштову скриньку _____@ukr.net.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

**Начальник управління / відділу** _____

Вик. _____ _._.

тел. ___-__-__

т. м. 0_____

## ЗАПИТ ПРО КОРИСТУВАЧА IP-АДРЕСИ

**[реквізити підрозділу]**

_____ 20_ року № _____

На № _____ від _____

**ТОВ «Інтернет Провайдер»**

вул. Хрещатик, 10, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який дата для доступу до всесвітньої інформаційної системи загального доступу Інтернет використовував IP-адресу ***.***.***.***.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

**Начальник управління / відділу** _____

Вик. _____ _._.

тел. ___-__-__

т. м. 0_____

## ЗАПИТ ПРО ВЛАСНИКА ДОМЕНУ

**[реквізити підрозділу]**

_____ 20_ року № _____

На № _____ від _____

**ТОВ «Хостинг»**

вул. Хрещатик, 10, м. Київ

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який протягом *період часу* використовував (-є) сервер (мережне обладнання) з IP-адресою ***.***.***.*** для розміщення на ньому сайту *домен* (лише у випадку послуг VPS-хостингу), а також інформацію про внесення зазначеним клієнтом оплати за отримані телекомунікаційні послуги. У разі наявності відповідних договорів або бухгалтерських документів прошу надіслати їх завірені копії.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

**Начальник управління / відділу** _____

Вик. _____ _._.

тел. ___-__-__

т. м. 0_____

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Про заходи щодо протидії торгівлі людьми: Конвенція Ради Європи від 16.05.2005, ратифікована Верховною радою України 21.09.2010. Офіційний вісник України. 2011. № 16. С. 329. Ст. 706.
2. Про кіберзлочинність : конвенція Ради Європи від 07.09.2005, ратифікована Верховною Радою України 07.09.2005. URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення: 22.09.2017).
3. Кримінальний кодекс України від 05.04.2001. Відомості Верховної Ради України. 2001. № 25-26 (29.06.2001). ст. 131.
4. Науково-практичний коментар Кримінального кодексу України / А. М. Бойко [ та ін.] ; за ред. М. І. Мельника, М. І. Хавронюка. 4-е вид., переробл. та доп. Київ : Юридична думка, 2007. 1184 с.
5. Узагальнення судової практики розгляду кримінальних справ (проваджень), пов'язаних із торгівлею людьми або іншою незаконною угодою щодо людини розглянутих Мурованокуриловецьким районним судом у 2012 році та і півріччі 2013 року. URL: http://mr.vn.court.gov.ua/sud0216/analiz/50237 (дата звернення: 22.09.2017).
6. Ухвала Колегії суддів Судової палати у кримінальних справах Верховного Суду України від 29 січня 2004 року, справа №5*5180 // Куц В. М., Орлеан А. М. Прокурорські засоби протидії торгівлі людьми: науково-практичний посібник / за ред. Г. П. Середи. К. : Варта, 2007. 168 с.
7. Вирок Бориспільського міськрайонного суду Київської області від 17.02.2014. URL: http://www.reyestr.court.gov.ua/Review/38915249 (дата звернення: 22.09.2017).
8. Вирок Приморського районного суду м. Одеси від 06 вересня 2016 року. URL: http://www.reyestr.court.gov.ua/Review/61524352 (дата звернення: 22.09.2017).
9. Вирок Хортицького районного суду м. Запоріжжя від 01 грудня 2014 року. URL: http://www.reyestr.court.gov.ua/Review/41745144 (дата звернення: 22.09.2017).
10. Вирок Тальнівського районного суду Черкаської області від 01.10.2013 року. URL: http://www.reyestr.court.gov.ua/Review/34251659 (дата звернення: 22.09.2017).
11. Вирок Котовського міськрайонного суду Одеської області від 29.06.2017 року. URL: http://www.reyestr.court.gov.ua/Review/67446334 (дата звернення: 22.09.2017).
12. Вирок Луцького міськрайонного суду Волинської області від 21.07.2016. URL: http://www.reyestr.court.gov.ua/Review/59090312 (дата звернення: 22.09.2017).
13. Вирок Апелляційнного суду Харьківської області від 19.11.2012. URL: http://www.reyestr.court.gov.ua/Review/44554334 (дата звернення: 22.09.2017).
14. Вирок Звенигородського районного суду від 11.04.2013 року. URL: http://www.reyestr.court.gov.ua/Review/30731811 (дата звернення: 22.09.2017).
15. Вирок Кременецького районного суду Тернопільської області від 11 листопада 2016 року. URL: http://www.reyestr.court.gov.ua/Review/66497188 (дата звернення: 22.09.2017).
16. Вирок Центрально-Міського районного суду м. Кривого Рогу від 27 квітня 2016 року. URL: http://www.reyestr.court.gov.ua/Review/57478543 (дата звернення: 22.09.2017).
17. Вирок Рахівського районного суду Закарпатської області від 30 червня 2011 року. URL: http://www.reyestr.court.gov.ua/Review/18501407 (дата звернення: 22.09.2017).
18. Реалізація права потерпілих від торгівлі людьми на компенсацію та відшкодування в Україні: аналіз ситуації / [І.О. Бандурка та ін.]; за заг. ред. О. М. Бандурки, К. Б. Левченко. К., 2012. 90 с.
19. Про внесення змін до статті 149 Кримінального кодексу України (щодо приведення у відповідність до міжнародних стандартів): текст законопроекту №6243 від 27.03.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61428 (дата звернення: 07.11.2017).
20. Підгородинський В. М. Відповідальність за торгівлю людьми за кримінальним законодавством України: автореф. дис. … канд. юрид. наук: спец. : 12.00.08. Одеса, 2005. 22 с.
21. Марков В. В. Торгівля людьми як порушення прав людини / В. В. Марков // Матеріали науково-практичної конференції «Проблеми розкриття, розслідування та попередження кіберзлочинів та злочинів пов'язаних з торгівлею людьми» (17 травня 2011 року, м. Харків). Х., 2011. С. 12-14.
22. Ukraine : 2017 Trafficking in Persons Report: Country Narrative. URL: https://www.state.gov/j/tip/rls/tiprpt/countries/2017/271306.htm (дата звернення: 22.09.2017).
23. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів: текст законопроекту №6232 від 23.03.2017 до другого читання (розділ II) 13.07.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=61415&pf35401=429428 (дата звернення: 22.09.2017).
24. Electronic evidence guide a basic guide for police officers, prosecutors and judges. Version 2.0. Cybercrime Division. Directorate General of Human Rights and Rule of Law. Strasbourg, France, 15 December 2014.

25. Рекомендація Rec (2000) 19 Комітету Міністрів Ради Європи державам-членам щодо ролі прокуратури в системі кримінального правосуддя, ухвалена Комітетом Міністрів Ради Європи на 724 засіданні заступників міністрів 6 жовтня 2000 року. URL: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/7864c99c46598282c2257b4c0037c014/7442a47eb0b374b9c2257d8700495f8b/$FILE/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%8F%20Rec%20(2000)%2019.pdf (дата звернення: 22.09.2017).

26. Вирок апеляційного суду Дніпропетровської області від 29.06.2017. URL: http://www.reyestr.court.gov.ua/Review/67469526 (дата звернення: 22.09.2017).

27. Вирок Святошинського районного суду м. Києва від 14.12.2015 року. URL: http://www.reyestr.court.gov.ua/Review/67440368 (дата звернення: 22.09.2017).

28. Навчальний посібник для суддів з питань судового провадження у кримінальних справах щодо торгівлі людьми з метою експлуатації праці / А. М. Орлеан, В. В. Касько, О. В. Пустова, Н. М. Ахтирська, О. А. Шаповалова, О. Г. Горбунова, О. Л. Кустова, О. А. Стрельцова, І. П. Лисенко. Київ : Фенікс, Представництво Міжнародної організації з міграції в Україні, 2014. С. 47.

29. Полюхович О. І. До питання використання як доказів матеріалів, отриманих за результатами проведення негласних слідчих (розшукових) дій. Часопис цивільного і кримінального судочинства. 2016. № 3(30). С. 97-108.

30. Постанова судової палати у кримінальних справах Верховного Суду України від 16.03.2017. URL: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/%28documents%29/46445E8A79A38 (дата звернення: 22.09.2017).

31. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с. URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf (дата звернення: 28.09.2017).

32. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 28.09.2017).

33. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 28.09.2017).

34. Манжай О. В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. Jurnalul Juridic National: Teorie si Practică. 2015. № 3(13). С. 100-105.

35. Carter J. G., Phillips S. W., Gayadeen S. M. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. Journal of Criminal Justice. 2014. № 42. P. 433-442.

36. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 28.09.2017).

37. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2016. № 3(75). С. 256-265.

38. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.

39. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (дата звернення: 22.09.2017).

40. Ташмагамбетов А. М. Оперативно-розыскные мероприятия с использованием социальных сетей: опыт Великобритании и Республики Казахстан. Наука и бизнес: пути развития. 2013. № 11 (29). С. 129-133.

41. Greenemeier L. A new set of search tools called Memex, developed by DARPA, peers into the «deep Web» to reveal illegal activity. URL: https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/ (дата звернення: 22.09.2017).

42. Соцсети позволяют легко найти номера мобильных телефонов многих пользователей. URL: http://www.securitylab.ru/news/440882.php (дата звернення: 22.09.2017).

43. Unique in the Crowd: The privacy bounds of human mobility / Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel. URL: http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html (дата звернення: 22.09.2017).

44. Trafficking in human beings: Internet recruitment: lections/ Athanassia P. Sykiotou. Directorate General of Human Rights and Legal Affairs Council of Europe, 2007. 150 p.

45. 2016 UNODC Global Report on Trafficking in Persons. URL: http://www.unodc.org/unodc/data-and-analysis/glotip.html (дата звернення: 22.09.2017).

46. Протидія торгівлі людьми в Україні: Статистика МОМ станом на 30 червня 2017 р. URL: http://iom.org.ua/sites/default/files/iom_vot_statistics_ukr_june2017.doc (дата звернення: 22.09.2017).

47. Збереження і отримання записів від провайдерів Інтернет-послуг в Сполучених Штатах Америки: довідник для правоохоронних органів іноземних країн. 2014. 33 с.

48. Social bookmarking. URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 22.09.2017).

49. Бандурка О. М., Перпелиця М. М., Манжай О. В., Шендрик В. В. Оперативно-розшукова компаративістика: монографія. Х. : Золота миля, 2013. 352 с.: іл.

50. Кримінальний процесуальний кодекс України : від 13.04.2012. Голос України. 2012. № 90-91.

51. Європейська конвенція про взаємну допомогу у кримінальних справах від 20.04.1959, ратифікована Верховною радою України 16.01.1998. Офіційний вісник України. 2004. № 26. С. 231. Ст. 173.

52. Електронна дошка оголошень. URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 22.09.2017).

53. Вирок Бориспільського міськрайонного суду Київської області від 06.03.2014 : Справа № 359/3337/13-к. URL: http://www.reyestr.court.gov.ua/Review/38915249 (дата звернення: 22.09.2017).

54. Вирок Московського районного суду м. Харкова від 15.11.2014 : Справа № 643/13575/14-к. URL: http://www.reyestr.court.gov.ua/Review/41233672 (дата звернення: 22.09.2017).

55. Ухвала Апеляційного суду Волинської області від 20.08.2013 : Справа № 1-78/2011. URL: http://www.reyestr.court.gov.ua/Review/33105682 (дата звернення: 22.09.2017).

56. Вирок Жовтневого районного суду м. Дніпропетровська від 01.03.2016 : Справа 201/5058/15-к URL: http://reyestr.court.gov.ua/Review/56296689 (дата звернення: 16.11.2017).

57. Радутний О. Е. Інформація, яка надходить у режимі реального часу через веб-камеру, як предмет злочину, що передбачений ст. 301 КК України / О. Е. Радутний // Інформація і право. – 2014. – № 1. – С. 115-119. – Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2014_1_16.

58. Марков В. В. Особливості впровадження зарубіжного досвіду боротьби з кіберзлочинністю в навчальний процес. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція). 2014. № 12. Т. 1. С. 101-103.

59. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к. URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 22.09.2017).

60. Вирок Золотоніського міськрайонного суду Черкаської області від 25.12.2012 : Справа № 1-218/11. URL: http://www.reyestr.court.gov.ua/Review/44532917 (дата звернення: 22.09.2017).

61. Відеохостинг. URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 22.09.2017).

62. Екс-прикордонник став торговцем українськими чоловіками. URL: http://expres.ua/news/2015/07/29/145476-eks-prykordonnyk-stav-torgovcem-ukrayinskymy-cholovikamy (дата звернення: 22.09.2017).

63. Cybercrime and its victims / Edited by Elena Martellozzo, Emma A Jane. 2017. Routledge. 230 p.

64. British paedophile Paul Leighton jailed for 16 years for rape. URL: https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape (дата звернення: 22.09.2017).

65. Skype. URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 22.09.2017).

66. Манжай О. Практичні вправи до тренінгу з виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (м. Харків, 20-24 березня 2017 року). Х., 2017. 51 с.

67. Are you sharing the same IP address as a criminal? Law enforcement call for the end of Carrier Grade NAT (CGN) to increase accountability online. URL: https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online (дата звернення: 20.10.2017).

68. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями на 19.04.2014]. Офіційний вісник України. 2001. № 20 (01.06.2001). ст. 828.

69. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями на 12.11.2014]. Офіційний вісник України. 2010. № 100 (04.01.2011). ст. 3571.

70. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

71. Криптовалюта. URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 22.09.2017).

72. WebMoney. URL: https://uk.wikipedia.org/wiki/WebMoney (дата звернення: 22.09.2017).

73. Ухвала Печерського районного суду міста Києва від 01.03.2017. URL: http://www.reyestr.court.gov.ua/Review/65121588 (дата звернення: 22.09.2017).

74. Ухвала Апеляційного суду м. Києва від 02.02.2017. URL: http://www.reyestr.court.gov.ua/Review/64737344 (дата звернення: 22.09.2017).

75. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.

76. Запотоцький А. П. Документи як процесуальні джерела доказів у кримінальному судочинстві : автореф. на здобуття наукового ступеня кандидата юридичних наук. – К.,2009. – 18 с.

77. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. Вісник Харківського національного університету внутрішніх справ. 2016. № 3(74). С. 111-120.

78. Про судову експертизу: закон України від 25.02.1994 р.; [із змінами і доповненнями на 01.04.2015]. Відомості Верховної Ради України. 1994. № 28 (12.07.1994). – ст. 232.

79. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України № 53/5 від 08.10.1998 р. [із змінами і доповненнями на 22.01.2013]. Офіційний вісник України. 1998. № 46 (03.12.1998). ст. 1715.

80. Манжай О. В., Бучак Т. А Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практичної конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського національного ун-ту внутр. справ. 2008. С. 151-153.

81. Kuhlee and Voelzow. Computer Forensik Hacks / O'Reilly. 2012. ISBN 978-3-86899-121-5 (http://www.forensikhacks.de).

82. Манжай О. В., Осятинська І. А. Використання спеціалізованого програмного забезпечення для роботи з мобільними телефонними пристроями // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжнарод. наук.-практ. конф. (Харків, 12 листопада 2014 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х. : Права людини, 2014. С. 143-145.

83. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016, ратифікована Верховною радою України 12.07.2017. Офіційний вісник України. 2017. № 62. С. 5. Ст. 1901.

84. Біленчук П. Д., Борисова Л. В., Паніотов Є. К. Взаємодія правоохоронних органів України та країн світу при розслідуванні електронних високотехнологічних транснаціональних злочинів. Право і безпека. 2003. 4(1). С. 54-59.

85. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями на 19.04.2014]. Офіційний вісник України. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.

86. Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку, та внесення поправок в Директиву 2002/58/ЄС: Директива 2006/24/ЄС Європейського парламенту і Ради Європи від 15.03.2006 року. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:FR:PDF (дата звернення: 22.09.2017).

87. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги : нормативний документ : затверджений спільним наказом Служби безпеки України та Адміністрації Держспецзв'язку від 13.02.2014 № 48/75. URL: http://ssu.kmu.gov.ua/sbu/doccatalog/document?id=122377 (дата звернення: 22.09.2017).

88. Методичні рекомендації щодо виконання вимог міжнародних договорів та КПК України про міжнародну правову допомогу при проведенні процесуальних дій у кримінальному провадженні, схвалені протоколом засідання науково-методичної ради 20.04.2017 № 3.

89. Інструкція про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів, затверджена спільним наказом № 3/1/2/5/2/2 Міністерства внутрішніх справ, Генеральної прокуратури, Служби безпеки, Державного комітету у справах охорони державного кордону, Державної митної служби, Державної податкової адміністрації від 09.01.1997. Офіційний вісник України. 1997. № 9.

90. Дубина В. І. Використання можливостей Укрбюро Інтерполу в протидії злочинам, пов'язаним з торгівлею людьми. Науковий вісник національної академії внутрішніх справ. 2014. № 4. С. 198-210.

91. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. Форум права. 2013. № 1. С. 646-650. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/FP_index.htm_2013_1_109.pdf. (дата звернення: 22.09.2017)

92. Торговля людьми и легализация преступных доходов. Вопросы противодействия: научно-практическое пособие / [А. Андреани и др.]: под. ред. О. П. Левченко. М. : ЮНИТИ-ДАНА, 2009. 271 с.