Протокол Берклі

з ведення розслідувань з використанням відкритих цифрових даних

Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права

| ПОПЕРЕДНЯ ВЕРСІЯ |

ЦЕНТР З ПРАВ ЛЮДИНИ
Юридична школа Каліфорнійського університету в Берклі

ОБ'ЄДНАНІ НАЦІЇ
ПРАВА ЛЮДИНИ
УПРАВЛІННЯ ВЕРХОВНОГО КОМІСАРА

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

HR/PUB/20/2 (попередня версія)

Ця попередня версія спільно опублікована Організацією Об'єднаних Націй від імені Управління Верховного комісара ООН з прав людини (УВКПЛ) та Центру з прав людини Каліфорнійського університету в Берклі, Юридична школа.

Подяка за обкладинку: супутниковий знімок з інформаційною цифровою фабрикацією, створений Ахмедом Елгамал (Ahmed Elgamal) за допомогою платформи штучного інтелекту Playform.

Центр з прав людини Каліфорнійського університету, Берклі, Юридична школа, вдячний за фінансову підтримку, отриману від таких спонсорів: Sigrid Rausing Trust; Oak Foundation; індивідуальні спонсори в Каліфорнійському університеті, Берклі; Фонд «Відкрите суспільство» (Open Society Foundations); та Rockefeller Foundation Bellagio Center.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Протокол Берклі

з ведення розслідувань з використанням відкритих цифрових даних

Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права

| ПОПЕРЕДНЯ ВЕРСІЯ |

ЦЕНТР З ПРАВ ЛЮДИНИ
Юридична школа Каліфорнійського університету в Берклі

ОБ'ЄДНАНІ НАЦІЇ
ПРАВА ЛЮДИНИ
УПРАВЛІННЯ ВЕРХОВНОГО КОМІСАРА

Нью-Йорк і Женева, 2020 рік

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Зміст

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Передмова

З початку 1990-х років цифрові інструменти та Інтернет, як камера і телефон перед ними, докорінно змінили спосіб отримання, збирання та поширення нами інформації про порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини.

Сьогодні слідчі можуть збирати дані про потенційні порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини, за допомогою великої кількості загальнодоступних супутникових знімків, відео та фотографій, включаючи матеріали, завантажені в Інтернет зі смартфонів та публікацій на платформах соціальних мереж. Такий розвиток подій допоміг слідчим обійти урядових та інших традиційних контролерів інформації для доступу до ключової інформації про правопорушення, навіть у режимі реального часу, яка в іншому випадку залишалася б прихованою для очей громадськості.

Однак цифрова інформація у відкритому доступі використовувалася переважно у конкретних випадках, оскільки правозахисні організації, міжурядові органи, слідчі механізми та суди часом намагалися адаптувати свою робочу практику, щоб включити нові цифрові методи встановлення фактів та аналізу. Однією з найбільших проблем, з якими вони стикаються, є вирішення питань виявлення та перевірки відповідних матеріалів у межах збільшення обсягу онлайн-інформації, особливо фотографій та відеозаписів, знятих на смартфони та інші мобільні пристрої, деякі з яких можуть бути скомпрометовані або неправильно віднесені.

Тим часом, поява міжнародних кримінальних судів та слідчих механізмів, а також національних підрозділів у справах військових злочинів ще більше посилила потребу у спільних стандартах для збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах. Для того щоб інформація у відкритому доступі була прийнятною як доказ у суді, прокурори та адвокати, як правило, повинні мати змогу встановити її достовірність та ланцюг забезпечення збереження.

Належне поводження та обробка цього матеріалу значно збільшить ймовірність того, що він може бути використаний прокурорами та адвокатами. Однак, якщо використовуються нерозумні методи збирання та збереження, інформація не може вважатися достовірною для встановлення фактів у справі. Суди та слідчі механізми мають користуватися чіткими критеріями для оцінки ваги інформації у відкритому доступі як зв'язку або як доказу конкретного злочину. Спільні методологічні стандарти щодо автентифікації та перевірки однаково слугуватимуть місіям з виявлення фактів у сфері прав людини, які також все частіше включають цифрові матеріали у відкритому доступі у свої розслідування. Слідчі комісії, компоненти з прав людини в операціях з підтримання миру, периферійні відділення Управління Верховного комісара ООН з прав людини (УВКПЛ) та інші зусилля Організації Об'єднаних Націй з питань моніторингу та розслідування прав людини отримують вигоду від обґрунтованих методологічних принципів та підходів щодо підтвердження достовірності та ваги їхніх висновків.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Щоб задовольнити цю потребу, наші установи, Центр з прав людини Каліфорнійського університету в Берклі, Юридична школа та УВКПЛ, об'єднали зусилля для публікації *Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних: Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права*. Шлях до цієї публікації розпочався у кампусі Берклі у 2009 році, коли Центр з прав людини зібрав юристів, технологів, журналістів та активістів для розробки стратегій використання цифрових технологій та методологій для виявлення та документування порушень прав людини. З тих пір Центр з прав людини провів низку міждисциплінарних семінарів у співпраці з рядом технічних, юридичних та методологічних експертів, у тому числі з УВКПЛ, для мозкового штурму, розробки нових інструментів та визначення та усунення критеріїв, стандартів та методів розкриття, оцінки, перевірки та збереження цифрової інформації у відкритому доступі для документування порушень прав людини та притягнення винних до відповідальності. Цей процес добре узгоджується із зусиллями УВКПЛ щодо розробки вказівок та інструментів для підтримки та надання консультацій комісіям Організації Об'єднаних Націй з питань розслідування та встановлення фактів та персоналу УВКПЛ щодо їх все більшого використання інформації у відкритому доступі у процесі встановлення фактів та розслідування.

Протокол Берклі був розроблений за допомогою внесків осіб з різними професійними перспективами, юридичним та культурним походженням, статтю та національністю, та для його розробки було проведено понад 150 консультацій з експертами та отримано внесок від ключових зацікавлених сторін, включаючи слідчих ООН з прав людини. Він також спирався на досвід спеціалізованих робочих груп Секції методології, освіти та навчання УВКПЛ та Канцелярії прокурора Міжнародного кримінального суду. Відповідно до міжнародних стандартів щодо розробки нової методології, УВКПЛ та Центр з прав людини піддали Протокол Берклі суворому процесу перегляду, перевірки та валідації.

Спираючись на цей підхід до співпраці, Протокол Берклі включає міжнародні стандарти для проведення онлайн-досліджень щодо ймовірних порушень міжнародного права в області прав людини та міжнародного гуманітарного та кримінального права. Він також містить вказівки щодо методологій та процедур збору, аналізу та збереження цифрової інформації у професійному, юридичному та етичному порядку. Нарешті, Протокол Берклі визначає заходи, які онлайн-слідчі можуть вжити для захисту цифрової, фізичної та психосоціальної безпеки для себе та інших, включаючи свідків, жертв та осіб, які надають першу допомогу (наприклад, громадян, активістів та журналістів), які ризикують власним благополуччям і документують порушення прав людини та серйозні порушення міжнародного права.

Протокол Берклі йде слідами двох попередніх протоколів Організації Об'єднаних Націй: Міннесотського протоколу з розслідування потенційно незаконного позбавлення життя (1991 рік, оновлено у 2016 році) та Посібника з питань ефективного розслідування і документування фактів катувань та іншого жорстокого, нелюдського чи такого, що принижує гідність, поводження або покарання (Стамбульський протокол) (1999 рік, оновлено у 2004 році). Міннесотський протокол, розроблений юристами та криміналістами, які займалися пошуком зниклих осіб у 1980-х роках, встановлює міжнародні стандарти та

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

процедури для проведення медико-правових розслідувань щодо підозрілих смертей або смертей, залишених без уваги, та служить засобом оцінки достовірності таких розслідувань. Так само Стамбульський протокол надає лікарям та адвокатам вказівки щодо того, як розпізнавати та документувати фізичні та психосоціальні наслідки катувань, щоб документація могла служити дійсним доказом у суді чи в інших контекстах, включаючи розслідування та моніторинг прав людини. Усі три протоколи ґрунтуються на переконанні, що наука, техніка та право можуть – і повинні – працювати разом на службі прав людини. Як і попередні протоколи, Протокол Берклі буде доступний офіційними мовами Організації Об'єднаних Націй для полегшення його використання та забезпечення його корисності в усьому світі.

Ми сподіваємось, що у все більш оцифрованому світі Протокол Берклі допоможе онлайн-слідчим – будь то юристам, правозахисникам, журналістам чи іншим особам – розробити та впровадити ефективні процедури документування та перевірки порушень міжнародного законодавства з прав людини та міжнародного гуманітарного та кримінального права, максимально використовуючи цифрову інформацію у відкритому доступі, щоб особи, відповідальні за такі порушення, могли бути справедливо притягнуті до відповідальності.

Підпис
Ерік Стовер (Eric Stover)
Декан факультету, Центр з прав людини,
Каліфорнійський університет, Берклі,
Юридична школа

Підпис
Мішель Башле (Michelle Bachelet)
Об'єднані Нації
Верховний комісар з прав людини

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Резюме

Розслідування з використанням відкритих даних – це розслідування, які повністю або частково спираються на загальнодоступну інформацію для проведення офіційних та систематичних онлайн-розслідувань щодо передбачуваних правопорушень. Сьогодні велика кількість загальнодоступної інформації доступна через Інтернет, де цифрове середовище, що швидко розвивається, призвело до нових типів та джерел інформації, які могли б допомогти у розслідуванні передбачуваних порушень прав людини та серйозних міжнародних злочинів. Можливість розслідувати такі твердження має особливе значення для слідчих, які не можуть своєчасно фізично отримати доступ до місця злочину, що часто буває у міжнародних розслідуваннях.

Інформація у відкритому доступі може надавати підказки, підтримувати результати розвідки та служити прямим доказом у судах. Однак для того, щоб вона могла бути використана в офіційних процесах розслідування, включаючи правові розслідування, місії з встановлення фактів та слідчі комісії, слідчі повинні застосовувати послідовні методи, які одночасно підвищують точність їхніх висновків та дозволяють суддям та іншим особам, які встановлюють факти, краще оцінити якість самого процесу розслідування. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних був розроблений з метою надання міжнародних стандартів та вказівок для слідчих у галузі міжнародного кримінального правосуддя та прав людини. Такі слідчі надходять із ряду установ, включаючи засоби масової інформації, групи громадянського суспільства та неурядові організації, міжнародні організації, суди та національні та міжнародні слідчі органи. Встановлення послідовних та вимірюваних стандартів на підтримку цієї багатопрофільної сфери є засобом професіоналізації практики розслідувань з використанням даних у відкритому доступі.

Хоча керівні принципи та навчання з використання спеціальних інструментів та програмного забезпечення є суттєвою частиною покращення якості розслідувань з використанням відкритих цифрових даних, Протокол Берклі зосереджується не на конкретних технологіях, платформах, програмному забезпеченні чи інструментах, а скоріше на основних принципах та методологіях, які можна послідовно застосовувати навіть при зміні самої технології. Ці принципи визначають мінімальні правові та етичні стандарти для проведення ефективних розслідувань з використанням даних у відкритому доступі. Дотримуючись вказівок Протоколу Берклі, слідчі допоможуть забезпечити якість своєї роботи, мінімізуючи при цьому фізичні, психосоціальні та цифрові ризики для себе та інших.

Протокол Берклі розроблений як навчальний інструмент та довідковий посібник для слідчих, які використовують дані у відкритому доступі. Після вступної глави наступні три глави присвячені загальним концепціям, включаючи принципи, правові міркування та безпеку. Решта глав зосереджені на самому процесі розслідування. Цей розділ Протоколу Берклі починається з глави про підготовку та стратегічне планування, після чого йде глава, присвячена різним необхідним слідчим крокам – а саме онлайн-запитам, попередній оцінці, збору, збереженню, верифікації та слідчому аналізу. Він завершується главою про

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

методологію та принципи звітування про результати розслідування з використанням даних у відкритому доступі.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Автори та учасники

Координаційний комітет Протоколу Берклі

Ліндсі Фріман (Lindsay Freeman), старший науковий співробітник, Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа

Алекса Кеніг (Alexa Koenig), Виконавчий директор, Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа

Ерік Стовер (Eric Stover), Декан факультету, Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа

Редакційний комітет Протоколу Берклі

Сарета Ашраф (Sareta Ashraph), старший юрисконсульт; баристер, Garden Court Chambers; колишній старший аналітик, Слідча група Організації Об'єднаних Націй зі сприяння відповідальності за злочини, скоєні Даїшем/Ісламською державою в Іраку та Леванті

Алікс Данн (Alix Dunn), виконавчий директор, The Engine Room

Річард Голдстоун (Richard Goldstone), колишній суддя, Конституційний суд ПАР; колишній головний прокурор, Міжнародний трибунал по колишній Югославії та Міжнародний кримінальний трибунал по Руанді

Бренда Дж. Холліс (Brenda J. Hollis), міжнародний співпрокурор, надзвичайні палати в судах Камбоджі; колишній головний прокурор, Залишковий спеціальний суд у Сьєрра-Леоне

Таня Каранасіос (Tanya Karanasios), Директор з програм, СВІДОК

Енріке Пірас (Enrique Piraces), Менеджер медіа-програми та програми з прав людини, Центр науки про права людини, Університет Карнегі-Меллона

Бет Ван Шаак (Beth Van Schaack), запрошений професор з прав людини, Стенфордська юридична школа; колишній заступник Посла з особливих доручень з питань військових злочинів, Управління глобального кримінального правосуддя, Міністерство закордонних справ США

Мішель де Смедт (Michel de Smedt), Директор, Відділ розслідувань, Прокуратура, Міжнародний кримінальний суд

Алан Тігер (Alan Tieger), старший судовий прокурор, спеціалізована прокуратура Косово; колишній старший юрист суду, Міжнародний трибунал по колишній Югославії

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Крістіан Венавезер (Christian Wenaweser), Постійний представник Ліхтенштейну при ООН; колишній Президент, Асамблея держав-учасниць Римського статуту Міжнародного кримінального суду

Алекс Уайтинг (Alex Whiting), Керівник Відділу розслідувань, спеціалізована прокуратура Косово; практикуючий професор, Гарвардська школа права; колишній координатор прокуратури та координатор розслідувань, Прокуратура, Міжнародний кримінальний суд

Сьюзан Вольфінбаргер (Susan Wolfinbarger), співробітник відділу закордонних справ та керівник групи аналітики, Міністерство закордонних справ США; колишній Старший директор проекту, Проект геопросторових технологій, Американська асоціація розвитку науки

Консультативний комітет Протоколу Берклі

Федеріка Д'Алессандра (Federica D'Alessandra), Виконавчий директор, Оксфордська програма міжнародного миру та безпеки, Оксфордський університет; редактор *Довідника Групи міжнародного публічного права та політики щодо документації громадянського суспільства про серйозні порушення прав людини: Принципи і передова практика*

Стюарт Кейсі-Маслен (Stuart Casey-Maslen), почесний професор, юридичний факультет, Преторійський університет; учасник *Міннесотського протоколу з розслідування потенційно незаконного позбавлення життя* (2016 рік)

Елісон Коул (Alison Cole), спеціаліст-радник з прав людини, Департамент внутрішніх справ, Нова Зеландія

Франсуаза Хемпсон (Francoise Hampson), почесний професор, Юридична школа Університету Ессексу; член слідчої комісії з питань Бурунді

Крістоф Гейнс (Christof Heyns), професор права в області прав людини, Преторійський університет; член Комітету з прав людини; колишній Спеціальний доповідач з питань позасудових, скорочених або довільних страт; координатор *Міннесотського протоколу про розслідування потенційно незаконного позбавлення життя* (2016 рік)

Вінсент Якопіно (Vincent Iacopino), старший медичний радник, Лікарі з прав людини; головний учасник *Посібника з питань ефективного розслідування і документування фактів катувань та іншого жорстокого, нелюдського чи такого, що принижує гідність, поводження або покарання* (Стамбульський протокол)

Келлі Матесон (Kelly Matheson), старший адвокат та менеджер програми, СВІДОК; автор посібника *Відео як доказове поле*

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Ганні Мегалі (Hanny Megally), комісар, Незалежна міжнародна комісія з розслідувань щодо Сирійської Арабської Республіки; Старший науковий співробітник, Центр міжнародного співробітництва, Нью-Йоркський університет

Хуан Мендес (Juan Mendez), професор кафедри права прав людини за місцем проживання, Вашингтонський юридичний коледж; колишній Спеціальний доповідач з питань катувань та інших жорстоких, нелюдських чи таких, що принижують гідність, видів поводження чи покарання; координатор універсального протоколу для проведення слідчого опитування та процесуальних гарантій

Ар'є Неєр (Aryeh Neier), Почесний президент, Фонд «Відкрите суспільство» (Open Society Foundations)

Наві Піллі (Navi Pillay), Президент, Міжнародна комісія проти смертної кари; колишній Верховний комісар ООН з прав людини; колишній суддя, Міжнародний кримінальний суд; колишній Президент, Міжнародний кримінальний трибунал по Руанді

Пауло Сержіо Піньейру (Paulo Sergio Pinheiro), Голова, Незалежна міжнародна комісія з розслідувань щодо Сирійської Арабської Республіки; колишній Спеціальний доповідач із ситуації з правами людини в Бурунді; колишній Спеціальний доповідач із ситуації з правами людини в М'янмі

Томас Проберт (Thomas Probert), Викладач з надзвичайних питань, Центр з прав людини, Університет Преторії; Науковий співробітник, Центр управління та прав людини, Кембриджський університет; учасник *Міннесотського протоколу про розслідування потенційно незаконного позбавлення життя* (2016 рік)

Стівен Рапп (Stephen Rapp), заслужений науковий співробітник, Центр запобігання геноциду Саймона-Скйодта, Меморіальний музей Голокосту США; колишній Посол з особливих доручень з питань військових злочинів, Управління глобального кримінального правосуддя, Міністерство закордонних справ США; колишній прокурор, Спеціальний суд у Сьєрра-Леоне

Крістіна Рібейро (Cristina Ribeiro), координатор розслідувань, Прокуратура, Міжнародний кримінальний суд

Патрісія Селлерс (Patricia Sellers), Спеціальний радник з гендерних питань Прокурора Міжнародного кримінального суду; запрошений науковий співробітник, Коледж Келлога, Оксфордський університет; колишній юрисконсульт та адвокат суду, Міжнародний трибунал по колишній Югославії та Міжнародний кримінальний трибунал по Руанді

Учасники семінару

Семінар з нової криміналістики: Використання інформації у відкритому доступі для розслідування тяжких злочинів (Белладжіо, Італія, 2017 рік)

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Хаді аль-Хатіб (Hadi Al Khatib), Сирійський архів
Стюарт Кейсі-Маслен (Stuart Casey-Maslen), Університет Преторії
Іван Кайперс (Yvan Cuypers), Міжнародний кримінальний суд
Скотт Едвардс (Scott Edwards), Amnesty International
Ліндсі Фріман (Lindsay Freeman), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Алекса Кеніг (Alexa Koenig), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Стів Костас (Steve Kostas), Open Society Justice Initiative
Андреа Лампрос (Andrea Lampros), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Келлі Метсон (Kelly Matheson), СВІДОК
Фелім Макмехон (Felim McMahon), Міжнародний кримінальний суд
Джуліан Ніколлс (Julian Nicholls), Міжнародний кримінальний суд
Томас Проберт (Thomas Probert), Кембриджський університет
Крістіна Рібейро (Cristina Ribeiro), Міжнародний кримінальний суд
Гевін Шерідан (Gavin Sheridan), Vizlegal
Ерік Стовер (Eric Stover), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Алан Тігер (Alan Tieger), Міжнародний трибунал у справах колишньої Югославії
Марк Уотсон (Mark Watson), Комісія з питань міжнародного правосуддя та підзвітності
Гай Віллоубі (Guy Willoughby), Асоціація з вивчення військових злочинів

Семінар з побудови етичної концепції для розслідувань з використанням даних у відкритому доступі (Університет Ессексу, Сполучене Королівство, 2019 рік)

Фред Абрахамс (Fred Abrahams), Страж прав людини
Ліна Басуні (Leenah Bassouni), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Федеріка Д'Алессандра (Federica D'Alessandra), Оксфордський університет Сем Дабберлі (Sam Dubberley), Amnesty International
Дженніфер Істерді (Jennifer Easterday), JustPeace Labs
Скотт Едвардс (Scott Edwards), Amnesty International
Ліндсі Фріман (Lindsay Freeman), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Джефф Гілберт (Geoff Gilbert), Університет Ессексу
Крістофер «Кіп» Хейл (Christopher «Kip» Hale), Комісія з питань міжнародного правосуддя та підзвітності
Еванна Ху (Evanna Hu), Omelas
Габріела Івенс (Gabriela Ivens), науковий співробітник Mozilla та СВІДОК
Алекса Кеніг (Alexa Koenig), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Метт Махмуді (Matt Mahmoudi), Кембриджський університет
Лорна Макгрегор (Lorna McGregor), Університет Ессексу
Дараг Мюррей (Daragh Murray), Університет Ессексу
Вівіан Нг (Vivian Ng), Університет Ессексу

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Енріке Пірас (Enrique Piraces), Центр наук про права людини, Університет Карнегі-Меллона
Зара Рахман (Zara Rahman), The Engine Room
Саша Робехмед (Sasha Robehmed), The Engine Room
Ілля Сятіца (Ilia Siatitsa), Privacy International
Представник УВКПЛ з Секції методології, освіти та навчання

Круглий стіл з юридичних питань, що виникають на підставі розслідувань з використанням даних у відкритому доступі (Гаага, 2019 рік)

Девід Акерсон (David Ackerson), слідча група Організації Об'єднаних Націй зі сприяння відповідальності за злочини, скоєні Даїшем/Ісламською державою в Іраку та Леванті
Сарета Ашраф (Sareta Ashraph), Garden Court Chambers
Даня Чайкель (Danya Chaikel), Спеціалізована прокуратура Косово
Алан Кларк (Alan Clark), Міжнародний кримінальний суд
Федеріка Д'Алессандра (Federica D'Alessandra), Оксфордський університет
Ніко Декенс (Nico Dekens), Bellingcat
Кріс Енгельс (Chris Engels), Комісія з питань міжнародного правосуддя та підзвітності
Ліндсі Фріман (Lindsay Freeman), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Емма Ірвінг (Emma Irving), Лейденський університет
Мішель Джарвіс (Michelle Jarvis), Міжнародний, неупереджений та незалежний механізм допомоги у розслідуванні та судовому переслідуванні осіб, відповідальних за найбільш тяжкі злочини згідно з міжнародним правом, вчинені у Сирійській Арабській Республіці з березня 2011 року
Едвард Джеремі (Edward Jeremy), Міжнародний кримінальний суд
Ешлі Джордана (Ashley Jordana), Global Rights Compliance
Санг-Мін Кім (Sang-Min Kim), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Алекса Кеніг (Alexa Koenig), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Ніколас Кумджян (Nicholas Koumjian), Незалежний слідчий механізм щодо М'янми
Бастіан Ван Дер Лаакен (Bastiaan Van Der Laaken), Міжнародний, неупереджений та незалежний механізм допомоги у розслідуванні та судовому переслідуванні осіб, відповідальних за найбільш тяжкі злочини згідно з міжнародним правом, вчинені у Сирійській Арабській Республіці з березня 2011 року
Дербла Міноуг (Dearbhla Minogue), Global Legal Action Network
Нік Ортіс (Nick Ortiz), Лейденський університет
Матевз Пездірц (Matevz Pezdirc), Мережа геноциду Агентства Європейського Союзу з питань співробітництва у галузі кримінального правосуддя
Саня Попович (Sanja Popovic), Спеціалізована прокуратура Косово
Стівен Поулз (Steven Powles), Doughty Street Chambers; Комітет Міжнародної асоціації адвокатів з питань військових злочинів
Стівен Рапп (Stephen Rapp), Центр запобігання геноциду Саймона-Скйодта, Меморіальний музей Голокосту США
Крістіна Рібейро (Cristina Ribeiro), Міжнародний кримінальний суд

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Марк Робсон (Mark Robson), Комісія з питань міжнародного правосуддя та підзвітності
Бред Семюелс (Brad Samuels), SITU Research
Даліла Сеоан (Dalila Seoane), Civitas Maxima
Карстен Стан (Carsten Stahn), Лейденський університет
Мелінда Тейлор (Melinda Taylor), Міжнародний кримінальний суд
Алан Тігер (Alan Tieger), Спеціалізована прокуратура Косово
Ракель Васкес Льоренте (Raquel Vazquez Llorente), очевидець злочинів

Додаткові експерти-рецензенти

Еліз Бейкер (Elise Baker), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Шон Брукс (Sean Brooks), Центр довгострокової кібербезпеки, Каліфорнійський університет, Берклі
Стефані Крофт (Stephanie Croft), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Сем Дабберлі (Sam Dubberley), Amnesty International
Томас Едвін (Thomas Edwin), Центр перспективних досліджень оборони
Крістофер «Кіп» Хейл (Christopher «Kip» Hale), Комісія з питань міжнародного правосуддя та підзвітності
Габріела Івенс (Gabriela Ivens), Страж прав людини
Фелім Макмехон (Felim McMahon), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Дараг Мюррей (Daragh Murray), Університет Ессексу
Івонн НГ (Yvonne Ng), СВІДОК
Зара Рахман (Zara Rahman), The Engine Room
Марк Робсон (Mark Robson), Комісія з питань міжнародного правосуддя та підзвітності
Джастін Зайц (Justin Seitz), Hunchly
Андреа Тревіннард (Andrea Trewinnard), Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа
Стів Труш (Steve Trush), Центр довгострокової кібербезпеки, Каліфорнійський університет, Берклі
Ракель Васкес Льоренте (Raquel Vazquez Llorente), очевидець злочинів

Особлива подяка

Особлива подяка висловлюється членам Робочої групи з розслідувань в Інтернеті, Прокуратура, Міжнародний кримінальний суд.

Також висловлюється подяка багатьом колегам з УВКПЛ, зусилля яких призвели до реалізації цієї спільної публікації.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

* Відповідно до політики УВКПЛ, внески до його публікацій не відносяться до тих, хто працює в Управлінні.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Абревіатури та скорочення

HTML	Мова гіпертекстової розмітки
ICRC	Міжнародний комітет Червоного Хреста
ІКТ	Інформаційно-комунікаційні технології
IP	Інтернет-протокол
ISP	Інтернет-провайдер
НУО	Неурядова організація
УВКПЛ	Управління Верховного комісара ООН з прав людини
PDF	Портативний формат документів
URI	Єдиний ідентифікатор ресурсу
URL	Єдиний локатор ресурсів
VPN	Віртуальна приватна мережа

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

I

ВСТУП

РЕЗЮМЕ ГЛАВИ

- Мета
- Цільова аудиторія
- Визначення

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних описує професійні стандарти, які слід застосовувати при виявленні, зборі, збереженні, аналізі та представленні цифрової інформації у відкритому доступі та її використанні у міжнародних кримінальних розслідуваннях та розслідуваннях у сфері прав людини. Інформація у відкритому доступі – це інформація, яку будь-який представник громадськості може спостерігати, купувати чи запитувати, не вимагаючи особливого правового статусу чи несанкціонованого доступу. Цифрова інформація у відкритому доступі – це загальнодоступна інформація в цифровому форматі, яка зазвичай отримується з Інтернету. Цифрова інформація у відкритому доступі містить дані, створені користувачами та машиною, і може включати, наприклад: вміст, розміщений у соціальних мережах; документи, зображення, відео та аудіозаписи на веб-сайтах та платформах для обміну інформацією; супутникові знімки; та опубліковані урядом дані.[1] Розслідування з використанням відкритих цифрових даних – це розслідування, засновані на цифровій інформації у відкритому доступі. Для зручності читання Протокол відтепер буде називати цифрову інформацію у відкритому доступі та розслідування з використанням відкритих цифрових даних як «інформація у відкритому доступі» та «розслідування з використанням даних у відкритому доступі», відповідно.

2. Хоча використання інформації у відкритому доступі у розслідуваннях не є чимось новим, обсяг і різноманітність відкритих джерел розширилися внаслідок все більшого використання Інтернету та інших цифрових ресурсів для обміну інформацією, включаючи поширення соціальних медіа. Протокол розглядає як складності, що виникають при роботі з цифровою інформацією, так і унікальні проблеми, які виникають під час оцінки джерел та перевірки інформації, що міститься на відкритих онлайн-форумах.

3. Хоча все більша кількість міжнародних слідчих з кримінальних справ і правозахисників зараз використовують Інтернет для полегшення своєї роботи, наразі не існує універсальних посилань, вказівок чи стандартів для ведення розслідувань з використанням даних у відкритому доступі. Протокол намагається заповнити цю прогалину, встановивши принципи та практику, які допоможуть слідчим проводити свою роботу відповідно до професійних стандартів та сприятимуть, де це доречно, збереженню інформації у відкритому доступі для потенційного використання механізмами підзвітності.

4. У Протоколі особлива увага приділяється розслідуванням з використанням даних у відкритому доступі, що проводяться з метою забезпечення міжнародного правосуддя та підзвітності, які загалом включають: документацію з прав людини, збереження, збір доказів та встановлення фактів; розслідування слідчими комісіями та місіями з встановлення

---

[1] Цей список не є вичерпним.
Див., наприклад, звіт Верховного комісара Організації Об'єднаних Націй з прав людини про ситуацію з правами людини у Боліварській Республіці Венесуела (A/HRC/41/18), поданий відповідно до резолюції 39/1 Ради з прав людини. Див. також резолюцію Ради 41/2, у якій Рада просила Верховного комісара підготувати звіт про ситуацію з правами людини на Філіппінах.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

фактів;[2] інші види міжнародних розслідувань;[3] процеси встановлення істини та примирення; цивільний судовий процес; та кримінальні процеси, включаючи міжнародні кримінальні провадження. Оскільки розслідування з використанням даних у відкритому доступі можуть сприяти різним типам зусиль із забезпечення підзвітності,[4] вимоги до методології та документації, викладені у Протоколі, можуть бути більш суворими, ніж ті, які традиційно використовуються в інших сферах, таких як журналістика та захист прав людини. Якою б не була мета їхнього розслідування, дотримуючись методологічних принципів, викладених у Протоколі, які розроблені на основі загальноприйнятих правових стандартів, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, забезпечать високу якість своєї роботи та максимально використовуватимуть зібрану інформацію в судах, трибуналах та інших процесах для забезпечення підзвітності.

5. Крім того, Протокол наголошує на стандартах розслідування порушень міжнародного права, включаючи порушення прав людини та порушення міжнародного кримінального права, включаючи військові злочини, злочини проти людяності та геноцид. Крім того, вказівки, передбачені Протоколом, можуть бути застосовані до інших видів розслідувань, у тому числі для національних чи муніципальних судів.

6. Зрештою, Протокол покликаний допомогти слідчим, що ведуть розслідування з використанням даних у відкритому доступі, виконувати свою роботу відповідно до професійної методології, яка в цілому відповідає юридичним вимогам та етичним нормам. Він також має на меті допомогти різним кінцевим користувачам процесу розслідування, включаючи адвокатів, суддів та інших осіб, які приймають рішення, краще зрозуміти та оцінити методи розслідування з використанням даних у відкритому доступі. Протокол однаково призначений як ресурс для досвідчених практиків та інструмент навчання та

---

[2] Слідчі комісії та місії з встановлення фактів – це органи, які можуть бути створені урядами чи міжнародними організаціями для вивчення різних питань. Слідчі комісії або місії з встановлення фактів повідомляють про факти, роблять юридичні висновки та надають рекомендації. Хоча висновки міжнародних слідчих комісій чи місій з встановлення фактів не є юридично обов'язковими, вони можуть мати великий вплив. Однак у деяких юрисдикціях висновки національних слідчих комісій можуть бути обов'язковими. Для отримання додаткової інформації про міжнародні слідчі комісії та місії з встановлення фактів див. документ Ради з прав людини, «Міжнародні слідчі комісії, комісії з прав людини, місії з встановлення фактів та інші розслідування». Доступно на сторінці www.ohchr.org/EN/HRBodies/HRC/Pages/COIs.aspx.

[3] Див., наприклад, звіт Верховного комісара Організації Об'єднаних Націй з прав людини про ситуацію з правами людини у Боліварській Республіці Венесуела (A/HRC/41/18), поданий відповідно до резолюції 39/1 Ради з прав людини. Див. також резолюцію Ради 41/2, у якій Рада просила Верховного комісара підготувати звіт про ситуацію з правами людини на Філіппінах.

[4] Наприклад, інформація у відкритому доступі була використана незалежною міжнародною місією з встановлення фактів у М'янмі поряд з джерелами з перших вуст та іншою інформацією у процесі перевірки та в її висновках. Остаточний звіт місії з встановлення фактів (A/HRC/42/50) став одним із факторів, що призвели до створення Радою з прав людини Незалежного слідчого механізму щодо М'янми, якому було надано повноваження проводити судові розслідування. Місія з встановлення фактів також отримала мандат передати свою інформацію, включаючи зміст розслідувань з використанням даних у відкритому доступі, Незалежному слідчому механізму щодо М'янми. Звіти місії з встановлення фактів також використовувалися у справі, порушеній Гамбією у Міжнародному суді ЄС проти М'янми за порушення останньою Конвенції про запобігання злочину геноциду та покарання за нього. Це демонструє, як інформація, зібрана з однією метою, може врешті-решт сприяти іншому процесу юридичної підзвітності.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

підготовки для тих, хто хоче навчитися проводити розслідування з використанням даних у відкритому доступі щодо передбачуваних порушень міжнародного права.[5]

A. Мета

7. Хоча слідчі довгий час спиралися на інформацію у відкритому доступі, її систематична експлуатація прискорилася на початку-середині двадцятого століття, зосередившись на вилученні інформації з іноземних засобів радіомовлення та друкованих газет.[6] З впровадженням Всесвітньої павутини у 1990-х роках, а потім популяризацією соціальних медіа та смартфонів у 2000-х роках, кількість та якість інформації у відкритому доступі різко змінилися. Сьогодні будь-яка особа зі смартфоном та доступом до Інтернету може створювати та поширювати цифровий контент у всьому світі, хоча і різної якості, достовірності та прозорості. Зростаючий обсяг даних та швидкість передачі та обміну такими даними створили нові можливості для слідчих, що ведуть розслідування з використанням даних у відкритому доступі, збирати та аналізувати інформацію про міжнародні злочини та порушення прав людини. У той же час творці контенту тепер можуть поширювати дезінформацію та відносно легко маніпулювати цифровими даними. Протокол є спробою відреагувати на це нове середовище та складність врегулювання таких можливостей та викликів.

8. Інформація у відкритому доступі корисна для всіх видів розслідувань, але вона відіграє особливо важливу роль у міжнародних кримінальних розслідуваннях та розслідуваннях у сфері прав людини. Це вірно з ряду причин. По-перше, міжнародні розслідування, у тому числі ті, які проводяться слідчими комісіями та місіями Організації Об'єднаних Націй з встановлення фактів, або санкціоновані Міжнародним кримінальним судом, залежать від правових та політичних процесів, які дозволяють проводити розслідування.[7] Таким чином, вони часто проводяться задовго після подій. По-друге, часто міжнародні розслідування можуть не мати доступу до фізичного місця, де відбувалися розслідувані інциденти, наприклад, через відмову держави співпрацювати або надавати доступ. По-третє, навіть якщо їм надається доступ до регіону чи території, слідчі можуть мати обмежений фізичний доступ до відповідного місця або можуть зіткнутися з перешкодами для проведення розслідування на місці або особистого опитування через занепокоєння щодо захисту. Нарешті, більшість слідчих не матиме повних правоохоронних повноважень щодо територій, на яких відбувалися передбачувані злочини чи порушення, і, отже, можуть бути не в змозі зібрати необхідну інформацію. Навіть у випадках, коли має місце державна співпраця, збір транскордонних доказів може бути важким процесом, уповільненим громіздкими бюрократичними процедурами. Усі ці фактори демонструють,

---

[5] Протокол також містить деякі шаблони для розслідувань з використанням відкритих даних, а також глосарій (див. главу VIII нижче).

[6] Нікіта Механдру (Nikita Mehandru) та Алекса Кеніг (Alexa Koenig), «ІКТ, соціальні медіа та майбутнє прав людини», Duke Law & Technology Review, том 17, № 1, стор. 129.

[7] Слідчі комісії та місії з встановлення фактів, уповноважені Організацією Об'єднаних Націй, були створені, зокрема, Радою Безпеки, Генеральною Асамблеєю, Радою з прав людини та Генеральним секретарем. Щодо Міжнародного кримінального суду, Прокуратура може розпочати розслідування за поданням держав-учасниць або Ради Безпеки, або з власної ініціативи та з дозволу суддів.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

чому методи розслідування з використанням даних у відкритому доступі, які можна проводити дистанційно та одночасно з подіями, є водночас потужними та необхідними.

9. Протокол спрямований на різноманітну групу слідчих, які працюють у різних контекстах з різними мандатами, слідчими повноваженнями та ресурсами розслідування. Тому потрібен гнучкий підхід, який не передбачає, що слідчі мають виконувати свою роботу однаково, а скоріше адаптує методології відповідно до кожного унікального робочого середовища. Більше того, оскільки технології, інструменти та методи, які допомагають проводити розслідування з використанням даних у відкритому доступі, постійно розвиваються, Протокол зосереджується не на конкретних інструментах, платформах, веб-сайтах, програмному забезпеченні чи джерелах, які можуть змінитися, а на основних принципах та процедурах, які повинні використовуватися при веденні розслідувань з використанням даних у відкритому доступі.

10. Протокол покликаний стандартизувати процедури та надати методологічні вказівки для різних розслідувань, установ та юрисдикцій, щоб допомогти слідчим, які використовують дані у відкритому доступі, усвідомити важливість:

(a) Відстеження походження онлайн-контенту та його віднесення до першоджерела, за можливості;

(b) Оцінки достовірності та надійності онлайн-джерел;

(c) Перевірки онлайн-контенту та оцінки його достовірності та надійності;

(d) Дотримання законодавчих вимог та етичних норм;

(e) Мінімізації будь-якого ризику заподіяння шкоди собі, своїм організаціям та третім сторонам;

(f) Посилення захисту прав людини джерел, включаючи право на конфіденційність.

B. Цільова аудиторія

11. Цільова аудиторія Протоколу – це фізичні особи та організації, які виявляють, збирають, зберігають та/або аналізують інформацію у відкритому доступі для розслідування міжнародних злочинів або порушень прав людини з метою забезпечення справедливості та підзвітності. Сюди входять слідчі, адвокати, архівісти та аналітики, які працюють у міжнародних, регіональних та гібридних кримінальних трибуналах; національні підрозділи з питань військових злочинів; слідчі комісії; місії з виявлення фактів; незалежні слідчі механізми; міжнародні організації; механізми правосуддя перехідного періоду; та неурядові організації (НУО). Інші, хто міг би отримати користь, – це ті, хто працює над різноманітними міжнародними та регіональними механізмами, які проводять судові та квазісудові розслідування з використанням даних у відкритому доступі

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

щодо порушень міжнародного права.[8] Протокол також може бути повчальним для тих, хто приймає перші відповідні заходи у цифровому просторі, таких як громадські організації та незалежні дослідники, які часто першими публікують висновки на основі інформації у відкритому доступі і чия робота часто відіграє ключову роль у створенні інших офіційних розслідувань з використанням цифрових даних. Цільова аудиторія також включає окремих осіб та організації, які підтримують жертв у поданні цивільних позовів проти окремих злочинців або держав. Протокол також може загалом допомагати тим, хто робить фактичні чи юридичні висновки на основі розслідувань з використанням даних у відкритому доступі, дозволяючи їм краще оцінити зміст будь-яких розслідувань з використанням даних у відкритому доступі, на які вони спираються або які вони оцінюють.

12. Інші потенційні зацікавлені сторони можуть включати постачальників веб-послуг, таких як платформи соціальних медіа, які зберігають великі обсяги даних і можуть відігравати ключову роль у збереженні даних, та розробників, які надають програмне забезпечення для посилення методів та процесів розслідування з використанням даних у відкритому доступі.

C. Визначення

13. Для надання практичних стандартів та вказівок для розслідувань з використанням даних у відкритому доступі слідчі повинні мати спільне розуміння конкретних термінів. У цьому розділі уточнюється ключова термінологія, яка використовується у всьому Протоколі, включаючи відмінності між поєднаними термінами.[9]

1. Відкрита інформація у порівнянні з закритою інформацією

14. Інформація у відкритому доступі включає загальнодоступну інформацію, яку будь-який представник громадськості може спостерігати, купувати чи запитувати, не вимагаючи особливого правового статусу чи несанкціонованого доступу. Інформація із закритих джерел – це інформація з обмеженим доступом або доступом, що охороняється законом,[10] але яка може бути отримана на законних засадах через приватні канали, такі як судові процеси, або запропонована добровільно. Незважаючи на просте визначення, визначення того, що представляє собою інформація у відкритому доступі, складніше, ніж здається спочатку в контексті онлайн-контенту. В Інтернеті зростає обсяг даних, які оприлюднюються без згоди власників, наприклад, злам, витік інформації, виявлення інформації через вразливості безпеки або публікація інформації третьою стороною без відповідних дозволів. Хоча ця інформація є загальнодоступною і, отже, технічно вважається відкритою, все ж можуть існувати юридичні та етичні обмеження щодо певних видів кінцевого використання. Крім того, цифрова інформація може бути доступною для тих, хто має спеціалізовані технічні навички та навчання, які можуть отримати доступ до

---

[8] Див., наприклад, повідомлення та інспекційні звіти про спеціальні процедури Ради з прав людини. Доступно на сторінці www.ohchr.org/en/ hrbodies/sp/pages/welcomepage.aspx. Дивіться також роботу Комітетів з санкцій, створених Радою Безпеки. Доступно на сторінці www.un.org/securitycouncil/content/repertoire/sanctions-and-other-committees.

[9] Для більш детальної компіляції відповідних термінів та визначень див. главу VIII.

[10] Наприклад, конфіденційна інформація та засекречена інформація.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

мереж та даних, недоступних для звичайної людини або доступ до яких вона навряд чи матиме.[11] Одним із прикладів є інформація, яку можна отримати лише в тіньовому Інтернеті, а саме в тій частині Інтернету, яка доступна лише за допомогою певного програмного забезпечення, наприклад, браузера Tor.[12] Хоча тіньовий Інтернет пропонує анонімність, що зробило його привабливим місцем для незаконної діяльності, використання браузера Tor та пошук у тіньовому Інтернеті є законним у більшості країн. Протокол включає цю інформацію в сферу «відкритого доступу», доки не відбувається несанкціонованого доступу до інформації. Найяскравішою відмінністю є те, що інформація у відкритому доступі не передбачає взаємодії або вимагання інформації від окремих користувачів Інтернету.[13] Отримання інформації від інших користувачів Інтернету шляхом спілкування з цими користувачами вважається закритим джерелом.

15. Цифрова інформація у відкритому доступі[14] – це інформація у відкритому доступі в Інтернеті, до якої можна отримати доступ, наприклад, на загальнодоступних веб-сайтах, в Інтернет-базах даних або на платформах соціальних медіа. Нижче наведено різні способи отримання інформації у відкритому доступі.

2. Отримання цифрової інформації у відкритому доступі

(a) Спостереження

16. Контент на багатьох платформах можна отримати, просто перейшовши на відповідний сайт з використанням будь-якої кількості безкоштовних веб-браузерів. Інші онлайн-платформи вимагають від користувачів входу або реєстрації для доступу та перегляду контенту. Такий контент вважається відкритим джерелом доти, доки ці процеси відкриті для всіх користувачів у юрисдикціях, в яких доступ є законним, і при доступі чи перегляді до нього не порушуються заходи конфіденційності та безпеки. Однак деякий контент, що відповідає цьому визначенню, не може розглядатися як відкрите джерело. Приклади включають конфіденційну, засекречену або іншим чином захищену законом інформацію. У таких випадках, хоча інформацію може спостерігати будь-який представник громадськості, її використання як доказу в судових розглядах може бути обмежено. Також можуть виникнути етичні або методологічні проблеми щодо довіри до такого матеріалу, наприклад, неможливість віднесення або перевірки цього контенту.

(b) Купівля

---

[11] Деякі дії можуть порушувати умови користувацької угоди щодо веб-сайту, але самі по собі не є незаконними. Наприклад, порушення умов користувацької угоди щодо веб-сайту з метою видалення даних є несанкціонованою поведінкою і може призвести до заборони використання веб-сайту.

[12] Тіньовий Інтернет відноситься до тієї частини Інтернету, доступ до якої можливий лише за допомогою спеціалізованого програмного забезпечення. Браузер Tor є одним із прикладів такого програмного забезпечення.

[13] Хоча придбання інформації з приватної бази даних або подання запиту на інформацію до державного органу вимагають певного ступеня обміну в Інтернеті, цей процес часто є автоматизованим і відрізняється від типу взаємодії з іншими окремими користувачами Інтернету, описаного тут.

[14] Інформація у відкритому доступі також може іменуватися у Протоколі як онлайн-контент, онлайн-матеріл або онлайн-дані.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

17. Кілька джерел даних для розслідувань з використанням даних у відкритому доступі знаходяться на платформах, які вимагають оплати, або відповідають поєднаній безкоштовній та преміальній моделі, в якій додаткові функціональні можливості та доступ до даних пов'язані з фінансовими витратами. Зростає кількість підприємств, які збирають загальнодоступні дані та пропонують як безкоштовні, так і платні послуги для доступу до цих даних. Багато інформації, яку слідчі, що ведуть розслідування з використанням даних у відкритому доступі, знайдуть корисною, існує в базах даних та на платформах, доступних лише на платній основі. Для цілей Протоколу інформація у відкритому доступі включає платні послуги, доступні для всіх представників громадськості, але не послуги, доступ до яких мають лише певні групи, такі як співробітники правоохоронних органів або ліцензовані приватні слідчі.

(c) Запит

18. У цьому контексті термін «запит» відноситься до запитів, які можуть бути подані будь-якою особою щодо публічної інформації до державних органів відповідно до законів про свободу інформації або доступу до інформації. Він не стосується запитів до окремих осіб, компаній чи організацій про добровільну передачу своєї інформації, а обмежується запитами до державних установ, які мають юридичні зобов'язання відповідати однаково всім особам. Розслідування з використанням даних у відкритому доступі може призвести до інших слідчих дій в Інтернеті, таких як взаємодія із зовнішніми джерелами за допомогою сервісів обміну повідомленнями, чатів, форумів або електронної пошти. Така взаємодія виходить за межі розслідування з використанням даних у відкритому доступі, про яке йдеться у Протоколі.

3. Розвідка за відкритими джерелами

19. Розвідка за відкритими джерелами відноситься до підкатегорії інформації у відкритому доступі, яка збирається та використовується для конкретних цілей допомоги у розробці політики та прийнятті рішень, найчастіше у військовому чи політичному контексті. Хоча інформація у відкритому доступі включає всю загальнодоступну інформацію, яку будь-хто може законно отримати, розвідка за відкритими джерелами є підмножиною тієї інформації, «яка збирається, використовується та розповсюджується своєчасно серед відповідної аудиторії з метою задоволення конкретних вимог до розвідки».[15] У контексті міжнародних кримінальних справ та справ з прав людини, розвідка за відкритими джерелами використовується як довідкова інформація для прийняття рішень, наприклад, для інформування про заходи, пов'язані з безпекою, такі як захист свідків та членів групи, які надходять до військ, чи відстеження осіб, які представляють інтерес, а не функції збору інформації, пов'язані з процесами розслідування, такими як встановлення елементів різних злочинів.

4. Розслідування з використанням даних у відкритому доступі

---

[15] National Open Source Enterprise, Директива про розвідувальну спільноту № 301, 11 липня 2006 року, стор. 8 (виноску пропущено).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

20. Розслідування з використанням даних у відкритому доступі стосується використання інформації у відкритому доступі для функцій збору інформації та доказів.

5. Докази з відкритих джерел

21. Термін «докази» слід відрізняти від «інформації».[16] Докази, як правило, визначаються у всіх юрисдикціях як доказ факту (фактів), який використовується під час розслідування або подається на судовому слуханні, наприклад, у судовому засіданні. Докази з відкритих джерел – це інформація у відкритому доступі із доказовою цінністю, яка може бути допущена для встановлення фактів у судовому процесі. Важливо правильно використовувати та не зловживати терміном «докази», посилаючись на «інформацію» взагалі.

6. Інформація у відкритому доступі у порівнянні з відкритим програмним забезпеченням

22. Термін «відкритий» часто використовується для опису програмного забезпечення або коду, які вільно доступні для використання та повторної публікації, без обмежень на підставі авторського права, патентів чи інших юридичних засобів контролю. Відкрите програмне забезпечення побудоване з вихідного коду, який кожен, хто має доступ, може перевірити, змінити та покращити.[17] Зазвичай його не видно користувачам, але він може бути скоригований та адаптований програмістом. Відкрите програмне забезпечення відрізняється від інформації у відкритому доступі, хоча програмне забезпечення та інструменти у відкритому доступі часто використовуються слідчими, що використовують інформацію у відкритому доступі, для пошуку, збирання, збереження та аналізу інформації у відкритому доступі.

7. Надійність у порівнянні з достовірністю

23. Що стосується свідчень у міжнародних кримінальних процесах, судді оцінюють «надійність свідка» та «достовірність його показань».[18] У розслідуваннях слідчих комісій, місій з встановлення фактів Організації Об'єднаних Націй та подібних розслідуваннях керівництво передбачає, що «інтерв'юер повинен оцінити надійність опитуваного та достовірність».[19] У керівництві уточнюється, що «оцінка враховуватиме релевантність інформації для предмета розслідування. Вона також розгляне достовірність джерела та надійність чи правдивість інформації».[20] Протокол використовує такі терміни наступним чином:

---

[16] Федеріка Д'Алессандра (Federica D'Alessandra) та інші, ред., Довідник з документації громадянського суспільства про серйозні порушення прав людини: Принципи і передова практика (Гаага, Група міжнародного публічного права та політики, 2016 рік), стор. 17.

[17] Див. Opensource.com, «Що таке відкрите джерело?».

[18] Міжнародний кримінальний суд, Прокурор проти Боско Нтаганди (Bosco Ntaganda), справа № ICC-01/04-02/06, Рішення від 08 липня 2019 року, пункт 53.

[19] УВКПЛ, Слідчі комісії та місії з встановлення фактів з міжнародних прав людини та гуманітарного права: Керівництво та практика (Нью-Йорк та Женева, 2015 рік), стор. 52. Доступно на сторінці www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf.

[20] У тому самому місці, стор. 59.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(a) «Надійність» означає правдоподібність або правдивість;

(b) «Достовірність» означає здатність працювати послідовно, надійно або відповідно до очікувань;

(c) «Справжність» або «дійсність» означає точність, правдивість або відповідність фактам.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

II

ПРИНЦИПИ

РЕЗЮМЕ ГЛАВИ

- Для дотримання професійних принципів, пов'язаних із розслідуваннями з використанням цифрових даних у відкритому доступі, слідчі повинні переконатися, що вони є відповідальними, компетентними та об'єктивними, а їхня робота виконується відповідно до законодавства та з належною повагою до міркувань безпеки.

- Слідчі також повинні враховувати методи, які вони використовують на всіх етапах життєвого циклу свого розслідування. Відповідні методологічні принципи включають, щонайменше, точність, мінімізацію даних, збереження даних та безпеку за замовчуванням.

- Нарешті, всі слідчі повинні керуватися етичними міркуваннями. Вони включають, щонайменше, захист гідності всіх осіб, які беруть участь у розслідуванні або причетні до нього, а також забезпечення тактичності, інклюзивності, незалежності та прозорості.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

24. Хоча технології, інструменти та методи, що використовуються у розслідуваннях з використанням даних у відкритому доступі, змінюватимуться, певні всеосяжні методологічні та етичні принципи мають зберігатися. Виявлення таких принципів є важливим кроком на шляху професіоналізації галузі розслідувань з використанням даних у відкритому доступі. Наступні принципи є основоположними для забезпечення якості розслідувань з використанням даних у відкритому доступі, що, у свою чергу, зміцнить їх достовірність, надійність та потенційну корисність для забезпечення підзвітності та мінімізації потенційної шкоди для різних зацікавлених сторін.

A. Професійні принципи

1. Підзвітність

25. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні нести відповідальність за свої дії, що часто можна забезпечити чіткою документацією, веденням обліку та наглядом. Прозорість у методах та процедурах розслідування є важливим елементом забезпечення підзвітності. Таким чином, наскільки це можливо і розумно, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вести записи про свою діяльність. Етапи розслідування з використанням даних у відкритому доступі – від виявлення відповідного матеріалу до збору, аналізу та звітування – слід послідовно та чітко документувати. Будь-які особи, які займаються збором або обробкою інформації в Інтернеті, повинні знати про можливість допиту щодо їх методології, включаючи можливість бути викликаними для надання свідчень у суді. Документація розслідувань з використанням даних у відкритому доступі може здійснюватися вручну або за допомогою автоматизованих процесів, наданих різним програмним забезпеченням. Поки документація послідовна і достатньо ретельна, можна використовувати як ручні, так і автоматичні методи. Автоматизовані процеси та програмне забезпечення мають бути зрозумілими користувачам та піддаватися поясненню в суді з боку користувачів або розробників. Крім того, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні фіксувати будь-які інструменти або програмне забезпечення, що використовуються під час їх роботи.

2. Компетентність

26. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні мати належну підготовку та технічні навички для виконання діяльності, якою вони займаються. Вони повинні вести діяльність в Інтернеті професійно та етично, уникаючи привласнення чужої роботи; висловлюючи подяку всім, хто бере участь у розслідуванні (коли це безпечно робити та за бажанням учасників); і точно повідомляючи дані, включаючи визнання будь-яких прогалин, які можуть існувати в онлайн-контенті. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, та процеси розслідування також повинні залишатися гнучкими, адаптуватися до нових розробок та застосовувати нові технології та методи у відповідних випадках. Крім того, організації та слідчі групи повинні мати механізми для забезпечення послідовного впровадження та дотримання процедур.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

3. Об'єктивність

27. Об'єктивність – це основний принцип, який застосовується до всіх розслідувань, будь то онлайн чи офлайн. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розуміти потенціал особистих, культурних та структурних упереджень, що впливають на їх роботу, і необхідність вживати контрзаходів для забезпечення об'єктивності. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні переконатися, що вони об'єктивно підходять до своїх розслідувань, розробляючи та розгортаючи численні робочі гіпотези, а не віддаючи перевагу якійсь конкретній теорії для пояснення своїх аргументів. Для розслідувань з використанням даних у відкритому доступі, що проводяться в Інтернеті, об'єктивність особливо важлива через спосіб структуризації та представлення користувачам інформації в Інтернеті. Використовуваний браузер, пошукова система, пошукові терміни та синтаксис можуть призвести до дуже різних результатів, навіть якщо основний запит однаковий. Властиві упередження в архітектурі та алгоритмах Інтернету, що використовуються пошуковими системами та веб-сайтами, можуть загрожувати об'єктивності результатів

пошуку.[21] На результати пошуку також може впливати низка технічних факторів, включаючи використовуваний пристрій та його розташування, а також попередню історію пошуку користувача та активність в Інтернеті. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні врівноважити такі упередження, застосовуючи методології, щоб гарантувати максимальну різноманітність результатів пошуку, наприклад, шляхом виконання кількох пошукових запитів та використання різноманітних пошукових систем та браузерів.[22] Слідчі повинні знати, що на результати пошуку також можуть впливати інші чинники, в тому числі внаслідок розбіжностей у цифровому середовищі, у результаті чого інформація в Інтернеті може бути нерівномірно доступною для певних груп чи верств суспільства.[23] Нарешті, слідчі завжди повинні

---

[21] Див. Сафія Ноубл (Safiya Noble), Алгоритми пригнічення: Як пошукові системи підсилюють расизм (Нью-Йорк, New York University Press, 2018 рік); Вірджинія Ойбанкс (Virginia Eubanks), Автоматизація нерівності: Як профіль високотехнологічних інструментів описує поліцію та карає бідних (Нью-Йорк, Пікадор, 2019 рік).

[22] Див., наприклад, Пол Майерс (Paul Myers), «Як проводити відкриття методами у відкритому доступі», у Digital Witness, Використання інформації у відкритому доступі для розслідування, документації та підзвітності в області прав людини, Сем Дабберлі (Sam Dubberley), Алекса Кеніг (Alexa Koenig) та Дараг Мюррей (Daragh Murray), ред. (Оксфорд, Oxford University Press, 2020 рік) (обговорення того, як вибір пошукових систем та пошукових термінів може сприяти упередженості результатів розслідувань з використанням даних у відкритому доступі).

[23] Див., наприклад, Алекса Кеніг (Alexa Koenig) та Улік Еган (Ulic Egan), «Приховування на простому сайті: використання інформації у відкритому доступі в Інтернеті для розслідування сексуального насильства та злочинів на гендерній основі», у Technologies of Human Rights Representation, Джеймс Доус (James Dawes) та Олександра С. Мур (Alexandra S. Moore), ред. (скоро) (обговорення того, як відносна відсутність доступу у жінок до смартфонів та використання кодованої мови в Інтернеті жертвами сексуального та гендерного насильства може зменшити кількість та доступність інформації у відкритому доступі, що стосується таких злочинів, а також як переважна кількість чоловіків як на посадах, пов'язаних з технологіями, так і в ролі слідчих у справах військових злочинів, може негативно вплинути на ймовірність того, що автоматизовані та/або ручні процеси виявлення нададуть інформацію у відкритому доступі, що стосується гендерних злочинів). Для подальшого обговорення упередженості див. главу II.C нижче про етичні принципи та главу V.B нижче про оцінку цифрового середовища.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

прагнути усвідомлювати та виправляти власні упередження, які можуть бути свідомими або підсвідомими.[24]

4. Законність

28. Розслідування з використанням даних у відкритому доступі повинні відповідати чинному законодавству, а це означає, що слідчі повинні мати базове розуміння законів, які застосовуються до їх роботи. Зокрема, слідчі повинні знати закони про захист даних та право на недоторканність приватного життя, яке охороняється міжнародним законодавством з прав людини.[25] Незважаючи на те, що інформація може бути загальнодоступною, це не означає, що її збирання та використання не впливають на конфіденційність. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні враховувати наслідки своїх дій для конфіденційності, включаючи розумне очікування особи на конфіденційність у різних цифрових просторах. Слідчі також повинні знати про мозаїчний ефект, завдяки якому публічні дані, навіть коли вони анонімізовані, можуть стати вразливими до повторної ідентифікації, якщо буде випущено чи об'єднано достатньо наборів даних, які містять подібну чи доповнювальну інформацію.[26] Крім того,

---

[24] Див., наприклад, Регулятор судової медицини, Ефекти когнітивної упередженості, що мають значення для судово-наукових розслідувань, FSR-G-217 (Бірмінгем, Сполучене Королівство, 2015 рік) (обговорення різних категорій когнітивних упереджень, які можуть негативно вплинути на якість розслідування, включаючи упередження очікувань, упередження підтвердження, прив'язка, зміст контексту, а також вплив ролі та реконструкції); Уейн А. Уоллес (Wayne A. Wallace), Вплив упередження підтвердження на прийняття рішень щодо кримінальних розслідувань (Міннеаполіс, Walden University ScholarWorks, 2015 рік) (пояснюючи упередженість підтвердження як процес, за допомогою якого слідчі шукають або довіряють інформації, яка підтверджує їхню улюблену теорію справи, «ігноруючи при цьому або не враховуючи докази протилежного»); Майкл Піттаро (Michael Pittaro), «Неявна упередженість у системі кримінального правосуддя», Psychology Today, 21 листопада 2018 року (обговорення упереджень, які можуть впливати на кримінальне розслідування загалом, та запропонування відомих методів упередженості до певних оцінок); Джон С. Берд (Jon S. Byrd), «Упередження підтвердження, етика та помилки в криміналістиці», Forensic Pathways, 21 березня 2020 року (обговорення різних когнітивних та етичних помилок, які можуть спотворити криміналістичний аналіз, а також методи уникнення цих помилок). Див. також Івонн Макдермотт (Yvonne McDermott), Дараг Мюррей (Daragh Murray) та Алекса Кеніг (Alexa Koenig), «Симпозіум з питань цифрової підзвітності: чиї історії та ким розповідаються? Репрезентативність у розслідуваннях щодо прав людини з використанням даних у відкритому доступі», Opinio Juris, 19 грудня 2019 року (обговорення того, як методи розслідування з використанням даних у відкритому доступі можуть негативно вплинути на «види порушень, жертв та свідків, які мають можливість бути почутими, і як будуються розповіді про масові порушення прав людини»); і проект під керівництвом Івонн Макдермотт (Yvonne McDermott) під назвою «Майбутнє розслідувань у сфері прав людини: використання розвідки за відкритими джерелами для перетворення документації та виявлення порушень прав людини».

[25] Стаття 12 Загальної декларації прав людини передбачає, що ніхто не може зазнавати довільного втручання у його особисте життя, сім'ю, житло чи листування, а також нападів на його честь та репутацію. Кожен має право на захист за законом від такого втручання або нападів. Міжнародний пакт про громадянські та політичні права в Статті 17 передбачає, що ніхто не може зазнавати свавільного або незаконного втручання у його особисте життя, сім'ю, житло чи листування, а також незаконних нападів на його честь та репутацію. У Статті 17 також зазначається, що кожен має право на захист за законом від такого втручання або нападів.

[26] «Поняття мозаїчного ефекту походить від мозаїчної теорії збору розвідувальних даних, в якій окремі фрагменти інформації, незважаючи на те, що вони окремо мають обмежену корисність, стають значними у поєднанні з іншими типами інформації (Pozen, 2005 рік). Застосовуючи дані загальнодоступного використання, концепція мозаїчного ефекту передбачає, що навіть анонімізовані дані, які можуть здатися безпечними окремо, можуть стати вразливими до повторної ідентифікації, якщо буде опубліковано достатньо наборів даних, що містять подібну чи доповнювальну інформацію». Див. Джон Чайка (John Czajka) та інші,

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

слідчі повинні знати, що в деяких юрисдикціях постійний моніторинг осіб в Інтернеті або систематичний збір та тривале зберігання персональних даних може вимагати додаткових дозволів та запобіжних заходів у зв'язку з посиленням проблем конфіденційності, викликаних такими видами діяльності.[27]

5. Поінформованість про безпеку

29. У той час як безпека за замовчуванням[28] стосується архітектури та інфраструктури розслідування та будь-яких другорядних дій, принцип поінформованості про безпеку зосереджується на міркуваннях, які люди повинні враховувати під час своєї роботи – зокрема, усвідомлення своєї поведінки в Інтернеті. Усі особи, які проводять розслідування в Інтернеті, повинні мати базову обізнаність щодо оперативної безпеки для мінімізації свого цифрового сліду та усвідомлення потенційних ризиків. Організації, які проводять розслідування з використанням даних у відкритому доступі, повинні забезпечити, щоб їх слідчі пройшли навчання з інформаційної безпеки, для розуміння ризиків, з якими вони можуть зіткнутися, і розуміння трьох основних рівнів інформаційної безпеки: (a) конфіденційність (наприклад, дозволяти лише повноважним користувачам отримувати доступ до даних); (b) цілісність (забезпечення того, щоб дані не підроблялися та не змінювалися іншим чином неавторизованими користувачами); і (c) доступність (забезпечення доступності систем та даних авторизованим користувачам, коли вони цього потребують). Навчання також має бути зосереджено на структурі управління Інтернету. Перед тим, як розпочати розслідування в Інтернеті, слід проводити оцінки загроз та ризиків і періодично їх переглядати та вносити необхідні зміни. Безпека – це відповідальність кожного, а не лише підрозділів інформаційних технологій або менеджерів з питань ризиків порушення безпеки.

B. Методологічні принципи

1. Точність

30. Існує методологічний та етичний імператив для забезпечення точності – а отже, і якості – розслідувань, спираючись лише на достовірні матеріали. Слідчі, що ведуть

Мінімізація ризику розкриття інформації у ініціативах відкритих даних HHS (Вашингтон, округ Колумбія, Mathematica Policy Research, 2014 рік), додаток E, стор. E-7. Доступно на сторінці https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. Див. також Девід Е. Позен (David E. Pozen), «Мозаїчна теорія, національна безпека та Закон про свободу доступу до інформації», Yale Law Journal, том 115, № 3 (грудень 2005 року), стор. 628-679

[27] Наприклад, у Сполученому Королівстві Великобританії та Північної Ірландії закон передбачає, що «особисті дані, які обробляються для ... правоохоронних цілей, повинні зберігатися не довше, ніж це необхідно для цілей, для яких вони обробляються» (Глава 12 Закон про захист даних 2018, частина 3, глава 3, розділ 39 (1)). Відповідно до Регламенту Європейського Парламенту та Ради 2016/679 від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЕС (Генеральний регламент про захист персональних даних), персональні дані можуть збиратися лише для «конкретних, явних та законних цілей», повинні обмежуватися інформацією, необхідною для цілей, для яких вони збираються, і повинні залишатися такими, що піддаються ідентифікації, лише стільки часу, скільки це необхідно для цілей збору (статті 5-6).

[28] Див. пункт 33 нижче.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

розслідування з використанням даних у відкритому доступі, повинні прагнути бути максимально правдивими та точними під час своїх розслідувань та представлення будь-яких результатів, особливо коли мова йде про визнання слабких місць у базових даних чи загальній ситуації. Точність часто підвищується за допомогою використання та перевірки кількох робочих гіпотез та/або експертної перевірки, обидві з яких можуть допомогти мінімізувати шанси упередженого відбору, інтерпретації та представлення даних. Не слід перебільшувати аналітичні висновки. Використання чіткої, об'єктивної, заснованої на фактах мови та уникнення емоційної мови захистить фактичну та сприйману об'єктивність розслідування та його результати.

2. Мінімізація даних

31. Принцип мінімізації даних передбачає, що збирати та обробляти цифрову інформацію можна лише у випадках, коли це: (a) виправдано для чіткої мети; (b) необхідно для досягнення цієї мети; і (c) пропорційно здатності досягти цієї мети.[29] У контексті розслідувань з використанням даних у відкритому доступі, онлайн-контент слід збирати лише у тому випадку, якщо він має відношення до конкретного розслідування. Цей принцип надає перевагу детальному, ручному збору, а не масовому, автоматизованому збору, зауважуючи, що останній може бути доречним у деяких випадках. Застосування цього принципу до збору онлайн-контенту допоможе уникнути надмірного збору, що важливо з кількох причин. Надмірний збір – особлива проблема при використанні процесів автоматизованого збору – може створювати або посилювати вразливості системи безпеки[30], зокрема, якщо це призводить до того, що слідчі не знають про типи інформації, якими вони володіють. Надмірний збір може також викликати проблеми конфіденційності та захисту даних, якщо автоматизований процес не проводить розмежування відповідно до типу контенту. Нарешті, уникнення надмірного збору служить практичним цілям мінімізації витрат на зберігання та запобігання перешкодам на різних етапах циклу розслідування, таких як огляд, аналіз та, у разі, якщо розслідування призведе до судового розгляду, розкриття інформації.

3. Збереження

32. Не менш важливим, ніж уникнення надмірного збору релевантної інформації, є запобігання недостатньому збору. Це може викликати особливе занепокоєння у контексті інформації в Інтернеті, постійність та доступність якої часто є сумнівною. Принцип збереження покликаний уникнути недостатнього збору, щоб не втратити відповідні та потенційно переконливі докази. Платформи соціальних медіа, наприклад, можуть видаляти контент, який порушує їхні умови користувацької угоди, навіть якщо цей контент має потенційну цінність для слідчих. Якщо до платформи не подано своєчасний запит на збереження або слідчі не збережуть контент в інший спосіб, така інформація може бути втрачена назавжди. Крім того, користувачі можуть вирішити видалити чи редагувати власний контент, що робить публічну інформацію недоступною. Крім того, інформацію в

---

[29] Протокол виводить принцип мінімізації даних із Генерального регламенту Європейського Союзу щодо захисту даних, але пристосовує його до контексту розслідування з використанням даних у відкритому доступі (див. статтю 5 Регламенту).

[30] Див. главу IV нижче про безпеку для отримання прикладів вразливостей системи безпеки.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Інтернеті можна легко деконтекстуалізувати, втратити, стерти чи пошкодити. Щоб цифровий матеріал залишався доступним та придатним для використання у майбутніх механізмах підзвітності, його потрібно активно та ретельно зберігати як у короткостроковій, так і в довгостроковій перспективі.[31]

4. Безпека за замовчуванням

33. Принцип безпеки за замовчуванням вимагає, щоб, наскільки це можливо, цифрова інформація та операції в Інтернеті були захищені за замовчуванням. Організації, які проводять онлайн-розслідування з використанням даних у відкритому доступі, повинні інвестувати та впроваджувати відповідні технічні та структурні заходи, щоб гарантувати належну анонімізацію та запобігання віднесенню інфраструктури за замовчуванням, включаючи апаратне та програмне забезпечення, коли слідчі виходять у мережу. Все обладнання повинно мати оновлене програмне забезпечення для захисту від шкідливого програмного забезпечення та відповідні налаштування конфіденційності та безпеки. До початку онлайн-розслідування мають бути вжиті заходи безпеки; їх слід постійно контролювати, оновлювати та коригувати у разі потреби. Слідчі, слідчі групи або організації можуть захотіти організувати постійне тестування, включаючи тестування на проникнення,[32] щоб переконатися, що їхня система безпеки працює відповідно до проекту.

C. Етичні принципи

1. Гідність

34. Розслідування слід проводити з усвідомленням та чутливістю до будь-яких проблем, пов'язаних з гідністю, особливо тих інтересів, які захищені міжнародним законодавством з прав людини. Наприклад, слідчі повинні дотримуватись принципів недискримінації, які можуть вплинути на те, що розслідується, і хто проводить розслідування або кому приписується розслідування, та інтегрувати запобіжні заходи щодо цифрової, фізичної та психосоціальної безпеки свідків, тих, хто вижив, інших слідчих, обвинувачених та інших, на кого це може негативно вплинути. Дотримання принципу гідності також може вплинути на те, що публічно повідомляється про розслідування, у тому числі в письмовій формі та у будь-яких наочних матеріалах – наприклад, не показуючи повного обсягу страждань чи насильства, якщо це не потрібно. Цей принцип гарантує, що норми прав людини є керівним набором стандартів для проведення етичних розслідувань з використанням даних у відкритому доступі.

2. Тактичність

35. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні бути тактичними, усвідомлювати свої обмеження та бути поінформованими про те, чого вони не знають. Для належного розуміння та інтерпретації інформації у відкритому доступі може знадобитися спеціалізоване навчання або консультації з експертами.

---

[31] Див. главу VI.D нижче про збереження для отримання більш детальної інформації.
[32] Тест на проникнення – це змодельована кібератака, що була санкціонована для перевірки безпеки системи.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Тактичність також означає брати на себе відповідальність за помилки. Якщо слідчі виявлять, що вони допустили помилку, її слід виправити або повідомити про це тих, хто може мінімізувати заподіяну шкоду. В ідеалі повинен існувати механізм повідомлення про помилки та виправлення, особливо для розслідувань, які є публічними та широко поширюються.

3. Інклюзивність

36. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні забезпечити, щоб у розслідування було включено цілий ряд перспектив та досвіду. Фактори, які слід врахувати, які можуть вплинути на загальну інклюзивність онлайн-розслідування, включають його географічний масштаб, порушення та/або міжнародні злочини, що розслідуються, та усвідомлення нерівномірності інформації в Інтернеті щодо різних верств суспільства.[33] Слідчі групи також повинні бути різноманітними, що включає наявність гендерного балансу. Крім того, принцип інклюзивності разом з принципом гідності може вплинути на матеріали, які слідчий вирішує зібрати та використати під час розслідування, і на те, як вони будуть представлені різним аудиторіям.

4. Незалежність

37. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні захищати себе та свої розслідування від неналежного впливу. Вони повинні виявляти і уникати будь-яких реальних або передбачуваних конфліктів інтересів та запроваджувати запобіжні заходи для пом'якшення тих конфліктів, яких неможливо уникнути. Прозорість процесу, методів та фінансування може допомогти з оцінкою незалежності та захистити фактичну та сприйману незалежність розслідування.

5. Прозорість

38. Хоча принцип підзвітності вимагає прозорості методів слідчого та результатів, етичний принцип прозорості стосується того, як слідчі, що проводять розслідування з використанням даних у відкритому доступі, поводяться в Інтернеті та у зовнішньому світі. Це означає уникати надання недостовірних даних.[34] While anonymity and non-attribution - including the use of virtual identities[35] – це може бути важливим з міркувань безпеки, слідчі повинні знати про потенційні негативні наслідки введення в оману, такі як шкода репутації та авторитету розслідування, групи чи організації або забруднення зібраної інформації. Одержання інформації шляхом введення в оману може порушити право цільової особи на конфіденційність та/або зашкодити розслідуванню, особливо якщо надання недостовірних даних є незаконним у відповідних юрисдикціях.

---

[33] Див. главу V.B нижче про оцінку цифрового середовища.

[34] Наприклад, намагаючись приєднатися до закритих груп або встановити зв'язок у соціальних мережах під фальшивими приводами.

[35] Обговорення віртуальних особистостей див. у главі IV.C нижче про міркування, пов'язані з інфраструктурою.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

III

НОРМАТИВНО-ПРАВОВА БАЗА

РЕЗЮМЕ ГЛАВИ

- Визначення того, які закони застосовуються, має вирішальне значення при прийнятті рішення про те, що збирати, та про найкращі способи це зробити. Це буде змінюватися в залежності від особи слідчих, особистості їх цілей, мети їх розслідування та юрисдикції, в якій вони, цілі, дані та юридичні процеси, знаходяться.

- Збереження цифрового матеріалу таким чином, щоб зберегти його автентичність та документувати ланцюг забезпечення збереження, збільшить ймовірність того, що він може бути прийнятий як доказ у суді.

- Визначення типу розслідування та його кінцевої мети (наприклад, кримінальне провадження, цивільне судочинство, процес правосуддя перехідного періоду тощо) визначатиме доказовий поріг, який слід застосувати.

- Порушення права особи на недоторканість приватного життя може призвести до виключення доказів.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

39. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розуміти нормативно-правову базу, в якій вони працюють. Це включає знання відповідних правових норм, що стосуються їхніх розслідувань, та правових основ юрисдикцій, у яких вони проводять слідчу діяльність. Знання основних законів, що застосовуються до розслідувань, включаючи елементи потенційних порушень[36] чи злочинів, а також способи відповідальності,[37] може призвести до більш цілеспрямованих розслідувань та збільшить ймовірність того, що зібрана інформація та будь-які зроблені аналітичні висновки будуть корисними при забезпеченні справедливості та відповідальності. Подібним чином, знання процесуального законодавства та правил доказування у відповідних юрисдикціях дозволить слідчим проводити свою роботу у спосіб, що відповідає вимогам щодо використання інформації у відкритому доступі у судових процесах.

40. Для міжнародних кримінальних розслідувань правова база буде прописана статутними документами відповідного трибуналу, суду або судової системи.[38] Для міжнародних розслідувань, таких як слідчі комісії, механізм розслідування, серед інших чинників, встановлюватиме чинні правові норми та географічний та часовий обсяг

---

[36] Наприклад, якщо розслідують мову ворожнечі та спонукання до насильства, слідчі повинні розуміти тип поведінки, який досягає високого порогу відповідно до статті 20(2) Міжнародного пакту про громадянські та політичні права. Див. План дій Рабату щодо заборони пропаганди національної, расової чи релігійної ворожнечі, що становить розпалювання дискримінації, ворожнечі чи насильства (A/HRC/22/17/Add.4, додаток), пункти 11 та 29 та його пороговий тест на основі прав людини, доступний 32 мовами. Доступно на сторінці www.ohchr. org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx. Щодо мови ворожнечі див. Стратегію та План дій Організації Об'єднаних Націй щодо мови ворожнечі (2019 рік). Доступно на сторінці www.un.org/en/genocideprevention/hate-speech-strategy.shtml.

[37] У кримінальному законодавстві злочинці можуть бути притягнуті до відповідальності на основі ряду видів відповідальності, визначених відповідним статутом. Такі види відповідальності включають пряме та непряме скоєння злочинів, співвиконання, сприяння та підбурювання та командну відповідальність. Див. Джером де Хемптінне (Jérôme de Hemptinne), Роберт Рот (Robert Roth) та Еліс ван Слідрегт (Elies van Sliedregt), ред., Режими відповідальності у міжнародному кримінальному праві (Кембридж, Велика Британія, Cambridge University Press, 2019 рік).

[38] Див., наприклад, Міжнародний кримінальний суд, Правила процедури та доказування (2013 рік); Міжнародний трибунал по колишній Югославії, Правила процедури та доказування (08 липня 2015 року); Міжнародний кримінальний трибунал по Руанді, Правила процедури та доказування (13 травня 2015 року); Залишковий спеціальний суд у Сьєрра-Леоне, Правила процедури та доказування (30 листопада 2018 року); Спеціальний трибунал по Лівану, Правила процедури та доказування (10 квітня 2019 року); Палати з надзвичайних справ у судах Камбоджі, Внутрішні правила (03 серпня 2011 року).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

географічний та часовий обсяг розслідування.[39] Для інших розслідувань, включаючи ті, які проводяться НУО, слідча установа сама може визначити власну правову базу.[40]

41. Ця глава була розроблена, щоб допомогти слідчим, що ведуть розслідування з використанням даних у відкритому доступі, краще оцінити та зрозуміти потенційне кінцеве використання своєї роботи та відповідно адаптувати свої методи розслідування. Оскільки чинне законодавство змінюється залежно від юрисдикції, типу розслідування та юридичних повноважень слідчого органу, у наступних розділах подається огляд основних міркувань при розслідуванні можливих порушень міжнародного права. Рекомендується, щоб слідчі, де це можливо, отримували експертні юридичні консультації від юристів, знайомих з відповідними юрисдикціями та предметом розгляду.

A. Міжнародне публічне право

42. Протокол зосереджений на трьох категоріях міжнародного публічного права зі значним перекриттям: міжнародному гуманітарному праві, міжнародному праві у сфері прав людини та міжнародному кримінальному праві. Три категорії взаємно зміцнюються; дійсно, застосування міжнародного гуманітарного права та/або міжнародного кримінального права не звільняє держави від виконання своїх зобов'язань за міжнародним правом у сфері прав людини. Нижче наведено огляд кожної галузі практики, включаючи джерела права та відмінності між галузями практики, щоб слідчі, що ведуть розслідування з використанням даних у відкритому доступі, знали, якими посиланнями вони повинні керуватися під час своєї роботи.

1. Міжнародне гуманітарне право

43. Міжнародне гуманітарне право або «право збройного конфлікту» регулює ведення бойових дій та вирішує гуманітарні питання, що виникають у контексті таких конфліктів, які можуть мати міжнародний або неміжнародний характер.[41] Міжнародне гуманітарне

---

[39] Наприклад, незалежна міжнародна місія з встановлення фактів у Болівариансько Республіці Венесуела, створена у вересні 2019 року, має мандат розслідувати позасудові страти, примусові зникнення, довільні затримання та катування та інше жорстоке, нелюдське чи таке, що принижує гідність, поводження, починаючи з 2014 року, та надавати доповідь Раді про свої висновки (резолюція Ради з прав людини 42/25, пункт 24). Незалежна міжнародна комісія ООН з розслідування подій в Сирійській Арабській Республіці, створена в 2011 році, має мандат розслідувати всі передбачувані порушення міжнародного законодавства з прав людини з березня 2011 року в Сирійській Арабській Республіці, щоб встановити факти та обставини, які можуть бути такими порушеннями та злочинами, і, за можливості, встановити осіб, відповідальних за це (резолюція Ради з прав людини S-17/1, пункт 13). Міжнародна група експертів, надіслана до регіону Касаї Демократичної Республіки Конго у 2017 році, отримала мандат збирати та зберігати інформацію про ймовірні порушення прав людини та порушення міжнародного гуманітарного права у регіонах Касаї та передавати до судових органів Демократичної Республіки Конго висновки цього розслідування (резолюція 35/33 Ради з прав людини, пункт 10).

[40] Деякі організації, включаючи НУО, часто мають власні внутрішні методології, які вимагають від них зосередження уваги на певній галузі права, наприклад, стосовно катувань або сексуального та гендерного насильства, які також надають вказівки щодо спрямованості розслідувань.

[41] Відмінність міжнародного та неміжнародного збройного конфлікту ґрунтується на двох факторах: структурі та статусі залучених сторін. Міжнародні збройні конфлікти стосуються суверенних держав. На противагу цьому, неміжнародні збройні конфлікти стосуються держав та організованих збройних формувань. Див.

право набуває чинності, коли збройний конфлікт починається і продовжується до досягнення миру, хоча ці розмежування не завжди є чіткими або однозначними.[42] Основними джерелами міжнародного гуманітарного права є Гаазькі конвенції 1899 та 1907 рр.,[43] Женевські конвенції від 12 серпня 1949 року[44] та Додаткові протоколи до них 1977 року,[45] а також кілька договорів, які регулюють застосування певних видів зброї.[46] Звичаєве право також є важливим джерелом міжнародного гуманітарного права, оскільки заповнює прогалини, залишені договорами. Звичаєве міжнародне гуманітарне право є обов'язковим для всіх сторін конфлікту і має особливе значення для неміжнародних збройних конфліктів, оскільки пов'язані з ним правила більш детальні, ніж правила міжнародного гуманітарного права на основі договорів.[47] До початку 1990-х років основними механізмами застосування міжнародного гуманітарного права були національні військові трибунали, де держави притягували до відповідальності своїх членів та офіцерів. З розвитком міжнародних кримінальних трибуналів деякі серйозні порушення міжнародного гуманітарного права

Ендрю Клафам (Andrew Clapham), Паола Гаета (Paola Gaeta) та Марко Сассолі (Marco Sassoli), ред., Женевські конвенції 1949 року, Коментар (Оксфорд, Oxford University Press, 2015 рік), глави 1 та 19.

[42] Хоча початок міжнародного конфлікту є відносно чітким, оскільки він викликаний будь-яким застосуванням сили між двома державами, початок збройного конфлікту, що не є міжнародним, є менш простим. Неміжнародні збройні конфлікти існують лише за умови, якщо збройні групи достатньо організовані і рівень насильства досягає певної інтенсивності – двох факторів, які потребують детального аналізу фактів у кожному конкретному випадку. Див. Сильвен Віте (Sylvain Vite), «Типологія збройних конфліктів у міжнародному гуманітарному праві: правові концепції та реальні ситуації», International Review of the Red Cross, том 91, № 873 (березень 2009 року), стор. 72 та 76-77. Існує також суперечка щодо того, коли закінчується збройний конфлікт і досягається мир. Хоча припинення вогню або мирні угоди можуть допомогти продемонструвати закінчення збройного конфлікту, вони не є диспозитивними. Були запропоновані різні критерії припинення збройного конфлікту, а саме загальне припинення військових операцій після досягнення загального миру, існування мирової угоди та припинення критеріїв для ідентифікації існування конфлікту. Див. Наталі Вейцман (Nathalie Weizmann), «Кінець збройного конфлікту, припинення участі у збройному конфлікті та припинення бойових дій: наслідки для операцій з утримання під вартою згідно з AUMF 2001», Columbia Human Rights Law Review, том 47, № 3 (2016 рік), стор. 221-224.

[43] Відповідно, Конвенція про закони та звичаї сухопутної війни (Гаазька конвенція II) та Конвенція про закони та звичаї війни на суші (Гаазька конвенція IV).

[44] Див. Женевська конвенція про покращення стану поранених та хворих у збройних силах на місцях (Женевська конвенція I); Женевська конвенція про поліпшення стану поранених, хворих та корабельних військовослужбовців збройних сил на морі (Женевська конвенція II); Женевська конвенція про поводження з військовополоненими (Женевська конвенція III); Женевська конвенція про захист цивільних осіб під час війни (Женевська конвенція IV).

[45] Див. Додатковий протокол до Женевських конвенцій 1949 року від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I); Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв не міжнародних збройних конфліктів (Протокол II).

[46] Див., наприклад, Конвенція про заборону розробки, виробництва та накопичення запасів бактеріологічної (біологічної) та токсичної зброї та про її знищення; Конвенція про заборону або обмеження використання певної звичайної зброї, яка може вважатися надмірно травмуючою або мати невибіркову дію; Конвенція про заборону розробки, виробництва, накопичення та використання хімічної зброї та про її знищення; Конвенція про заборону використання, накопичення запасів, виробництво та передачу протипіхотних мін та про їх знищення; Конвенція про касетні боєприпаси. Див. також Міжнародний Комітет Червоного Хреста (МКЧХ), «Зброя», 30 листопада 2011 року. Доступно на сторінці www.icrc.org/en/document/weapons.

[47] Див. МКЧХ, «Звичаєве міжнародне гуманітарне право», 29 жовтня 2010 року. Доступно на сторінці www.icrc.org/en/document/customary-international-humanitarian-law-0. Див. також МКЧХ, «Ласкаво просимо до звичайної бази даних МГП». Доступно на сторінці https://ihl-databases.icrc. org/customary-ihl/eng/docs/home.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

були кодифіковані в установчих статутах трибуналів як військові злочини,[48] що відкрило новий шлях до застосування міжнародного гуманітарного права на міжнародному рівні. Деякі держави також кодифікували військові злочини у своєму національному законодавстві,[49] щоб такі справи могли розглядатись у їхніх звичайних судових системах, на відміну від військових судів. Національні справи можуть мати місце у країні конфлікту або все частіше в інших країнах за принципом універсальної юрисдикції.[50] Ряд держав створили спеціалізовані підрозділи з питань військових злочинів для розгляду таких справ. Міжнародні кримінальні трибунали та національні суди сприяють зростанню судово-правової практики з міжнародного гуманітарного права, що також служить важливим джерелом права, норми якого можуть бути обов'язковими в залежності від юрисдикції.

2. Міжнародне право у сфері прав людини

44. Держави мають зобов'язання та обов'язки відповідно до міжнародного права поважати, захищати та виконувати права людини. Загальна декларація прав людини, прийнята 1948 у році, є основою міжнародного права у сфері прав людини. Незважаючи на те, що вона має амбіційний характер і не має юридичної сили, деякі її статті є частиною міжнародного звичаєвого права.[51] Вона також стала основою для двох угод і великого пласта договорів з прав людини.[52] Держави пов'язуються лише тими угодами та договорами, які вони підписали та ратифікували, якщо тільки норми, що містяться в цих документах, не набули статусу міжнародного звичаєвого права.[53] Міжнародне право в

---

[48] Наприклад, стаття 8 Римського статуту Міжнародного кримінального суду кодифікує міжнародне гуманітарне право у визначенні військових злочинів.

[49] Див., наприклад: Австралія (Закон про військові злочини 1945 року, зі змінами та доповненнями, розділ 7); Боснія і Герцеговина (Кримінальний кодекс, статті 171-184); Кенія (Закон про міжнародні злочини 2008, розділ 6 (1) (c) та (2)-(4)); Нова Зеландія (Закон про міжнародні злочини та Міжнародний кримінальний суд 2000 року, розділ 11); Південно-Африканська Республіка (Закон про впровадження Женевських конвенцій 2012 року).

[50] Відповідно до «універсальної юрисдикції» національний суд може притягати до відповідальності осіб за тяжкі злочини проти міжнародного права, такі як злочини проти людяності, військові злочини, геноцид та катування, які мали місце поза межами держави, на основі принципу, що такі злочини завдають шкоди міжнародній спільноті та самому міжнародному порядку, для захисту яких можуть діяти окремі держави. Див. Міжнародний ресурсний центр правосуддя, «Універсальна юрисдикція». Доступно на сторінці https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

[51] Численні країни, чиновники та науковці Організації Об'єднаних Націй заявляли, що більшість статей Загальної декларації прав людини, якщо не всі, становлять звичаєве міжнародне право. Зокрема, заборони проти рабства, свавільного позбавлення життя, катувань, свавільних затримань та расової дискримінації, кодифіковані у Загальній декларації прав людини, прийняті як такі, що становлять звичаєве міжнародне право. Див. Херст Ханнум (Hurst Hannum), «Статус Загальної декларації прав людини в національному та міжнародному праві», Hurst Hannum, том 25, № 1 (1996 рік), стор. 322-332 та 341-346.

[52] Див. Міжнародна конвенція про ліквідацію всіх форм расової дискримінації; Міжнародний пакт про громадянські та політичні права; Міжнародний пакт про економічні, соціальні та культурні права; Конвенція про ліквідацію всіх форм дискримінації щодо жінок; Конвенція проти катувань та інших жорстоких, нелюдських чи таких, що принижують гідність, видів поводження чи покарання; Конвенція про права дитини. Для отримання додаткової інформації про основні договори Організації Об'єднаних Націй з прав людини див. УВКПЛ «Основні міжнародні документи з прав людини та їх моніторинг». Доступно на сторінці www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx.

[53] Звичаєве міжнародне право відноситься до міжнародних зобов'язань, що випливають із усталеної міжнародної практики, на відміну від зобов'язань, що випливають з офіційних письмових конвенцій та договорів. Воно випливає із загальної та послідовної практики держав, яку вони встановлюють із почуття

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

галузі прав людини також було включено до статутної бази багатьох міжнародних кримінальних трибуналів. Крім того, існує кілька регіональних судів з прав людини, створених міжнародними конвенціями з мандатами розглядати справи проти держав-учасниць цих конвенцій про порушення міжнародного законодавства з прав людини, включаючи Африканський суд з прав людини та народів,[54] Європейський суд з прав людини[55] та Міжамериканський суд з прав людини.[56] На регіональному рівні існують додаткові органи з прав людини, включаючи Африканську комісію з прав людини та народів, Європейський комітет із соціальних прав та Міжамериканську комісію з прав людини, які продовжують розвивати юриспруденцію щодо міжнародного права в області прав людини.

45. Міжнародні організації також відіграють ключову роль у розробці та встановленні стандартів звичаєвого міжнародного права з прав людини.[57] Управління Верховного комісара Організації Об'єднаних Націй з прав людини (УВКПЛ), а також інші міжнародні утворення публікують тематичні звіти щодо галузей права, які сприяють встановленню стандартів та розробці правових норм, які не носять обов'язковий характер. Договірні органи з прав людини[58] складають звіти,[59] прецедентне право[60] та інші форми керівництва,

---

юридичного обов'язку. Фундаментальною складовою міжнародного звичаєвого права є jus cogens, який посилається на певні фундаментальні принципи міжнародного права. Див., наприклад, Інститут правової інформації, «Звичаєве міжнародне право» та «Jus cogens», Юридична школа Корнелла. Доступно на сторінці www.law.cornell.edu/wex.

[54] Заснований відповідно до Африканської хартії прав людини та народів (Хартія Банджула).

[55] Заснований відповідно до Конвенції про захист прав людини та основоположних свобод (Європейська конвенція з прав людини).

[56] Заснований відповідно до Американської конвенції з прав людини (Пакт Сан-Хосе).

[57] Приклади міжнародних організацій включають Міжнародний кримінальний суд, Міжнародну організацію з міграції та Організацію із заборони хімічної зброї, а також механізми захисту прав людини, такі як спеціальні процедури та слідчі комісії Ради з прав людини або їх еквівалент. Спеціальні процедури здійснюють свої мандати стосовно всіх держав-членів Організації Об'єднаних Націй; вони не залежать від ратифікації певного договору. Існують відмінності в правових нормах та механізмі роботи цих правозахисних механізмів, а також відмінності у методах та стандартах збору інформації. Наприклад, основним методом роботи Робочої групи з питань довільних затримання є отримання інформації від зацікавлених осіб, їх сімей чи представників, урядів, громадських організацій та національних установ щодо окремих випадків. Потім Робоча група розслідує випадки, про які повідомлялося, у тому числі під час відвідування країн. Див. A/HRC/36/38 щодо останніх методів роботи Робочої групи. Навпаки, слідчі комісії створюються Радою з прав людини на спеціальній основі і зазвичай ініціюють власні розслідування відповідно до умов їхніх мандатів, часто шляхом відвідування країн, під час яких вони, серед іншого, проводять опитування свідків. Див., наприклад, повноваження слідчої комісії щодо Бурунді. Доступно на сторінці www.ohchr.org/Documents/HRBodies/HRCouncil/ColBurundi/TermsofreferenceCOIBurundiENGL.pdf.

[58] Див., наприклад, УВКПЛ «Договірні органи з прав людини». Доступно на сторінці www.ohchr.org/EN/HRBodies/Pages/TreatyBodies.aspx.

[59] Звіти можуть бути у формі заключних зауважень, при яких договірний орган розглядає доповіді, подані державами-учасницями та іншими зацікавленими сторонами щодо виконання зобов'язань держав за певним договором. Деякі договірні органи також можуть видавати звіти про запити. Див., наприклад, Комітет з ліквідації дискримінації щодо жінок, «Процедура розслідування». Доступно на сторінці www.ohchr.org/EN/HRBodies/CEDAW/Pages/InquiryProcedure.aspx.

[60] Договірні органи видають Погляди на індивідуальні скарги у відповідь на конкретні справи. Див., загалом, УВКПЛ «Договірні органи з прав людини – індивідуальні повідомлення». Доступно на сторінці www.ohchr.org/EN/HRBodies/TBPetitions/Pages/IndividualCommunications.aspx#proceduregenerale.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

включаючи загальні зауваження та загальні рекомендації,[61] які сприяють розробці та розумінню статей відповідних договорів. Так само спеціальні процедури Ради з прав людини відіграють певну роль у еволюції норм встановлення стандартів у міжнародному праві прав людини,[62] як і інші механізми, включаючи місії з встановлення фактів та слідчі комісії.

46. Подібно до міжнародного гуманітарного права, міжнародне право у галузі прав людини стало частиною правової бази багатьох країн або в результаті моністичних правових традицій, які безпосередньо застосовують міжнародні зобов'язання у національній сфері, або шляхом прямої інтеграції міжнародного права у національне законодавство, або шляхом застосування універсальної юрисдикції, тим самим розвиваючи важливу судову практику щодо такого права.[63]

3. Міжнародне кримінальне право

47. Міжнародне кримінальне право застосовується як у мирний час, так і під час збройного конфлікту, покладаючи кримінальну відповідальність на осіб, які здійснюють злочини відповідно до міжнародного права, включаючи військові злочини, злочини проти людяності та геноцид.[64] These crimes are sometimes collectively referred to as "atrocity crimes"[65] або «серйозні міжнародні злочини» і були значною мірою кодифіковані в Римському статуті, який, як правило, відображає звичаєве міжнародне кримінальне право. Міжнародне кримінальне право також включає деякі злочини, не кодифіковані Римським статутом, наприклад тероризм.[66] Можливо, існує певне перекриття між міжнародним кримінальним правом та суміжною галуззю транснаціонального кримінального права, яке передбачає кримінальну відповідальність за транскордонні дії, такі як торгівля людьми, наркотиками, зброєю та іншими незаконними товарами.[67] На відміну від міжнародного гуманітарного права та міжнародного права у галузі прав людини, міжнародне кримінальне право зосереджується на індивідуальній кримінальній відповідальності, а не на відповідальності держави. Справи міжнародного кримінального права можуть

---

[61] Див. УВКПЛ «Договірні органи з прав людини – загальні коментарі». Доступно на сторінці www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx.

[62] Див., загалом, УВКПЛ, «Спеціальні процедури Ради з прав людини». Доступно на сторінці www.ohchr.org/en/HRBodies/SP/Pages/Welcomepage.aspx.

[63] Amnesty International, Універсальна юрисдикція: Попередній огляд законодавства у всьому світі – оновлення 2012 року (Лондон, 2012 рік), стор. 1-2.

[64] Роберт Кріер (Robert Cryer), Дарріл Робінсон (Darryl Robinson) та Сергій Васильєв (Sergey Vasiliev), Вступ до міжнародного кримінального права та процесу, 4-е вид. (Кембридж, Великобританія, Cambridge University Press, 2019 рік), глава 15.

[65] Хоча термін «етнічна чистка» не включений до Римського статуту і не визначений як незалежний злочин згідно з міжнародним правом, він розглядався як такий, що належить до категорії «жорстоких злочинів». У цьому контексті див. Організацію Об'єднаних Націй, «Межі аналізу жорстоких злочинів: інструмент запобігання», стор. 1. Доступно на сторінціwww.un.org/en/genocideprevention/documents/about-us/Doc.3_Framework%20of%20Analysis%20for%20Atrocity%20Crimes_EN.pdf.

[66] Див. Резолюцію 1757 (2007) Ради Безпеки, додаток, Доповнення (Статут Спеціального трибуналу по Лівану), стаття 2.

[67] Кріер (Cryer), Робінсон (Robinson) та Васильєв (Vasiliev), Вступ до міжнародного кримінального права та процесу, глава 15.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

розглядатися в національних кримінальних судах, гібридних кримінальних трибуналах,[68] міжнародних кримінальних судах або трибуналах,[69] включаючи Міжнародний кримінальний суд, або національні суди, які здійснюють універсальну юрисдикцію. Джерела міжнародного кримінального права включають установчі документи судів і трибуналів (наприклад, резолюції Ради Безпеки, статути, правила процедури та доказування та положення судів) та національне законодавство держав, які здійснюють юрисдикцію щодо міжнародних злочинів. Іншим важливим джерелом міжнародного кримінального права є судова практика, яка може бути обов'язковою чи переконливою залежно від юрисдикції.[70]

B. Юрисдикція та підзвітність

48. Юрисдикція – це юридичний термін, який позначає повноваження, надані юридичній особі, наприклад, суду або трибуналу, для встановлення, винесення та виконання закону. Справедливість та відповідальність широко визначені в Протоколі для посилання на різні типи судових та несудових процесів. Відповідальність за міжнародні злочини та порушення міжнародного права в галузі прав людини та/або міжнародного гуманітарного права може бути результатом судових розглядів, які можуть мати кримінальний, цивільний або адміністративний характер, а також неправомірних процедур, таких як звіти про міжнародні розслідування прав людини, включаючи слідчі комісії та місії з встановлення фактів, та інших механізмів правосуддя перехідного періоду, включаючи ініціативи, спрямовані на пошук правди. Слідчі повинні прагнути, за можливості, враховувати коло можливих юрисдикцій, в яких можна вимагати відповідальності.

49. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні визначити механізми відповідальності, які можуть мати відношення до їхньої роботи, та потенційні місця, де зібрані докази могли або можуть бути допущені для встановлення фактів. Однак на ранніх стадіях міжнародних розслідувань це може бути невідомим або неясним. Це особливо вірно, якщо держава, в якій були вчинені злочини, не має функціонуючої судової системи або коли міжнародне співтовариство ще не повністю охоплене розслідуванням цього питання. Крім того, може бути неможливо передбачити всі юрисдикції, які можуть бути релевантними в майбутньому. Коли слідчі, що ведуть розслідування з використанням даних у відкритому доступі, не знають конкретного механізму чи юрисдикції, вони повинні прагнути збирати та зберігати інформацію таким чином, щоб максимально використовувати її у найширшому діапазоні потенційно релевантних юрисдикцій. Якщо слідчі знають про відповідні вимоги до місця, де врешті-решт буде розглядатися справа, вони повинні адаптувати свої процеси до цих конкретних вимог.

---

[68] Цей термін включає, серед іншого, Палати з надзвичайних справах у судах Камбоджі, Спеціальний суд у Сьєрра-Леоне, Спеціальний трибунал по Лівану, Спеціальні палати Косово та Прокуратуру і Спеціальний кримінальний суд Центральноафриканської Республіки.

[69] Цей термін включає постійний Міжнародний кримінальний суд та Спеціальний Міжнародний трибунал по колишній Югославії, Міжнародний кримінальний трибунал по Руанді та Міжнародний залишковий механізм для міжнародних кримінальних трибуналів.

[70] Див. Роза Теофаніс (Rosa Theofanis), «Доктрина res judicata у міжнародному кримінальному праві», International Criminal Law Review, том 3, № 3 (2003 рік).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

50. Юрисдикцію можна встановити такими способами:

(a) Територіальна юрисдикція – це повноваження суду розглядати справи, що стосуються дій, які відбуваються на визначеній території. Для міжнародних трибуналів територіальна юрисдикція зазвичай обмежується територіями держав, які ратифікували засновницький договір;

(b) Тимчасова юрисдикція – це повноваження суду розглядати справи, у яких передбачувані дії мали місце протягом встановленого періоду часу;

(c) Особиста юрисдикція – це повноваження суду приймати рішення щодо учасника процесу;

(d) Предметна юрисдикція – це повноваження суду розглядати справи певного типу або справи, що стосуються конкретного предмета;

(e) Універсальна юрисдикція – це вимога суду щодо повноважень щодо обвинуваченого, незалежно від того, де був вчинений передбачуваний злочин, і незалежно від громадянства обвинуваченого, країни проживання чи будь-яких інших стосунків із суб'єктом обвинувачення.

C. Слідчі повноваження та обов'язки

51. Офіційні повноваження щодо розслідування – це право, надане законом конкретному суб'єкту для розслідування у межах певної юрисдикції. Подібно до обмежень судової влади, судова чи прокурорська установа може проводити розслідування лише тією мірою, якою вони мають на це право за законом.[71] Слідчі повноваження можуть включати здатність викликати свідків, видавати повістки та виконувати ордери на обшук. За законом слідча установа може бути зобов'язана за законом дотримуватися суворих процедур, а в деяких випадках може мати можливість визначити власні процедури.[72]

52. Більшість інших осіб, які розслідують порушення міжнародного права, як правило, не будуть наділені слідчими повноваженнями або примусовими засобами збирання доказів, такими як повістки або ордери на обшук. Таким чином, вони можуть повністю покладатися на інформацію з відкритого джерела та інформацію, надану добровільно, наприклад документи, цифрові файли та свідчення свідків.

53. Як правило, слідчі повноваження супроводжуються окремими обов'язками.[73] Незважаючи на те, що деякі слідчі можуть не мати поліцейських або інших юридичних

---

[71] Див. Justia, «Агентські розслідування». Доступно на сторінці www.justia.com/administrative-law/agency-investigations.

[72] З того самого джерела.

[73] Наприклад, стаття 54 Римського статуту визначає обов'язки та повноваження прокурора щодо розслідувань, встановлюючи здатність прокурора, зокрема, проводити розслідування, збирати та досліджувати докази, опитувати жертв та свідків і співпрацювати з державами та міжнародними організаціями.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

повноважень, рекомендується, наскільки це можливо, щоб усі слідчі прагнули виконувати ключові обов'язки слідчих з метою забезпечення якості розслідувань. Загальні обов'язки та зобов'язання судових слідчих та прокурорів включають обов'язок розслідувати обвинувальні та виправдальні обставини, обов'язок захищати свідків, обов'язок зберігати докази, обов'язок забезпечувати справедливість судового розгляду та зобов'язання поважати права обвинувачених.

54. У кримінальних справах прокурори також зобов'язані розкривати відповідну інформацію та докази стороні захисту.[74] Це включає більше, ніж просто докази, допущені під час судового розгляду, але й будь-яку інформацію, зібрану в межах розслідування, яка обвинувачує або виправдовує, включаючи інформацію, що стосується надійності свідків.[75] Існують певні винятки, пов'язані з конфіденційною інформацією або інформацією, яка може поставити людину під загрозу. Суд може наказати не розголошувати особу потерпілого чи свідка, якому таке розкриття може загрожувати, але це ніколи не гарантується.[76] У багатьох кримінальних юрисдикціях діють правила розкриття інформації, які вимагають від прокурорів передати все, що є потенційно виправдовувальним.[77] Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, які працюють над будь-якою справою з навіть найменшою ймовірністю, що вона опиниться в суді, повинні брати до уваги ці зобов'язання щодо розкриття інформації під час виконання своєї роботи.[78] Є ще кілька причин, чому слідчі повинні розглянути можливість розкриття інформації. Наприклад, якщо прокурори зобов'язані переглянути весь матеріал, зібраний під час розслідування, слідчим слід обережно збирати їх масово, оскільки великий обсяг інформації

---

[74] Див., наприклад, Міжнародний трибунал по колишній Югославії, Правила процедури та доказування, правило 66 (A); Міжнародний кримінальний трибунал по Руанді, Правила процедури та доказування, правило 66 (A); Спеціальний трибунал по Лівану, Правила процедури та доказування, правило 110 (A).

[75] Див., наприклад, Міжнародний кримінальний суд, Правила процедури та доказування, правила 76-84; Міжнародний трибунал по колишній Югославії, Правила процедури та доказування, правило 66 (A) (ii); Міжнародний кримінальний трибунал по Руанді, Правила процедури та доказування, правило 66 (A) (ii); Спеціальний суд з Сьєрра-Леоне, Правила процедури та доказування, правило 66 (A) (ii); Спеціальний трибунал по Лівану, Правила процедури та доказування, правило 110 (A) (ii); Спеціальні групи з розгляду тяжких злочинів у Східному Тиморі, Перехідні правила кримінального процесу, розділ 24.4.

[76] Див., наприклад, Міжнародний кримінальний суд, Правила процедури та доказування, правило 81 (4); Міжнародний трибунал по колишній Югославії, Правила процедури та доказування, правило 69; Міжнародний кримінальний трибунал по Руанді, Правила процедури та доказування, правило 69; Спеціальний суд у Сьєрра-Леоне, Правила процедури та доказування, правило 69; Спеціальний трибунал по Лівану, Правила процедури та доказування, правила 115-116; Спеціальні групи з розгляду тяжких злочинів у Східному Тиморі, Перехідні правила кримінального процесу, розділ 24.6.

[77] Див., наприклад, Міжнародний трибунал по колишній Югославії, Правила процедури та доказування, правило 68; Міжнародний кримінальний трибунал по Руанді, Правила процедури та доказування, правило 68; Спеціальний суд з Сьєрра-Леоне, Правила процедури та доказування, правило 68; Спеціальний трибунал по Лівану, Правила процедури та доказування, правило 113; Римський статут Міжнародного кримінального суду, стаття 67 (2); Спеціальні групи з розгляду тяжких злочинів у Східному Тиморі, Правила процедури та доказування, правило 24.4 (c). Виправдувальні докази – це докази, які можуть виправдати обвинуваченого. У Сполучених Штатах доктрина Брейді – це правило досудового відкриття, яке було встановлене Верховним Судом Сполучених Штатів і вимагало від прокуратури передати всі обвинувальні докази підсудному у кримінальній справі. Див. «Брейді (Brady) проти Меріленду», 378 США 83 (1963 рік).

[78] Оскільки зобов'язання щодо розкриття інформації можуть вимагати передачі частини або всіх зібраних матеріалів стороні захисту, здатність слідчих, що ведуть розслідування з використанням даних у відкритому доступі, захищати особу та іншу конфіденційну інформацію може бути заперечена.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

може бути надто обтяжливим або навіть неможливим для огляду. Це також має значення, коли йдеться про збереження та зберігання зібраної інформації, включаючи належне позначення тегами, що принесе значну користь тим, хто прагне отримати та переглянути матеріал пізніше.

D. Правила процедури та доказування

55. Під час роботи в контексті правового розслідування основне завдання слідчих, що ведуть розслідування з використанням даних у відкритому доступі, – збирати актуальну та достовірну інформацію, щоб її можна було використати для фактичних та юридичних висновків. Зокрема, у міжнародних судах та трибуналах слідчі повинні прагнути до забезпечення того, щоб будь-які зібрані докази у відкритому доступі були прийнятними, а також релевантними, достовірними та доказовими. Кримінальне розслідування відрізняється від розслідувань, що проводяться з іншими цілями, їх більш високим стандартом доказування[79] та більш жорсткими правилами процедури та доказування, включаючи допустимість, з метою захисту належного процесу та прав на справедливий судовий розгляд будь-яких обвинувачених.[80] Хоча планка допустимості доказів у міжнародних кримінальних судах та трибуналах, як правило, нижча, ніж у деяких національних судах, методи збору доказів все одно впливатимуть на вагу, яку судді надають доказам. Це справедливо у всіх юрисдикціях. В епоху, позначену розповсюдженням цифрової інформації, включаючи неправдиву інформацію та дезінформацію,[81] надзвичайно важливо, щоб слідчі мали змогу визначити, чи є інформація у відкритому доступі достовірною, та встановити чи спростувати її достовірність з достатньою точністю.[82]

56. Щодо судового розгляду, допустимість означає, чи може предмет, поданий стороною у провадженні, бути допущений до протоколу як доказ. Як правило, міжнародні кримінальні трибунали оцінюють допустимість предмета, що пропонується, за допомогою трифакторного критерію: a) релевантність; (b) доказова сила; та (c) доказова сила, зважена

---

[79] Наприклад, хоча міжнародні суди зазвичай застосовують кримінально-правовий стандарт доказування «поза розумним сумнівом», слідчі комісії та подібні органи найчастіше приймають нижчий стандарт «розумні підстави вважати», на якому базуються їх висновки. Для отримання додаткової інформації див. УВКПЛ, Слідчі комісії та місії з встановлення фактів з міжнародних прав людини та гуманітарного права: Керівництво та практика, стор. 62-63.

[80] Міжнародний кримінальний суд, Прокурор проти Жан-П'єра Бемби, справа № ICC-01/05-01/08 A, Рішення за апеляційною скаргою пана Жан-П'єра Бемби Гомбо (Jean-Pierre Bemba Gombo) на «Судове рішення Судової палати Іл відповідно до статті 74 Статуту», 08 червня 2018 року, Апеляційна палата, Окрема думка судді Ван ден Вінгерта (Van den Wyngaert) та судді Моррісона (Van den Wyngaert), пункт 5.

[81] Неправдива інформація – це недостовірна інформація, що не призначена для заподіяння шкоди. Наприклад, люди, які не знають, що інформація є неправдивою, можуть поширювати її в соціальних мережах, намагаючись бути корисними. Дезінформація – це неправдива інформація, яка навмисно створюється або поширюється з явною метою заподіяння шкоди. Ті, хто створюють дезінформацію, зазвичай мають політичні, фінансові, психологічні чи соціальні мотиви. Див. Клер Уордл (Claire Wardle), «Інформаційний розлад: основний глосарій» (Кембридж, Массачусетс, Центр Шоренштайна з медіа, політики та публічної політики, 2018 рік). Доступо на сторінці https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x32994.

[82] З того самого джерела.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

проти будь-якого шкідливого впливу на справедливість судового розгляду.[83] Річ буде релевантною, якщо вона допоможе зробити факт більш-менш ймовірним, тоді як її доказова сила означає, чи допомагає ця річ довести чи спростувати той факт, про який йдеться у справі. У разі несудових розслідувань застосовується оцінка, подібна до допустимості. Кожну інформацію слід оцінювати з точки зору її достовірності, релевантності та доказової сили, щоб визначити, чи може вона використовуватися та як її слід використовувати для визначення правових та/або фактичних висновків.[84]

57. Вага відноситься до сили, приписаної предмету, та до ступеня, на який в кінцевому підсумку будуть покладатися під час прийняття юридичного чи фактичного висновку. Визначення ваги має бути цілісною оцінкою, яка частково залежить від іншої інформації, яка може підтверджувати, підкріплювати чи суперечити даному факту. У багатьох судових розглядах допустимість та вага оцінюються окремо. В інших контекстах, у ситуаціях, коли допустимість доказів не є чинником, слідчі з прав людини застосовуватимуть подібний підхід для оцінки ваги, яку слід приписати інформації.

58. Правила процедури та доказування, що застосовуються до міжнародного кримінального провадження, можна знайти в установчих документах кожного суду, найчастіше в їх правилах процедури та доказування. Судова практика надає подальші вказівки. Залежно від характеру розслідування, можливо, варто звернутися за консультацією до юриста. Це особливо вірно, якщо розслідування має на меті сприяти судовим розглядам.

59. Інформація у відкритому доступі може бути поєднанням документальних доказів та свідчень. Наприклад, відеозапис особи, яка робить заяви, потрібно буде автентифікувати, а висловлювання, зроблені в ній, потрібно буде перевірити окремо.[85] Тому можуть застосовуватися засоби автентифікації цифрового об'єкта як документа або оцінки його

---

[83] Відповідно до Римського статуту (статті 64 (9) (a) та 69 (4)), Судова палата Міжнародного кримінального суду має «повноваження щодо звернення сторони або за її власним бажанням ... винести рішення щодо допустимості чи відповідності доказів... враховуючи, зокрема, доказову цінність доказів та будь-які упередження, які такі докази можуть спричинити до справедливого судового розгляду чи справедливої оцінки показань свідка, відповідно до Правил процедури та доказування».

[84] Див., наприклад, УВКПЛ, Слідчі комісії та місії з встановлення фактів з міжнародних прав людини та гуманітарного права: Керівництво та практика, зокрема глава IV.C про збір та оцінку інформації.

[85] Див. Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа, «Цифрові відбитки пальців: використання електронних доказів для переслідування у Міжнародному кримінальному суді» (Берклі, 2014 рік). Доступно на сторінці www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. Докази з чужих слів – це інформація, що не входить до прямих знань свідків. У деяких юрисдикціях докази з чужих слів неприпустимі, якщо вони не відповідають певному винятку. В інших випадках вони допустимі, але вони мають невелику вагу через те, що вони не може бути належним чином перевірені під час перехресного допиту ні стороною обвинувачення, ні стороною захисту. За даними Організації з безпеки та співробітництва в Європі, «хоча докази з чужих слів, як правило, неприпустимі в юрисдикціях загального права за відсутності особливих обставин, немає заборони на докази з чужих слів у юрисдикціях цивільного права або в міжнародних трибуналах». Див. Організація з безпеки та співробітництва в Європі, Місія в Боснії та Герцеговині, Посібник з розслідування військових злочинів, злочинів проти людяності та геноциду в Боснії та Герцеговині (Сараєво, 2013 рік), стор. 26. Доступно на сторінці www.osce.org/bih/281491?download=true. Незважаючи на таку відсутність бар'єрів у юрисдикціях цивільного права та міжнародних трибуналах, як правило, докази з чуток розглядаються як особливо ненадійна категорія непрямих доказів, і судді часто надають їм відносно невелику вагу.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

надійності та допустимості як свідчення. Слідчі повинні знати, як кожна категорія доказів розглядається у відповідній юрисдикції. Документальні докази часто можуть бути допущені, навіть якщо автор не відомий або недоступний для дачі показань. Вони також можуть бути допустимими без необхідності представляти документ через свідка, який може його автентифікувати, за умови, що сторона, яка його пропонує, може чітко і конкретно продемонструвати, де і як цей документ вбудовується у справу.[86]

60. У ситуаціях, коли відповідальність за злочини та порушення покладається на тих, хто знаходиться вище у структурі управління, зібрана інформація може бути використана не лише для встановлення «бази злочинів» (див. нижче), але також може бути доречною для доведення способу відповідальності[87] передбачуваного окремого злочинця.[88] Особи можуть вважатися відповідальними, якщо кожен елемент злочину чи порушення, включаючи фізичні дії (actus reus) та психічний стан обвинуваченого (mens rea), продемонстрований відповідно до застосовного стандарту доказування. Для того, щоб визначити це, особа, яка здійснює перевірку фактів, вивчає інформацію, подану стосовно кожного елементу порушення чи злочину. Слідчі повинні знати, які злочини чи порушення можуть бути заявлені, ознаки кожного, кого звинувачують у їх скоєнні та за якою теорією відповідальності. У справах міжнародного кримінального права практики часто відокремлюють «докази на основі злочину» від «доказів взаємозв'язку». Ці два поняття пояснюються так:

(a) Докази на основі злочину – це докази злочинів, на яких ґрунтуються звинувачення, включаючи інформацію про те, хто, що, де і коли.[89] Наприклад, якщо підозрюваного злочинця звинувачують у вбивстві як злочині проти людяності, будь-яка інформація, що підтверджує факт вбивства, вважається доказом на основі злочину;

---

[86] Див., наприклад, Міжнародний трибунал у справах колишньої Югославії, Прокурор проти Павла Стругара (Pavle Strugar), справа № IT-01-42-T, Рішення про прийнятність деяких документів, 26 травня 2004 року, Судова палата II та Прокурор проти Мілана Мілютіновича (Milan Milutinovic) та ін., справа № IT-05-87-T, Рішення за клопотанням обвинувачення про прийняття документальних доказів, 10 жовтня 2006 року, Судова палата; Міжнародний кримінальний трибунал по Руанді, Прокурор проти Едуарда Каремери (Milan Milutinovic) та інших, справа № ICTR-98-44-T, Рішення за клопотанням Джозефа Нзірорери (Milan Milutinovic) про прийняття документів до суду від адвокатури: Публічні заяви та протоколи, 14 квітня 2009 року, Судова палата III; Міжнародний кримінальний суд, Прокурор проти Томаса Лубанга Дійло (Thomas Lubanga Dyilo), справа № ICC-01/04/-01/06, Рішення про допуск матеріалів за «адвокатури», 24 червня 2009 року; Міжнародний трибунал у справах колишньої Югославії, Прокурор проти Радована Караджича (Radovan Karadzic), справа № IT-95-5/18-PT, Наказ про клопотання прокуратури про роз'яснення та пропозицію щодо Настанов щодо ведення судового розгляду, 20 жовтня 2009 року, Судова палата та Прокурор проти Радована Караджича (Radovan Karadzic), справа № IT-95-5/18-T, Рішення за першим клопотанням обвинувачення, 13 квітня 2010 року, Судова палата; Міжнародний кримінальний суд, Прокурор проти Жермена Катанги (Germain Katanga) та Матьє Нгуджоло Чуї (Mathieu Ngudjolo Chui), справа № ICC-01/04-01/07, Рішення щодо клопотань прокурора, що подають на суд, 17 грудня 2010 року, Судова палата II.

[87] Крієр (Cryer), Робінсон (Robinson) та Васильєв (Vasiliev), Вступ до міжнародного кримінального права та процесу, глава 15.

[88] Див. УВКПЛ, Хто відповідальний? Приписування індивідуальної відповідальності за порушення міжнародних прав людини та гуманітарного права у слідчих комісіях ООН, місіях з встановлення фактів та інших розслідуваннях (Нью-Йорк та Женева, 2018 рік). Доступно на сторінці https://ohchr.org/Documents/Publications/AttributingIndividualResponsibility.pdf.

[89] Келлі Матесон (Kelly Matheson), Посібник «Відео як доказове поле» (WITNESS, 2016 рік), стор. 42. Доступно на сторінці https://vae.witness.org/video-as-evidence-field-guide.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(b) Докази взаємозв'язку є доказами відповідальності передбачуваного виконавця за вчинені злочини, що є особливо важливим, якщо злочинець не вчинив злочин безпосередньо.[90] Іншими словами, це докази, які пов'язують відповідальну сторону зі злочином. Наприклад, у випадках, коли стверджується, що начальник не в силах запобігти або покарати передбачувані порушення, про які вони знали, доказом взаємозв'язку є те, що доводить це усвідомлення чи той факт, що начальник мав «ефективний контроль» над безпосереднім злочинцем.

E. Право на недоторканість приватного життя і захист даних

61. Право на недоторканість приватного життя є основним правом людини. [91] Важливим елементом права на недоторканість приватного життя є право на захист персональних даних, яке було сформульоване у різних законах про захист даних.[92] Зокрема, закони про захист даних та недоторканість приватного життя стають все більш актуальними у розслідуваннях, які використовують цифрову інформаційно-комунікаційну технологію (ІКТ). Нижче наведено короткий огляд концепцій міжнародного права людини на недоторканість приватного життя та глобальних меж захисту даних, безпеки даних та обміну даними, про що слід знати слідчим, що ведуть розслідування з використанням даних у відкритому доступі. У цифровому середовищі особливе значення набуває інформаційна конфіденційність, яка охоплює інформацію, яка існує або може бути отримана про людину.[93]

62. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні поважати права людини і повинні бути особливо чутливими до права на недоторканість приватного життя, яке часто піднімається в контексті цифрової інформації. Наприклад, порушення права на приватне життя є однією з небагатьох підстав, за якими судді можуть виключити докази в Міжнародному кримінальному суді.[94] Недоторканість приватного життя лежить в основі та захищає людську гідність та інші ключові цінності, такі як свобода асоціацій та свобода вираження поглядів. Європейський суд з прав людини надає деякі з найсильніших тлумачень законів про недоторканість приватного життя із

---

[90] З того самого джерела.

[91] Право на недоторканість приватного життя включено до численних документів з прав людини та до конституційних статутів більш ніж 130 країн. Див., гаприклад, Американську декларацію прав та обов'язків людини, стаття V; Європейська конвенція з прав людини, стаття 8; Американська конвенція з прав людини, стаття 11; Конвенція про права дитини, стаття 16; Міжнародна конвенція про захист прав усіх трудящих-мігрантів та членів їх сімей, стаття 14; Африканська хартія про права та добробут дитини, стаття 10; Арабська хартія прав людини, стаття 16 і 21; Декларація прав людини Асоціації країн Південно-Східної Азії, стаття 21. Див. також Privacy International, «Що таке недоторканість приватного життя?», 23 жовтня 2017 року. Доступно на сторінці https://privacyinternational.org/explainer/56/what-privacy.

[92] Існують закони про захист даних у більш ніж 100 країнах та у численних міжнародних та регіональних документах. Див., наприклад, Організація економічного співробітництва та розвитку, Вказівки щодо захисту конфіденційності та транскордонних потоків персональних даних; Рада Європи, Конвенція про захист осіб щодо автоматичної обробки персональних даних; Хартія основних прав Європейського Союзу; Рамки конфіденційності Азіатсько-Тихоокеанського економічного співробітництва; Додатковий акт про захист персональних даних в рамках Економічної спільноти держав Західної Африки.

[93] Див., загалом, A/HRC/39/29, пункт 5.

[94] Див. Римський статут, стаття 69 (7).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

швидко зростаючим набором судової практики, що стосується питань цифрових прав. Порушення таких основних прав неминуче призведе до оскарження захистом у кримінальному провадженні і навіть може призвести до цивільних причин позову проти слідчих сторін. Окрім законів про недоторканість приватного життя, численні закони та нормативні акти щодо захисту даних допомагають забезпечити безпеку персональних даних. Зокрема, слідчим, що ведуть розслідування з використанням даних у відкритому доступі, слід знати про Регламент Європейського Парламенту та Ради 2016/679 від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЕС (Генеральний регламент про захист персональних даних), та його підхід до захисту індивідуальних даних, оскільки цей закон встановив високі стандарти, а інші держави розглядають можливість прийняття подібного законодавства.[95] Однак правила захисту даних відрізняються від країни до країни зі значними відмінностями і навіть іноді прямо суперечливими правилами. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні проконсультуватися з юристом, щоб ознайомитись із чинним законодавством та нормативними актами щодо захисту даних, що стосуються юрисдикцій, у яких вони діють.

63. Нарешті, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати про загальну заборону несанкціонованого доступу до даних та мереж. Наприклад, це включатиме використання просоченого пароля, знайденого в наборі даних, що порушується, для доступу до обмежених матеріалів, а також отримання несанкціонованого доступу до обмеженої інформації за допомогою обману та інших форм соціальної інженерії.[96]

F. Інші відповідні правові міркування

64. У ході розслідувань з використанням даних у відкритому доступі можуть мати значення інші закони. Нижче наведено невичерпний перелік деяких юридичних міркувань, про які слідчим, що ведуть розслідування з використанням даних у відкритому доступі, слід знати.

1. Порушення умов надання послуг

---

[95] У Регламенті зазначено, що фізичні особи мають права, пов'язані із захистом персональних даних, захистом обробки персональних даних та необмеженим переміщенням персональних даних у межах Європейського Союзу. Подібні права також передбачені Конвенцією про захист осіб щодо автоматичної обробки персональних даних і, зокрема, Протоколом до неї до 2018 року. Конвенція пов'язує не тільки держави-члени Ради Європи, а й низку інших держав.

[96] За даними Національного інституту стандартів і технологій Сполучених Штатів, соціальна інженерія – це «акт обману окремої особи для розкриття конфіденційної інформації шляхом спілкування з нею для завоювання впевненості та довіри» (Пол А. Грассі (Paul A. Grassi), Майкл Е. Гарсія (Michael E. Garcia) та Джеймс Л. Фентон (James L. Fenton), Настанови щодо цифрової ідентичності (Gaithersburg, Меріленд, Національний інститут стандартів і технологій, 2017 рік), стор.54. Див. Також Майкл Уоркман (Michael Workman), «Отримання доступу за допомогою соціальної інженерії: емпіричне дослідження загрози», Безпека інформаційних систем, том 16, № 6 (2007 рік). Для подальшого обговорення несанкціонованого та оманливого доступу див. пункт 65 нижче. Для обговорення маскування користувача див. пункт 107 нижче.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

65. Деякі поширені методи розслідування з використанням даних у відкритому доступі передбачають порушення умов користувацької угоди щодо веб-сайту або платформи. Наприклад, скрейпінг даних або використання віртуальної особистості (а не справжньої особистості) порушує умови користувацької угоди платформ і, зокрема, платформ соціальних медіа.[97] Порушення умов користувацької угоди – це порушення договору. Слідчі повинні перевірити, чи це також може бути незаконним діянням у юрисдикціях, у яких вони працюють. Необхідність дотримуватись принципів безпеки, які можуть бути забезпечені шляхом використання віртуальних особистостей, повинна бути збалансована з потенційною шкодою за порушення договору за таких обставин, найпоширенішим засобом захисту яких є відключення доступу користувача до платформи. Однак, хоча віртуальні особистості необхідні, коли вони використовуються для пошуку та моніторингу з використанням даних у відкритому доступі, як зазначено вище, віртуальні особистості не слід використовувати для спроб доступу до контенту, поширеного в соціальних мережах, що підлягає обмежувальному контролю доступу; або як привід для отримання інформації безпосередньо від особи під прикриттям неправдивої особистості. Така поведінка виводить слідчих за межі розслідування з використанням даних у відкритому доступі, порушує етичні принципи[98] та може порушувати закон.[99]

2. Закони про інтелектуальну власність

66. Слідчим слід знати про будь-які дозволи на інтелектуальну власність, які їм можуть знадобитися для законного опублікування, розповсюдження та/або іншого використання інформації, яку вони зібрали під час розслідування. Відповідні закони варіюються від юрисдикції до юрисдикції, хоча більшість юрисдикцій передбачають (як мінімум) певну форму захисту авторських прав для творця контенту, наприклад, відео, фотографії або фрагменту тексту, опублікованого в Інтернеті. «Творець» зазвичай визначається як особа, яка насправді створила матеріал

- наприклад, зробивши знімок, записавши відео або написавши оригінальний текст – а не завантажувач, хоча це може бути одна і та сама особа. Кінцевому користувачу може знадобитися отримати згоду автора на запропоноване використання, щоб уникнути порушення авторських прав (наприклад, якщо використовувати контент у публічному звіті або журналістському сюжеті)
- отримання згоди завантажувача, якщо ця особа не є також автором, зазвичай недостатньо, щоб уникнути порушення закону. Це ще одна причина для спроби знайти першоджерело кожного матеріалу, який слідчі можуть придбати. Деякі (але не всі) юрисдикції передбачають винятки з необхідності отримання згоди – їх часто називають винятками щодо «добросовісного використання»

---

[97] Наприклад, Умови використання Facebook вимагають від користувачів «використовувати те саме ім'я, яке ви використовуєте у повсякденному житті», «надавати точну інформацію про себе» та «створити лише один обліковий запис (власний) та використовувати свою хронологію в особистих цілях». Див. www.facebook.com/terms.php. Видавання себе за іншу особу порушує Правила та політику Twitter. Див. «Політика видавання себе за іншу особу» на веб-сторінці https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy.

[98] Обговорення надання недостовірної інформації див. у главі II.C вище про етичні принципи.

[99] Див. главу III.E вище про право на недоторканість приватного життя та захист даних.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

або «торгової чесності» – коли відео, фотографії, текст та інша інформація використовуються для певних суспільно корисних цілей, таких як освіта, правоохоронні органи чи журналістика. Однак ці винятки, за наявності, часто є досить вузькими, і тому ніколи не слід вважати, що конкретне використання підпадає під такий виняток без ретельного огляду. Механізми, які іноді можуть допомогти мінімізувати ймовірність та/або масштаби порушення, включають вбудовування посилання на оригінальний контент у цифровий звіт без видалення його з першоджерела; висловлення подяки творцю; і використання лише невеликої частини оригінального контенту – однак, знову ж таки, це залежить від контексту та юрисдикції. Інформація, на яку поширюються ліцензії Creative Commons або інші безкоштовні ліцензії, може мати широкий спектр дозволеного безкоштовного використання. Однак, якщо такі безкоштовні ліцензії застосовуються, важливо дотримуватися умов ліцензії та не розглядати контент як такий, для використання якого не вимагаються дозволи.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

IV

БЕЗПЕКА

РЕЗЮМЕ ГЛАВИ

- Кожен несе відповідальність за забезпечення безпеки розслідування та тих, на кого воно впливає, а не лише фахівці з інформаційних технологій.

- Міркування безпеки мають бути подвійними: (a) пов'язані з інфраструктурою, включаючи апаратне забезпечення, програмне забезпечення та мережі; і (b) пов'язані з поведінкою, включаючи поведінку слідчих та всіх тих, з ким вони спілкуються.

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

- Заходи захисту повинні бути розроблені для зменшення ризиків та загроз, як це визначено в оцінці ризику розслідування.

- Оцінки безпеки повинні враховувати всі види шкоди, включаючи цифрову, фінансову, юридичну, фізичну, психосоціальну та репутаційну шкоду.

- Деякі з найбільших уразливостей у розслідуваннях з використанням даних у відкритому доступі пов'язані з Інтернет-з'єднаннями/IP-адресами, пристроями та їх функціями, а також поведінкою користувачів.

- Слідчі та слідчі організації повинні брати участь у постійному навчанні з питань безпеки та застосовувати заходи захисту, які розвиваються із зміною характеру будь-яких загроз чи уразливостей.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

67. У цій главі міститься огляд онлайн- та офлайн-міркувань безпеки, пов'язаних із розслідуваннями, що проводяться з використанням даних у відкритому доступі. Завдяки належній підготовці, інвестиціям та зосередженню на оцінці загрози та зменшенні ризиків слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні мати можливість мінімізувати ризик заподіяння шкоди людям, даним та іншим активам. Інфраструктуру безпеки, включаючи апаратне та програмне забезпечення, та протоколи поведінки користувачів слід, наскільки це можливо, запровадити до початку розслідування, регулярно оцінювати та оновлювати за необхідності. Розмір та ресурси організації можуть вплинути на здійснення певних заходів захисту; тому ця глава містить гнучкі стандарти, які слід адаптувати відповідно до конкретних потреб організації та розслідування. Організації, які проводять розслідування з високим ризиком – наприклад, розслідування щодо особливо вразливих жертв або в ситуаціях, коли передбачувані злочинці є державними суб'єктами та/або ідентифіковані окремо – повинні залучати послуги досвідчених фахівців із кібербезпеки. Крім того, надійна система безпеки повинна включати якийсь незалежний механізм аудиту та постійне навчання, щоб користувачі могли бути в курсі нових технологічних досягнень та передової практики.

A. Мінімальні стандарти

68. Оскільки інфраструктура безпеки та передова практика поведінки користувачів постійно змінюються, Протокол пропонує всеосяжні принципи, які допоможуть надавати керівництво слідчим, які ведуть розслідування з використанням даних у відкритому доступі, щодо продумування безпеки. Слідчі повинні нести відповідальність за власну безпеку, включаючи оцінку рівня ризику, пов'язаного з їхньою поведінкою, та вжиття відповідних заходів щодо зменшення ризиків та захисту. Незважаючи на необхідність спеціального та індивідуалізованого підходу до безпеки, існують деякі мінімальні стандарти, які слідчі, що ведуть розслідування з використанням даних у відкритому доступі, завжди повинні застосовувати до своєї роботи для дотримання принципів безпеки:

(a) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні уникати розкриття ідентифікованих елементів про себе, свої організації та будь-яких партнерів чи джерела третім сторонам, якщо це не є метою розслідування або зобов'язанням. Тому слідчі повинні зберігати свою анонімність в Інтернеті та стежити за тим, щоб їх діяльність в Інтернеті не була віднесена до них, наскільки це можливо;

(b) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні проводити діяльність в Інтернеті з розрахунком на те, що така діяльність може контролюватися та аналізуватися третіми сторонами. Тому вони повинні вести діяльність в Інтернеті таким чином, щоб це відповідало їхнім віртуальним особам і таким чином, що не розкриває їх особи та цілі розслідування, або загрожує їхнім людським джерелам чи іншим третім сторонам;

(c) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати, що надмірне використання єдиного онлайн-джерела інформації, такого як певний сайт, може збільшити ризик моніторингу та аналізу сторонніх виробників. Тому їм

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

слід запровадити практику мінімізації цієї ймовірності, наприклад, урізноманітнення цифрових джерел;

(d) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні уникати ідентифікованих або передбачуваних моделей поведінки, таких як повторювані шаблони пошуку на пристроях, що ідентифікуються, що може допомогти третій стороні визначити цілі розслідування, а також спростити слідчим цілі для фішингових атак та інших форми соціальної інженерії;[100]

(e) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розмежовувавати свою професійну роботу та особисту діяльність в Інтернеті. Особисті облікові записи в мережі та, наскільки це можливо, особисте обладнання не повинні використовуватися для професійних розслідувань, а професійне обладнання ніколи не повинно використовуватися для особистої діяльності в Інтернеті;[101]

(f) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, які проводять численні розслідування, не повинні змішувати свої розслідування. Тому вони повинні фіксувати різні часи початку та закінчення кожного розслідування, зберігати дані та документацію для кожного розслідування в окремих місцях та використовувати різні віртуальні особистості, якщо це необхідно;[102]

(g) Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні використовувати технічні системи чи середовища, які піддаються мінімальному впливу можливого впровадження агресивного чи шкідливого програмного забезпечення чи іншим руйнівним впливам, які можуть виникнути під час діяльності.

B. Оцінки безпеки

69. Для того, щоб розробити відповідну та ефективну систему безпеки, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розуміти ключові концепції кібербезпеки та управління ризиками. Вони також повинні мати можливість ідентифікувати активи, які потребують захисту, та потенційну шкоду, та оцінити потенційні загрози, ризики та вразливості.

70. Ризик – це потенціал втрати, пошкодження або знищення активу в результаті загрози з використанням вразливості. Кожен з цих термінів визначено нижче. Оскільки розслідування з використанням даних у відкритому доступі, що проводяться в Інтернеті, включають різні методи збору інформації до традиційних розслідувань, вони породжують різні види ризиків. Виявлення та оцінка цих ризиків є важливою частиною планування та підготовки розслідування. Деякі приклади поширених ризиків у розслідуваннях з

---

[100] Нижче наведено пояснення щодо фішингових атак та соціальної інженерії.

[101] Якщо використання особистого обладнання неминуче, користувачам слід проводити професійні розслідування та особисту діяльність в окремих онлайн-середовищах, наприклад за допомогою віртуальної машини для своїх досліджень.

[102] На додаток до мінімізації ризику заплутати розслідування, така практика допоможе ефективно зберегти ланцюг забезпечення збереження.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

використанням даних у відкритому доступі включають: технологічні можливості та обізнаність щодо цілі розслідування, або суб'єктів, що підтримують ціль, які могли б ухилитися від розслідування або ввести в оману; проблеми в технічній конфігурації інтернет-середовища, що використовується для розслідування, що може призвести до розкриття інформації, яка може поставити під загрозу розслідування; шкідливе програмне забезпечення або код, які можуть поставити під загрозу комп'ютерні системи, діяльність, особистість або зібрані дані слідчого; або технічні функції, такі як трекери, файли cookie, маячки та аналітика, які можуть поставити під загрозу слідчу діяльність.

71. Нижчевикладений розділ містить пояснення ключових термінів та їх застосування до розслідувань з використанням даних у відкритому доступі, таким чином надаючи дорожню карту для проведення оцінки загрози та ризику.

1. Активи

72. Актив – це все, що потребує захисту, включаючи людей,[103] майно та інформацію. У контексті розслідувань з використанням даних у відкритому доступі, особи, які потребують захисту, можуть включати слідчих або слідчі групи, включаючи всіх, з ким працюють слідчі або слідчі групи (тобто внутрішні колеги та зовнішні партнери, як місцеві, так і ті, хто працює у цій галузі), автори чи джерела інформація, свідки, жертви, передбачувані злочинці та сторонні особи. Майно складається з матеріальних та нематеріальних об'єктів, яким можна присвоїти вартість.[104] До матеріальних активів належать будівлі, обладнання та документи, тоді як до нематеріальних активів належать репутація та власність, такі як цифрові дані, метадані, бази даних, код програмного забезпечення та записи.

2. Шкода

73. Шкода – це фізичне або психічне пошкодження майна або його знищення. Сюди може входити цифрова, фінансова, юридична, фізична, психосоціальна чи репутаційна шкода.

(a) Цифрова шкода

74. Цифрова шкода – це пошкодження будь-якої цифрової інформації чи інфраструктури. Потенційна цифрова шкода може включати знищення, маніпуляції або втрату доступу до даних або порушення роботи сервісів з комп'ютерних систем та платформ.

(b) Фінансова шкода

75. Фінансова шкода може виникнути з ряду джерел, включаючи юридичну та репутаційну шкоду, пов'язану з розслідуванням. Слідчі, цілі та сторонні особи можуть

---

[103] Посилання на людей як на активи здійснюється лише в контексті проведення оцінок безпеки.
[104] Див. Група аналізу загроз, «Загроза, уразливість, ризик – загально заплутані терміни». Доступно на сторінці www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

відчути таку шкоду. Крім того, фінансовий збиток може виникнути, коли слідчі не зможуть належним чином оцінити довгострокові витрати на розслідування.

(c) Юридична шкода

76. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, можуть брати на себе юридичну відповідальність як за процес, так і за результати своєї роботи. Слідчі повинні знати про юридичні обмеження щодо того, що їм дозволяється робити, та юридичні наслідки своїх дій, щоб мінімізувати ризик юридичної відповідальності для себе та/або третіх сторін. Розслідування також може завдати юридичної шкоди суб'єктам таких розслідувань і навіть стороннім особам, які можуть бути причетні до правопорушень, виявлених під час розслідування.[105]

(d) Фізична шкода

77. До фізичної шкоди можна віднести пошкодження людей або майна. Хоча слідчі, що ведуть розслідування з використанням даних у відкритому доступі, зазвичай працюють з офісу чи будинку, а не перебувають на місці, фізичну шкоду все ж слід оцінювати як потенційний наслідок діяльності в Інтернеті. Дії в кіберпросторі можуть призвести до реальних наслідків, про які слідчим слід знати і до яких вони повинні бути готові. Наприклад, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати про тих осіб – чи то колеги, онлайн-користувачі в ситуаційних країнах чи інші – які можуть перебувати в небезпечному середовищі та під загрозою отримати фізичні ушкодження внаслідок поведінки слідчого в мережі. Інтернет-слідчі мають етичний – а в деяких випадках і юридичний – обов'язок піклуватися про інших,[106] щоб гарантувати, що ті, кому загрожує фізичне пошкодження, не піддаються більшій небезпеці через їх діяльність. Фізичні ризики слід розглядати як частину всебічної оцінки загрози перед початком роботи та повторно оцінювати протягом усього життєвого циклу розслідування.

(e) Психосоціальна шкода

78. Психосоціальна шкода може варіюватися від психологічного дистресу до травми і може вплинути на будь-якого члена слідчої групи та/або осіб, які інакше беруть участь у розслідуванні або на яких воно впливає, включаючи суб'єктів розслідування та сторонніх осіб. Окрім морально-етичної важливості захисту себе та інших від психологічної шкоди, люди іноді можуть бути найвразливішою ланкою ефективного функціонування будь-якої організації. Психосоціальна шкода, що зазнає людини, може бути особливо вразливою, що створює нові можливості для суб'єктів загрози для використання або інших ризиків для фізичної та цифрової безпеки, особливо якщо негативні психологічні наслідки призводять до погіршення функціонування, наприклад, слабшого, ніж зазвичай, дотримання протоколів безпеки. Відомо, що перегляд великої кількості насильницьких та інших образних відеороликів є особливо складним для обробки та може спричинити психологічний дистрес або травму, що може потребувати професійної підтримки. Ознаки

---

[105] Див. також глави IV.E та IV.F вище щодо подальшого обговорення відповідних правових міркувань.
[106] Римський статут, стаття 54 (1) (b).

вторинної травми можуть включати зміни в поведінці, зміну настрою, зміну звички прийому їжі або пиття, неможливість заснути, бажання спати більше, ніж зазвичай, або кошмари.[107] Стратегії пом'якшення психосоціальної шкоди описані в розділі про підготовку та створення плану стійкості та турботу про себе.[108]

(f) Репутаційна шкода

79. Репутаційна шкода в контексті розслідувань з використанням даних у відкритому доступі може бути найбільш гострою для слідчих, що ведуть розслідування з використанням даних у відкритому доступі, та/або їх організацій, наприклад, якщо слідчі публікують помилкову інформацію, порушують етику чи іншим чином створюють проблемний контент. Репутаційна шкода також може бути завдана суб'єктам розслідування, які можуть зіткнутися зі стигмою за свою передбачувану поведінку, коли таку поведінку буде оприлюднено. Це може бути особливою проблемою, якщо обвинувачення висуваються особам чи організаціям, які згодом виявляються неправдивими.

3. Захисні заходи

80. Захисні заходи – це зусилля, спрямовані на запобігання або мінімізацію вразливостей, і можуть включати фізичні, технологічні та політичні заходи. Фізичний захист може включати замки на будівлях, кімнатах або шафах, у яких зберігається чутливий матеріал. Технологічні заходи можуть включати використання паролів, шифрування та багатофакторну автентифікацію на пристроях або контроль доступу до систем даних. Політичні заходи включають внутрішні та зовнішні правила, закони та механізми застосування, такі як правила проти надсилання внутрішнього робочого продукту з робочого листа на особистий електронний лист або політики проти використання особистих облікових записів у соціальних мережах на своєму робочому комп'ютері.

4. Загрози

81. Загрози – це те, від чого активи повинні бути захищені. Загроза – це все, що може навмисно чи випадково використати вразливість та отримати, пошкодити або знищити

---

[107] Див. Dart Center for Journalism and Trauma, «Робота з травматичними образами», 12 серпня 2014 року (доступно за посиланням https://dartcenter.org/content/working-with-traumatic-imagery); Сем Дабберлі (Sam Dubberley), Елізабет Гріффін (Elizabeth Griffin) та Халук Мерт Баль (Haluk Mert Bal), Вторинна травма як основна проблема: Дослідження травм медіа-очевидців та вікарних травм на цифровій передовій (Eyewitness Media Hub, 2015 рік) (доступно за посиланням http://eyewitnessmediahub.com/research/vicarious-trauma); Сем Дабберлі (Sam Dubberley) та Мішель Грант (Michele Grant), «Журналістика та вікарна травма: посібник для журналістів, редакторів та інформаційних організацій» (First Draft News, 2017 рік) (доступно за посиланням https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf); Центр з прав людини та глобальної справедливості, «Проект захисту прав людини відкриває новий веб-сайт», 21 травня 2018 року (доступно за посиланням https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website); Керамет Райтер (Keramet Reiter) та Алекса Кеніг (Alexa Koenig), «Райтер та Кеніг про виклики та стратегії дослідження травм», Palgrave MacMillan (доступно за посиланням www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

[108] Див. главу V.D нижче для отримання додаткової інформації про турботу про себе.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

актив. Загрози можуть бути внутрішніми або зовнішніми для організації чи розслідування та можуть виконуватися окремими особами, групами, установами чи мережами. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати про такі загрози, серед іншого.

(a) Поширені атаки типу «відмова в обслуговуванні»

82. Поширені атаки типу «відмова в обслуговуванні» – це кібератаки, покликані порушити можливість цілі отримати доступ до машини або мережі. Слід запровадити систему пом'якшення таких атак для публічних активів, таких як веб-сайти та інші портали віддаленого доступу. Крім того, слід запровадити систему реєстрації інцидентів і використовувати її у разі нападу для запису всіх дій та відповідних суб'єктів.

(b) Фішингові атаки

83. Фішинг – це шахрайська спроба отримати конфіденційну інформацію, таку як імена користувачів, паролі та дані кредитної картки, прикидаючись надійною особою в електронному спілкуванні.[109] Фішинг або телефонні афери використовуються для отримання конфіденційної інформації або для переслідування слідчих. Особисті облікові записи, як правило, піддаються більшому ризику, ніж професійні; таким чином, їх використання може поставити під загрозу дослідження або продукт роботи.

(c) Атаки через посередника

84. Атаки через посередника – це тип кібератаки, в якій зловмисники вмикаються у розмови між двома сторонами, видають себе за обидві сторони та отримують доступ до інформації, яку обидві сторони намагалися надіслати одна одній.[110] Атака через посередника дозволяє зловмиснику перехоплювати, надсилати та отримувати дані, призначені для когось іншого, або взагалі не призначені для надсилання, не знаючи жодної сторони, поки не буде надто пізно.[111]

(d) Соціальна інженерія

85. Соціальна інженерія – це психологічна маніпуляція людьми, щоб змусити їх виконати потенційно шкідливі дії, такі як розкриття конфіденційної інформації. Існує багато різних прикладів соціальної інженерії, таких як цільовий фішинг.[112] Оскільки тактика соціальної інженерії продовжує адаптуватися та розвиватися, слідчі повинні брати участь у постійному навчанні щодо виявлення та уникнення визначених тактик соціальної інженерії.

---

[109] Див. Phishing.org, «Що таке фішинг?». Доступно на сторінці www.phishing.org/what-is-phishing.
[110] Див. Veracode, «Атака через посередника (MITM)». Доступно на сторінці www.veracode.com/security/man-middle-attack.
[111] З того самого джерела.
[112] Цільовий фішинг – це шахрайська практика надсилання електронних листів нібито від відомого або надійного відправника з метою спонукати цільових осіб розкривати конфіденційну інформацію.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(e) Шкідливе програмне забезпечення

86. Шкідливе програмне забезпечення означає комп'ютерні програми, призначені для проникнення і пошкодження комп'ютерів без згоди користувача. Існує кілька типів шкідливих програм, включаючи шпигунські програми та програми-вимагачі.

5. Суб'єкти загрози

87. Суб'єкт загрози чи зловмисний суб'єкт – це особа або організація, яка несе відповідальність за подію чи інцидент, що має вплив або може мати вплив на безпеку чи захист іншої організації чи суб'єкта. У міжнародних кримінальних розслідуваннях та розслідуваннях у сфері прав людини суб'єктами загрози, ймовірно, є передбачувані злочинці, об'єкти розслідування, включаючи уряди чи їх прихильників. Для слідчих, що ведуть розслідування з використанням відкритих даних, важливо виявити потенційних суб'єктів загрози та зрозуміти їх можливості та ймовірність здійснення ними атак.

6. Уразливості

88. Уразливість – це слабкість або розрив у захисних заходах, які можуть існувати як у цифровій, так і у фізичній сфері. Що стосується діяльності в Інтернеті, то вразливі місця можуть включати слабкість заходів безпеки, які можна використати для отримання несанкціонованого доступу до активу, дефекти безпеки програмного забезпечення, небезпечний проект та надпривілейовані користувачі та код. В автономному режимі вони також можуть включати слабкі місця людей, таких як член команди, який схильний до шантажу чи примусу, або який може стати вразливим внаслідок надмірного впливу графічних матеріалів або внаслідок інших складних умов праці.[113] Нові вразливі місця можуть бути створені шляхом виявлення того, що розслідування триває до цілі, або виявлення обсягу розслідування. Нарешті, вразливі місця безпеки можуть виникати через зовнішні загрози, такі як нові шкідливі програми та віруси, про що слідчим слід знати. Картографування безпеки та оцінка ризиків повинні враховувати такі види вразливостей.

89. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, також повинні знати про такі вразливі місця в Інтернеті.

(a) Файли cookies

90. Файл cookie – це невеликий файл, який часто надсилається через веб-сайт та зберігається або в пам'яті комп'ютера користувача, або записується на диск комп'ютера для використання браузером. Файли cookie часто необхідні для правильного функціонування веб-сайту – наприклад, пропонуючи можливість зберігати налаштування веб-сайту та дані особи, щоб уникнути необхідності повторного введення даних під час наступних відвідувань. Файли cookie були розроблені таким чином, щоб вони могли збирати та зберігати значні – часто конфіденційні – дані про відвідувачів та їх відвідування. Деякі з них перетворилися на централізовані інструменти, які можна використовувати для збору

---

[113] Див. главу V.D нижче для отримання додаткової інформації про стійкість та турботу про себе.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

даних, щоб створити уявлення про інтереси та звички перегляду користувачів. Файл cookie може бути присутнім на комп'ютері до моменту його закінчення або видалення користувачем.

(b) Трекери

91. Трекер – це тип файлів cookie, який використовує здатність веб-браузера зберігати дані про те, які веб-сторінки були відвідані, які критерії пошуку введені тощо. У своїй найпростішій формі трекери призначають унікальний ідентифікатор веб-браузеру користувача, а потім пов'язують цей ідентифікатор із усіма подальшими переглядами та пошуковою діяльністю (критерії пошуку, відвідані сторінки, послідовність відвідуваних сторінок тощо). Це надає власнику трекера можливість зв'язати попередні та наступні відвідування веб-сайту (або набору афілійованих веб-сайтів) разом, щоб створити детальну картину користувачів та їхніх звичок перегляду. Трекери часто вбудовуються в рекламу, яка потім розповсюджується на кількох веб-сайтах, пропонуючи трекеру набагато більші шанси зафіксувати активність та поведінку користувачів. Навіть відвідування «надійного» веб-сайту може призвести до встановлення трекерів на комп'ютерах користувачів та до їх подальшої діяльності в Інтернеті.

(c) Маячки

92. Маячок – це механізм відстеження активності та поведінки користувачів. Маячки зроблені з невеликого і ненав'язливого (часто непомітного) елемента на веб-сторінці (щось таке маленьке, як один прозорий піксель), що, коли він відображається браузером, призводить до того, що подробиці про цей браузер та дочірній комп'ютер надсилаються третій стороні. Маячки можна використовувати разом з файлами cookie для ініціації збору та передачі даних, а також для однозначної ідентифікації користувачів та запису їхніх звичок перегляду. Маячки тісно пов'язані з сайтами соціальних медіа, де ідентифікація відносин та мереж є ключовими будівельними блоками для цих сайтів. Нарешті, маячки можна використовувати в електронній пошті на основі HTML для збору та звітування про особистість користувача та для доступу до будь-яких файлів cookie, які раніше зберігалися на цьому комп'ютері.

(d) Інші коди та сценарії

93. Все більша кількість веб-сайтів використовують невеликі фрагменти коду, завантажені веб-браузером відвідувача, які мають можливість зберігати інформацію про відвідування. Такий код може впливати на те, як веб-сайт виглядає, як веб-сайт реагує на вхідні дані та як браузер реагує на веб-сайт. Код також може зберігати конфіденційні дані, пов'язані з обліковими даними відвідувачів, діяльністю тощо. Збір даних може бути постійним і може надсилати дані третій стороні.

C. Міркування щодо інфраструктури

94. Інфраструктура відноситься до структур, засобів та систем, включаючи програмне та апаратне забезпечення, необхідних для проведення розслідувань з використанням даних

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

у відкритому доступі. Інфраструктура повинна забезпечувати (і бути оснащеною) достатніми засобами безпеки для захисту та збереження активів та даних організації. Для забезпечення стійкості інфраструктури повинні бути вжиті заходи щодо пом'якшення, щоб забезпечити безперервність у разі будь-чого з наступного:

(a) Зрив або втрата Інтернет-з'єднання;

(b) Порушення або втрата доступу до збережених даних;

(c) Втрата, пошкодження або знищення даних;

(d) Зрив або втрата програмного забезпечення;

(e) Пошкодження або втрата апаратного забезпечення;

(f) Несанкціонований доступ до пристроїв;

(g) Несанкціонований доступ до мережі;

(h) Випадкове видалення або маніпулювання даними;

(i) Навмисне знищення або маніпулювання даними;

(j) Витік даних або утримання даних «у заручниках».

95. Необхідна архітектура визначається масштабами слідчих заходів в Інтернеті, які мають бути проведені, характером розслідування та предметом інтересу, а також наявними фінансами для побудови, підтримки та модифікації інфраструктури, за необхідності.

1. Інфраструктура

96. Інфраструктура, що використовується для розслідувань з використанням даних у відкритому доступі, включатиме як мінімум наступні компоненти з додатковими функціями, що стосуються конкретних стратегій розслідування.

(a) Пристрої

97. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні мати обладнання для доступу до онлайн-контенту, таке як настільний комп'ютер, ноутбук, планшет або смартфон. Апартне забезпечення та обладнання мають бути захищені паролем, повинні мати включене повне шифрування та в ідеалі використовувати багатофакторну автентифікацію.[114] Дані з усього обладнання слід регулярно резервувати.

---

[114] Багатофакторна автентифікація – це покращення безпеки, яке вимагає від користувача представити два типи облікових даних для входу в обліковий запис, наприклад надання як пароля, так і біометричної (відбиток пальця) або смарт-картки. Див. США, Національний інститут стандартів і технологій, «Назад до основ:

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Коли апаратне забезпечення не використовується, воно має надійно зберігатися з обмеженням доступу для користувача та затвердженого персоналу. Особисте обладнання не слід використовувати для діяльності, пов'язаної з роботою. Подібним чином обладнання, пов'язане з розслідуванням, не слід використовувати для особистої діяльності через ризик пов'язування особистих соціальних медіа з віртуальними особистостями, створеними для цілей розслідування.[115]

(b) Інтернет-підключення

98. В ідеалі слідчі матимуть міцне, стабільне та приватне з'єднання з Інтернетом і повинні уникати використання загальнодоступного Wi-Fi. Хоча безкоштовний, публічний Wi-Fi – включаючи напівприватні мережі, наприклад, які надаються готелями чи Інтернет-кафе – пропонує зручний варіант, він дуже небезпечний і сприйнятливий до численних загроз, найбільша з яких – здатність хакерів позиціонувати себе між користувачем і точкою з'єднання. Використання особистої точки доступу, захищеної паролем, вимагає фінансових вкладень, але це має важливе значення для проведення безпечних розслідувань в Інтернеті. Крім того, хоча це не завжди під контролем слідчого, міцне та стабільне підключення до Інтернету є кращим як з точки зору функціональності, так і безпеки. При використанні віртуальної приватної мережі (VPN) на нестійкому з'єднанні слідчі повинні запровадити механізм захисту від збоїв, щоб гарантувати, що у разі розриву з'єднання їхня IP-адреса не буде виявлена.

(c) Веб-браузери

99. Одним з основних інструментів, що використовуються в онлайн-розслідуваннях, є веб-браузер, який використовується для запитів, пошуку та доступу до веб-сайтів, опублікованих в Інтернеті. Браузери виступають в якості основного інтерфейсу між слідчими та Інтернетом, проте їх часто не помічають як джерело ризику. Сучасні браузери постійно модифікуються і мають широкий спектр вбудованих функцій для задоволення безлічі вимог. Браузери також є ключовою мішенню для тих, хто хоче вести спостереження або розпочинати атаки проти супротивника, оскільки функціональні можливості можуть бути неправильно використані та відносно легко можна додати додаткові функції. Браузер має одночасний доступ до Інтернету та комп'ютера і, відповідно, потенційно ідентифікує інформацію про користувача. Витік даних через веб-браузер може розкрити достатньо даних, щоб попередити суб'єкта розслідування. Сучасні веб-браузери мають кілька вбудованих функцій і можуть мати додані численні додаткові функції, відомі як доповнення для браузера, які можуть поодиноко або разом вилучати дані, що призводить до ідентифікації розслідування, слідчого або рядку запитів та пов'язаної пошукової діяльності. Браузери також за замовчуванням мають можливість завантажувати та виконувати комп'ютерний код, отриманий із веб-сайту. Наявність та/або функціональність

багатофакторна автентифікація (МЗС)». Доступно на сторінці www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

[115] Цю рекомендацію може бути важко виконати під час подорожі, оскільки багато слідчих використовуватимуть свій робочий пристрій, але хочуть або потребують ведення особистого бізнесу поза робочим часом. Тому організації, які проводять розслідування з використанням даних у відкритому доступі, повинні розробити розумну політику щодо подорожей.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

комп'ютерного коду може не бути очевидною для слідчих, проте код може змінити наданий їм цифровий контент, отримати доступ до функціональних можливостей та даних на їхніх комп'ютерах і навіть змусити комп'ютери поводитися інакше, ніж передбачається. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні намагатися мінімізувати ці ризики, гарантуючи, що вони використовують безпечні, оновлені веб-браузери, які регулярно перевіряються, та використовуючи відповідне програмне забезпечення та встановлені плагіни, які пом'якшують деякі з описаних вище ризиків.[116]

2. Заходи безпеки

100. Ці основні елементи інфраструктури можна використовувати для ідентифікації користувачів та їх місцезнаходження. Для того, щоб дотримуватись принципу анонімності та недотримання авторства, слідчі повинні використовувати такі стратегії, щоб замаскувати свої Інтернет-з'єднання. Такі стратегії маскують місцезнаходження та IP-адресу та маскують машину, маскуючи її ідентифікаційні функції, операційну систему та браузер.

(a) Маскування підключення

101. IP-адреса може видавати інформацію, яка може бути використана для націлювання на інфраструктуру організації. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні прагнути використовувати VPN, проксі-сервери або інше програмне забезпечення для маскування IP-адрес своїх комп'ютерів, що означає, що IP-адреси, розкриті Інтернету, не пов'язані зі слідчими чи їх організаціями. VPN також створюють зашифрований канал для зв'язку між комп'ютером слідчого та сервером VPN, так що будь-які мережі/вузли, які проходять через з'єднання, бачитимуть лише зашифровані дані, що забезпечує додатковий рівень захисту. Однак використання певних мереж VPN заблоковано деякими країнами та веб-сайтами і може позначити слідчі дії як потенційно підозрілі для третіх сторін. В ідеалі VPN повинні дозволяти слідчим використовувати кілька IP-адрес з можливістю швидкого перемикання між ними, коли це необхідно. IP-адреси не повинні піддаватися відстеженню в одній країні, їй потрібно розділяти так, щоб вони відображали кілька місць у всьому світі.

(b) Маскування машини

102. Для того, щоб замаскувати певні функції, які можуть бути використані для ідентифікації користувачів, слідчі можуть використовувати віртуальні машини, які є програмними продуктами або операційними системами, які демонструють поведінку окремих комп'ютерів. Використання віртуальної машини по суті створить новий комп'ютер усередині комп'ютера – абсолютно окреме середовище від решти комп'ютерів. Віртуальна машина також здатна виконувати такі завдання, як запуск додатків і програм, як ніби це взагалі окремий комп'ютер,[117] змушуючи дослідника, який її використовує, з'являтися в Інтернеті як інший предмет. Під час використання віртуальної машини слідчі

---

[116] Щоб отримати найновіші вказівки щодо веб-браузері та інших заходів безпеки, див. Центр ресурсів з комп'ютерної безпеки Національного інституту стандартів і технологій США (https://csrc.nist.gov).

[117] Див. Techopedia, «Віртуальна машина (ВМ)», 21 травня 2020 року. Доступно на сторінці www.techopedia.com/definition/4805/virtual-machine-vm.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

мають систему для зміни веб-браузера, агента користувача, програмного забезпечення, відкритих портів, операційної системи та іншої інформації про машину, щоб з'являтися як інший суб'єкт кожного разу, коли вони виходять в Інтернет. В ідеалі, інфраструктура дозволила б слідчому використовувати віртуальну машину, яка маскує фактично використовувану машину. Віртуальні машини можуть бути знищені та відтворені, відновлені до попереднього пункту, налаштовані різними способами, тиражовані для нових справ або збережені для майбутніх потреб. Крім того, слідчі можуть скористатися більш обтяжливим, але також відносно ефективним підходом до зміни їх зовнішнього вигляду вручну, використовуючи різні веб-браузери кожного разу, коли вони виходять в Інтернет, змінюючи налаштування, щоб обмежити унікальність відбитків пальців своїх машин, і використовуючи плагіни, які перешкоджають відстеженню.

3. Інша інфраструктура

103. Перед початком роботи слідчі повинні розглянути іншу інфраструктуру для захисту своїх мереж та інфраструктури, включаючи такі системи:

(a) Системи резервного копіювання;

(b) Системи реєстрації для аудиту діяльності та відстеження дій користувачів;

(c) Окремі системи зберігання та відповідні місця зберігання для збору цифрових матеріалів, виявлених під час обшуків. Для того, щоб захистити дані ззовні, організації повинні мати платформи (наприклад, сховища доказів, бази даних чи інші системи управління інформацією), які зберігаються окремо від первинних мереж. Платформи повинні мати дві основні частини: одну підключену до Інтернету, а іншу відключену. У деяких випадках може бути доцільним якнайшвидше видалити дані з інфраструктури, підключеної до Інтернету, до більш безпечної мережі/сховища, щоб інформацію можна було безпечно переглянути.

D. Міркування щодо користувачів

104. Одним з найслабших місць будь-якої системи безпеки є користувач. Навіть за наявності ідеальної інфраструктури принципи безпеки не будуть дотримуватися без адаптації поведінки користувачів шляхом регулярного навчання та контролю. Безпека – це відповідальність кожного. Окремі особи не повинні займатися діяльністю, яка може поставити під загрозу дані або осіб без належного навчання щодо того, як зменшити ці ризики. Слідчих слід навчити оцінювати, яка поведінка є доцільною під час проведення різних видів діяльності в Інтернеті.

105. Анонімність може допомогти мінімізувати шкоду в ситуаціях, коли суб'єкт загрози намагається відстежити походження діяльності до мережі або користувача.[118] Будь-яка діяльність в Інтернеті вразлива для відстеження третіми сторонами; тому слідчі повинні

---

[118] Відстежити – це виявити точку походження будь-кого або будь-чого, відстежуючи інформацію чи низку подій.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

припускати таку загрозу під час проведення онлайн-діяльності. Найпоширеніші об'єкти відстеження включають IP-адреси, веб-браузери та роздільну здатність екрана (використовуються для ідентифікації обладнання), а також час навігації та активність на веб-сайтах (наприклад, введені терміни пошуку або відвідані сторінки). Суб'єкт загрози може спробувати визначити джерело онлайн-активності. Якщо відбувається спроба зворотного відстеження, суб'єкта загрози слід направити подалі від справжнього місцезнаходження чи особистості слідчого чи слідчої організації. Це можна зробити, вживши заходів для того, щоб Інтернет виглядав так, ніби доступ відбувається звідкись ще, через використання VPN, наприклад, або як інший, шляхом створення та використання віртуальних особистостей.[119]

106. Маскування зв'язку та машина, яка використовується в онлайн-розслідуванні, забезпечує важливий захист, але такий захист може бути підірваний, якщо користувачі розкриваються шляхом самоідентифікації на веб-сайті або, наприклад, за допомогою особистої інформації для реєстрації або входу на платформу соціальної мережі або до іншого приватного облікового запису. Слідчі ніколи не повинні використовувати свої особисті облікові записи для розслідування або входу до особистих облікових записів у веб-браузері, який використовується для розслідувань з використанням даних у відкритому доступі. Деякі облікові записи можуть вимагати використання фотографій, номерів телефонів або електронних листів під час створення. Ніколи не можна використовувати фотографії, телефони, електронні листи або дані, які є особистими або можуть бути пов'язані зі слідчими чи іншими особами.

Маскування користувача

107. Віртуальна особистість[120] – це неправдива онлайн-особистість або профіль, який може бути використаний для проведення безпечних слідчих заходів на платформах соціальних медіа та інших відкритих веб-платформах, які вимагають від користувачів входу для доступу до контенту. Це також може включати віртуальний обліковий запис або службу електронної пошти або обміну повідомленнями, базу даних, продукт або додаток, які використовують несправжню онлайн-особистість, а не справжню особистість. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні, з точки зору безпеки, створювати та використовувати віртуальні особистості для онлайн-розслідувань з використанням матеріалів у відкритому доступі. Це робиться для того, щоб гарантувати, що якщо суб'єкт загрози спробує простежити онлайн-діяльність цього профілю, він знайде послідовну та переконливу інформацію на основі віртуальної особистості, яка не розкриває реальної інформації про слідчого чи слідчу організацію чи інформацію про контент або спрямованість розслідування. Це також важливий захід безпеки для захисту тих, хто може підтримувати розслідування. Слід планувати віртуальні профілі та облікові записи,[121] а також заходи, що проводяться з їх використанням, слід вести облік інформації, яка використовується для створення облікових записів, а діяльність із використанням таких

---

[119] Обговорення віртуальних особистостей див. у главі IV.D вище про міркування, пов'язані з користувачами.

[120] Будь-яке використання віртуальних особистостей має збалансувати потребу в безпеці з етичним принципом прозорості. Див. главу II.C вище про етичні принципи.

[121] Див. главу V.C нижче про план онлайн-розслідування.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

облікових записів має реєструватися, щоб її можна було пояснити пізніше, за необхідності, наприклад, у суді.[122]

[122] Див. главу VI.D нижче щодо збереження.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

V

ПІДГОТОВКА

РЕЗЮМЕ ГЛАВИ

- Підготовка та стратегічне планування є ключем до ретельного та безпечного розслідування.

- Підготовка включає три процеси: (a) оцінка загроз та ризиків та розробка плану пом'якшення цих загроз та ризиків; (b) оцінка інформаційного ландшафту; і (c) розробка плану розслідування. Ці процеси можуть перекриватися та/або повторюватися протягом усього життєвого циклу дослідження.

- Підготовка включає розробку плану поводження з будь-якими негативними психосоціальними аспектами розслідування, такими як ті, які можуть виникнути внаслідок впливу графічних або інших потенційно травматичних матеріалів.

- Підготовка включає розробку плану того, як поводитись з будь-якою інформацією, зібраною протягом її життєвого циклу, включаючи, коли і за яких умов вона повинна бути видалена, як і за яких умов вона може бути надана і кому має бути наданий доступ.

- Підготовка повинна включати оцінку потенційно корисного програмного забезпечення та інших інструментів. Слідчі повинні розуміти компроміси між комерційними, спеціально створеними та відкритими ресурсами.

108. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розпочинати розслідування в Інтернеті лише після вжиття певних підготовчих заходів. Підготовчі кроки мають включати проведення цифрової оцінки загроз та ризиків та оцінку цифрового середовища.[123] Тоді слідчі повинні розробити плани онлайн-розслідувань, інтегруючи висновки з цих оцінок. Нижче докладно описано кожен із цих видів діяльності.

109. На організаційному рівні також важливо встановити політику щодо збереження даних, видалення даних, доступу до даних та обміну ними, перш ніж збирати та зберігати інформацію, як детально описано нижче.

A. Оцінка цифрових загроз та ризиків

110. Роздуми про потенційні загрози та прийняття стратегії управління ризиками – фізичними, цифровими чи психосоціальними – забезпечить дотримання принципів безпеки та етики. Спочатку слід провести оцінку цифрових загроз та ризиків, щоб визначити загальні та конкретні загрози, які можуть виникнути в результаті діяльності в Інтернеті, зокрема відвідування цільових веб-сайтів, постійного моніторингу конкретних джерел або вилучення даних із платформ соціальних медіа . Оцінка повинна включати елементи традиційного аналізу загроз, такі як виявлення всіх потенційних суб'єктів загрози, оцінка інтересів та можливостей цих суб'єктів загрози, а також ймовірності нападу, врахування вразливостей та запровадження заходів захисту для мінімізації цих уразливостей. Такій оцінці сприятимуть консультації з експертами з безпеки або вихідні дані від них, особливо від тих, хто має досвід у галузі кібербезпеки.[124] Оцінку слід періодично переглядати та оновлювати за необхідності. Крім того, можуть знадобитися додаткові оцінки для вирішення конкретних видів діяльності в Інтернеті або впровадження нових потенційних суб'єктів загрози.[125]

B. Оцінка цифрового середовища

111. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розуміти цифрове середовище досліджуваної ситуації. Тип доступної та використовуваної технології, у тому числі ким вона використовується, матиме вплив на типи доступних цифрових даних. Для цього потрібно визначити найбільш часто використовувані онлайн-платформи, послуги зв'язку, платформи соціальних медіа, мобільні технології та мобільні додатки, що використовуються у досліджуваному географічному регіоні. Наприклад, під час розслідування військових злочинів слідчим потрібно буде знати види транспорту, ІТК та цифрові носії інформації, які використовуються усіма сторонами, що беруть участь у збройному конфлікті, а також сторонніх осіб чи інших свідків, щоб знати, які типи інформації найімовірніше будуть захоплені та розповсюджені в Інтернеті.

---

[123] Див. нижче додаток II щодо шаблону оцінки цифрових загроз та ризиків та додаток III щодо шаблону оцінки цифрового середовища.

[124] Загальну інформацію про загрози та ризики у розслідуваннях з використанням даних у відкритому доступі див. у главі IV вище про безпеку.

[125] Див. Додаток II нижче щодо шаблону оцінки цифрових загроз та ризиків.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

112. Слідчі повинні вивчити категорії людей, які використовують або мають доступ до кожної з цих технологій у цьому географічному регіоні. У зв'язку з цим слідчі повинні знати, що створений користувачами загальнодоступний цифровий контент, включаючи публікації в соціальних мережах та інформацію, що передається через мережеві платформи, не може однаково охоплювати весь обсяг порушень щодо всіх осіб та груп. Це пояснюється тим, що використання цифрових технологій може бути різним залежно від, зокрема, статі,[126] етнічної приналежності, релігії, переконань, віку, соціально-економічного статусу, приналежності до расової, мовної,[127] етнічної чи релігійної меншини, корінної ідентичності, міграційного статусу та географічного розташування.[128] This imbalance may be a result of lack of access to devices, facilities or resources,[129] внаслідок чого ці особи не мають можливості створювати або завантажувати в мережі інформацію про проблеми чи порушення, що стосуються їх. Іншим фактором може бути те, що згадані, серед інших, можливо, не мали доступу до рівної освіти, а отже, мали менші можливості з точки зору технічних навичок. Внаслідок перетину форм дискримінації деякі верстви суспільства можуть бути вдвічі непомітними в Інтернеті. Наприклад, інформація про жінок та дівчат, які належать до однієї з вищезгаданих маргінальних груп, може бути ще менш представлена у відкритій інформації. Ці фактори можуть означати, що такі особи не є тими, хто створює контент або охоплюється контентом, тим самим спотворюючи результати будь-якого онлайн-розслідування.

113. Крім того, нерівний доступ до технологій з боку всіх верств суспільства також може спотворити не тільки увагу до того, хто представлений в Інтернет-контенті, а й види порушень, які доступні в Інтернеті, зокрема стосовно контенту, створеного користувачами. Наприклад, коли жінки спільно користуються мобільними телефонами, що належать членам їх сімей чоловічої статі, або діляться обліковим записом з іншими, вони можуть не обговорювати делікатні питання, такі як сексуальне та гендерне насильство, або питання навколо сексуального та репродуктивного здоров'я. Більше того, контент, створений користувачами в соціальних мережах, включаючи фотографії та відео, може легше зобразити певні порушення, ніж інші. Наприклад, сексуальне та гендерне насильство, яке може бути вчинено у приватних умовах, може бути важче зобразити, ніж фотографії виселення, наприклад.

---

[126] Наприклад, жінки, дівчата та лесбіянки, геї, бісексуали, трансгендери та інтерсексуали можуть не мати доступу до сімейного мобільного телефону або бути його власниками. Для подальшого обговорення того, що було названо «гендерним цифровим розривом», див. A/HRC/35/9. Див. також резолюцію Ради з прав людини 32/13 та Араба Сей (Araba Sey) та Ненсі Хафкін (Nancy Hafkin), ред., Підведення підсумків: Дані та докази щодо гендерної рівності у цифровому доступі, кваліфікації та лідерстві (Макао, Китай, Глобальне партнерство EQUALS та Університет Організації Об'єднаних Націй, 2019 рік). Доступно на сторінці www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf.

[127] Ті, хто належить до мовних меншин, наприклад, можуть зіткнутися з перешкодами щодо доступу до Інтернет-простору, який зазвичай ведеться домінуючою мовою. Однак деякі мовні меншини також можуть мати власний інтернет-простір, який ведеться чи на якому користуються власними мовами. Тому слідчим може знадобитися здійснити пошук через мови меншин (у тому числі мовами корінних народів).

[128] Наприклад, у сільській місцевості підключення до Інтернету може бути меншим.

[129] Наприклад, відсутність фізичного доступу до швидкого з'єднання з Інтернетом або неможливість придбати пристрої або оплатити абонплату.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

114. Хоча деякі з цих факторів можна пом'якшити, намагаючись отримати доступ до безлічі типів онлайн інформації, а не лише до контенту, створеного користувачами, ці ж фактори слід враховувати при аналізі інших типів інформації у відкритому доступі. Наприклад, під час доступу до даних та статистичних даних, створених урядом, слідчі завжди повинні ставити під сумнів, чи точно дані охопили всі сегменти та аспекти суспільства.[130] Існує ряд ключових питань та технологій, які можна оцінити, залежно від того, що має значення для конкретного дослідження, виходячи з його географічного та часового масштабу. Слідчі повинні брати до уваги стать, вік, географію, соціально-економічні відмінності та іншу відповідну демографічну інформацію. Мета цієї оцінки – покращити розуміння слідчими ситуацій, що розслідуються, для розробки ефективних онлайн-стратегій розслідування, а також змусити слідчих заздалегідь розглянути потенційні упередження у даних, доступних в Інтернеті. Усі ці категорії можуть не мати відношення до всіх розслідувань, тому слідчим слід адаптувати оцінку цифрового середовища до того, що відповідає їх конкретному випадку.[131] Повний перелік категорій інформації, які можуть бути включені до оцінки цифрового середовища, див. у додатку III нижче.

C. План онлайн-розслідування

115. Перед початком розслідування з використанням даних у відкритому доступі слід створити план онлайн-розслідування,[132] який охоплює (a) загальну стратегію розслідування; і (b) конкретні операції з розслідування в Інтернеті. Якщо онлайн-розслідування є частиною більш широкого розслідування з використанням традиційних методів, таких як взяття показань свідків або збір речових доказів, план онлайн-розслідування слід включити до основного плану розслідування. Слідчі повинні включити гендерну перспективу до плану розслідування, щоб гарантувати, що розслідування поширюватиметься на всі проблеми, що стосуються статі, та враховуватиме диференційований характер доступу до технологій.[133] План онлайн-розслідування має стосуватися наступних тем.

1. Цілі та заплановані заходи

116. План повинен визначати цілі та пріоритети розслідування з використанням даних у відкритому доступі, запропоновану стратегію досягнення цих цілей та строки їх реалізації.

2. Стратегія управління ризиками

---

[130] Див., загалом, УВКПЛ «Підхід до даних на основі прав людини: не залишаючи нікого позаду у Порядку денному для сталого розвитку на період до 2030 року» (Женева, 2018 рік). Доступно на сторінці www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

[131] Шаблон див. у додатку III нижче.

[132] Див. додаток I нижче щодо шаблону онлайн-розслідування.

[133] Додаткові вказівки щодо того, як інтегрувати гендерну перспективу, див. у роботі *Інтеграція гендерної перспективи у розслідування у сфері прав людини: Керівництво та практика* (публікація Організації Об'єднаних Націй, товарний № 19.XIV.2).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

117. План повинен включати основні висновки вищезгаданої цифрової загрози та оцінки ризиків, такі як потенційні кіберзагрози, а також стратегію управління ризиками, включаючи способи виявлення, реагування та відновлення після порушень чи атак.

3. Відображення суб'єктів та можливостей співпраці

118. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі,, можливо, захочуть зіставити інших суб'єктів, які проводять подібні чи дублюючі розслідування, щоб оцінити, як їх діяльність може вплинути один на одного, а також дослідити потенційні партнерські відносини та можливості для співпраці. Це може включати ідентифікацію цифрових архівістів, журналістів чи інших груп чи осіб, які зберігають онлайн-контент, який може мати відношення до розслідування. Це відображення також має враховувати потенційну упередженість та обмеження інших суб'єктів, що може призвести до висновків третіх сторін, які не повністю враховують складності певної ситуації, або можуть виключати певні групи через властиву упередженість цифрової сфери, що не є пристосованою, як описано вище. Якщо такі партнерства формуються, може бути корисно укласти письмову угоду для обміну інформацією.

4. Ресурси

119. План повинен визначати ресурси, необхідні для проведення запланованих заходів, включаючи персонал, навчання, інструменти та обладнання. Оцінка потреб у персоналі може включати кількість членів команди, необхідну для виконання завдань, їх компетенцію, інклюзивність та різноманітність членів команди та оцінку додаткових вимог до навчання. Це може включати оцінку необхідної інфраструктури, включаючи апаратне та програмне забезпечення, та фінансові витрати на збереження цифрового матеріалу в довгостроковій перспективі. План також повинен забезпечити наявність спеціальних ресурсів для забезпечення гендерно-чутливого психологічного благополуччя слідчих, особливо в ситуаціях, коли розслідування з використанням даних у відкритому доступі стосується графічного контенту або слідчих або причетних третіх осіб, особливо під загрозою репресій, якщо їх особистість або конфіденційність ставляться під загрозу.[134]

5. Ролі та обов'язки

120. У разі роботи в команді або із зовнішніми партнерами слід чітко визначити роль та відповідальність слідчих, що ведуть розслідування з використанням даних у відкритому доступі, враховуючи необхідність координації діяльності, включаючи необхідність уникати дублювання діяльності та збору даних. Крім того, у цьому розділі плану слід розглянути,

---

[134] Наприклад, слідчі можуть зіткнутися з мовою ворожнечі чи переслідуванням в Інтернеті, і ці напади можуть бути гендерними (наприклад, слідчі-жінки та лесбіянки, геї, бісексуали, трансгендери, гомосексуалісти та інтерсексуалісти можуть зіткнутися з вищими, ніж у середньому, ризиками висловлювання ненависті в Інтернеті, докси, погроз згвалтування та інших видів загроз сексуального або гендерного характеру). Див., наприклад, Amnesty International, «Токсичний Twitter – токсичне місце для жінок». Доступно на сторінці www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

які спеціалізовані галузі знань можуть знадобитися для конкретного розслідування, і чи слідчим слід буде проконсультуватися або залучити експерта, якщо його немає у наявній групі. Спеціалізовані галузі знань можуть включати цифрову криміналістику, аналіз супутникових знімків та науку про дані. У деяких галузях експертизи можуть знадобитися активні зусилля для виявлення експертів різної статі та інших категорій, щоб забезпечити всебічність та різноманітність слідчої групи та її аналізу.

6. Документація

121. Розслідування з використанням даних у відкритому доступі мають бути задокументовані таким чином, щоб забезпечити їх ефективне управління та дотримання принципу підзвітності. У разі судового розгляду ця документація повинна дозволити слідчим продемонструвати, що зібрані докази є актуальними та доказовими, та пояснити кроки, вжиті або не вжиті під час діяльності в Інтернеті, і причини. Незалежно від того, чи було поставлено завдання самостійно або воно було отримано від керівника, система повинна мати механізм для створення завдань для конкретних слідчих заходів, включаючи діяльність в Інтернеті, наприклад, запити на дослідження конкретної особи чи інші запити. Результати завдань, включаючи звіти, повинні містити посилання на використовувані методології та прийоми. Звітування повинно відокремлювати оперативну інформацію, яку, можливо, потрібно зберегти в таємниці, щоб захистити джерела та методи розслідування від інформації розслідування, яку необхідно розкрити під час судового розгляду.

122. План онлайн-розслідування слід регулярно переглядати та, за необхідності, вносити в нього зміни. Шаблон плану онлайн розслідування див. у додатку I нижче.

D. План стійкості та турбота про себе

123. Хоча слідчі, що ведуть розслідування з використанням даних у відкритому доступі, не можуть проводити особисті опитування чи фізично відвідувати місця злочину, особливості цифрових досліджень означають, що вони можуть бути піддані перегляду, збору та аналізу значної кількості графічної чи іншої травматичної цифрової інформації, що може призвести до вторинної травми, серед інших питань. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні знати принципи турботи про себе,[135] а керівники розслідувань повинні створити організаційне середовище, яке цінує турботу про себе та гендерну та культурну чутливість. Це повинно бути розпочато на підготовчому етапі розслідування шляхом розробки плану сприяння стійкості та пом'якшення негативних психосоціальних наслідків розслідування, які можуть мати різні наслідки залежно від статі, культури та віку. Такий план є надзвичайно важливим з етичних міркувань, як частина просування та поваги прав людини кожного члена слідчої групи. Це також важливо для забезпечення максимальної фізичної та цифрової безпеки. Навіть при належному навчанні особа, що піддається стресу, може представляти вразливість для безпеки команди, безпеки інформації та якості роботи. Необхідно виділити спеціальний час та ресурси для

---

[135] Для подальшого обговорення важливості турботи про себе для тих, хто працює у сфері розслідування порушення прав людини, див. УВКПЛ, Посібник з моніторингу прав людини (Женева, 2011 рік), глава 12 про травми та турботу про себе, стор. 20-39. Доступно на сторінці www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

забезпечення належного виконання плану, зокрема, коли передбачається, що онлайн-розслідування може включати перегляд великої кількості графічних зображень, включаючи насильницький або інший тривожний контент. Стратегії пом'якшення потенційного негативного впливу перегляду графічного контенту різноманітні, але, як правило, поділяються на три категорії: індивідуальна обізнаність, тактика мінімізації впливу та підтримка громади.

124. По-перше, слідчі повинні знати про свою власну поведінку та поведінку товаришів по команді, включаючи схеми роботи, відпочинку, сну та харчування, щоб можна було виявити та усунути відхилення. Політика того, як слідчі працюють у парах, може допомогти виявити, оскільки люди можуть не визнати або не захотіти визнати своїх власних змін у поведінці, які інші можуть легше помітити. Члени команди повинні бути чутливими та поважати відмінності у відповідях на графічний та інший матеріал, які можуть викликати сильні емоції, та усвідомлювати, що такі відмінності можуть відрізнятися між окремими особами, статтю та культурними групами, а також з часом для окремих осіб через ступінь стресу, в якому вони перебувають, та інших ситуативних факторів. Слідчі також повинні визнати, що емоційна реакція на графічний або кричущий контент часто є цілком нормальною і не є ознакою слабкості, але може бути ознакою здорового функціонування – і навіть сили.

125. По-друге, слід прийняти тактику мінімізації впливу шкідливого контенту. Загальні стратегії в цьому відношенні включають вимкнення звуку при першому перегляді потенційно графічного контенту або коли це не потрібно для негайного аналітичного завдання, оскільки стільки емоційного вмісту вбудовано у звук; зведення до мінімуму розмірів екранів; висвітлення графічного матеріалу при аналізі контексту навколо конкретної дії, а не самої дії; позначення будь-якого графічного контенту, що міститься у наборі даних, щоб люди не переглядали цей контент, не знаючи заздалегідь, що вони збираються побачити; попередження один одного при обміні графічним контентом, щоб пом'якшити елемент несподіванки; робота в парах; уникнення роботи ізольовано або пізно вночі; і регулярні перерви, якщо це необхідно.

126. По-третє, окремі особи та організації повинні виховувати почуття спільності серед членів команди, що може мати захисний ефект – по суті відтворюючи почуття товариства, яке може виникнути під час проведення розслідувань на місцях. Цього можна досягти шляхом регулярних аналізів, які можуть зменшити ізоляцію та допомогти слідчим краще зрозуміти позитивний вплив їх роботи; колективні виїзди, включаючи святкування важливих етапів розслідування; та навчання команди стратегіям стійкості. Спроби підвищити стійкість можуть бути особливо впливовими, коли вони вирішуються на індивідуальному, культурному та структурному рівнях, наприклад, шляхом надання особам можливості критично обмірковувати свої психосоціальні потреби під час роботи над розслідуванням та створення середовища, в якому серйозно враховуються психосоціальні аспекти роботи, явно та неявно заохочується підтримуюча практика, а також вітається інклюзивність та різноманітність.

E. Політика щодо даних та інструменти

127. Політика щодо поводження, збереження та знищення даних повинна бути розроблена, впроваджена та дотримуватися під час розслідування. Організації повинні розробити політику збереження інформації (політики збереження) та видалення інформації (політики видалення), коли це доречно, а також політику щодо надання доступу до інформації (на внутрішньому рівні) та обміну інформацією (на зовнішньому рівні). Крім того, може бути корисною специфічна політика щодо створення та використання віртуальних особистостей, а також доступ до затвердженого програмного забезпечення та використовуваних інструментів.

1. Політика щодо даних

(a) Політика збереження даних

128. Політика збереження даних важлива для того, щоб дотримуватись багатьох законів про захист даних та правил зберігання даних. У деяких випадках існують мінімальні вимоги щодо того, як довго дані повинні зберігатися, тоді як в інших випадках існує максимальне обмеження щодо того, як довго дані можна зберігати. Політика повинна визначати підходи до зберігання постійних даних та управління записами з метою задоволення вимог щодо архівування юридичних та комерційних даних. Різні правила збереження даних порівнюють правові проблеми та проблеми конфіденційності з економічними проблемами та проблемами, що потребують знання, щоб визначити час зберігання, архівні правила, формати даних та допустимі засоби зберігання, доступу та шифрування.[136] Розуміння правил, які застосовуються, буде необхідним для створення такої політики.

(b) Політика видалення даних

129. Видалення частин набору даних без чіткої політики видалення та збереження та без журналів того, що було видалено, ким і коли – і для яких цілей – може викликати значні проблеми, зокрема, коли інформація може бути використана в суді. Слідчі повинні дотримуватися чинних нормативних актів щодо видалення цифрових даних і знати, що при використанні одного методу, а не іншого, можуть виникнути правові проблеми.

(c) Політика надання доступу до даних

130. Організації, які збирають та обробляють дані, особливо конфіденційні, повинні мати чітку політику щодо того, хто має доступ до різних типів даних. Будь-які налаштування в базах даних або системах мають здійснюватися відповідно до цієї політики.

(d) Політика щодо обміну даними

131. Можливо, організації захочуть розробити політику обміну даними із зовнішніми суб'єктами. У разі роботи із зовнішніми партнерами слід укласти меморандуми про

---

[136] Івон Нг (Yvonne Ng), «Як ефективно зберігати інформацію у відкритому доступі», у Digital Witness, Використання інформації у відкритому доступі для розслідування, документації та підзвітності в області прав людини, Сем Дабберлі (Sam Dubberley), Алекса Кеніг (Alexa Koenig) та Дараг Мюррей (Daragh Murray), ред. (Оксфорд, Oxford University Press, 2020 рік), стор. 143-164.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

взаєморозуміння або укласти договори, щоб гарантувати, що партнери дотримуватимуться такої політики.

2. Управління інформацією

132. Перш ніж брати участь у розслідуваннях з використанням даних у відкритому доступі, зокрема у зборі та збереженні цифрових матеріалів, слідчі, групи та організації повинні створити систему управління інформацією. Існує цілий ряд варіантів такої системи, і Протокол не виступає за конкретний з них. Натомість нижче наведено основні функціональні можливості, які можуть бути корисними для процесу розслідування – і в деяких контекстах можуть знадобитися. Крім того, як обговорювалось у главі IV, мають бути встановлені інфраструктура та протоколи безпеки.

(a) Система управління розслідуваннями

133. Система управління розслідуванням – це система документування діяльності, яка проводиться в рамках розслідування. Не всі організації, які проводять розслідування, мають такі системи, але вони настійно рекомендуються, особливо для великих організацій або слідчих груп. Такі системи можна використовувати для призначення завдань та звітування про діяльність, щоб процес був структурованим та максимально ефективним, оскільки це може допомогти зменшити дублювання зусиль.

(b) Системи управління інформацією та доказами

134. Системи управління інформацією використовуються для зберігання даних, зібраних у рамках розслідувань. Система управління інформацією повинна виконувати дві різні функції: (a) відстеження збору та поводження з матеріалом; та (b) відокремлення матеріалу, який може бути використаний як доказ.

3. Інфраструктура – питання логістики та безпеки

135. Незалежно від проектування інфраструктури для організації, що займається розслідуваннями з використанням даних у відкритому доступі, або прийняття рішення про те, які інструменти використовувати як незалежним слідчим, існує кілька важливих логістичних міркувань та питань безпеки. Загалом, існує три підходи до розвитку систем: (a) спеціальні системи та інструменти; (b) використання відкритих або безкоштовних інструментів та програмного забезпечення, доступного в Інтернеті; або (c) придбання комерційних продуктів у третіх сторін. Кожен із цих підходів має свої переваги та недоліки, і їх успіх залежить від конкретних обставин та контексту, в якому працюють слідчі. Знову ж таки, Протокол не виступає за один конкретний підхід, а представляє переваги та недоліки кожного з них, а також конкретні фактори, які слід враховувати, приймаючи рішення про те, які продукти використовувати.

(a) Комерційна продукція

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

136. Перевага комерційних продуктів полягає в тому, що приватний бізнес може мати кращу інфраструктуру для забезпечення безпеки та мати можливість надавати постійну та послідовну технічну підтримку. Однак комерційна продукція має очевидну зворотну сторону вартості. Крім того, взаємодія з третіми сторонами та покладання на них можуть бути проблемою для організацій, які намагаються зберегти конфіденційність своїх розслідувань. Багато комерційних продуктів мають закритий вихідний код для захисту своєї інтелектуальної власності. Комерційні продукти також можуть викликати занепокоєння щодо володіння даними, переносу та експорту даних та сумісності з іншими системами. Крім того, компанії можуть реагувати на тиск уряду щодо доступу до приватної інформації. Ключовою проблемою є те, що, хоча у компаній є групи безпеки для захисту своїх продуктів та користувачів, ці користувачі мають вірити, що компанії розробили та належним чином обслуговуватимуть свої системи, і що на пізньому етапі не буде прихованих витрат.

(b) Спеціальні інструменти

137. Перевага створення спеціального інструменту з нуля або налаштування вже існуючого інструменту полягає в тому, що слідчі або організації зберігають контроль над усією системою та їх даними, і, як наслідок, можуть уникнути взаємодії з третіми сторонами. Спеціальні системи також можна легше інтегрувати з іншими спеціальними системами. Негативною стороною є час, вартість та досвід, необхідні для побудови та підтримки таких систем, що стане проблемою для більшості організацій. Крім того, закрита система з обмеженими бета-тестерами та користувачами може ускладнити виявлення вразливих місць або отримання достатнього відгуку для максимізації функціональних можливостей.

(c) Відкриті та безкоштовні інструменти

138. Інструменти у відкритому доступі – це інструменти, для яких розробники відкрито опублікували вихідні коди, щоб кожен міг вільно їх використовувати або змінювати. Деякі комерційні продукти існують з відкритими кодами, а деякі безкоштовні інструменти доступні із закритими кодами, але це винятки. Найчастіше інструменти у відкритому доступі безкоштовні. Для невеликих організацій з обмеженим бюджетом, а також для великих організацій, які мають обтяжливі процедури закупівель платної продукції, безкоштовні інструменти можуть стати важливою альтернативою для розгляду. Однак безкоштовні для користувачів інструменти можуть приносити прибуток іншими способами, такими як продаж даних користувачів та аналітика, що піднімає питання безпеки та конфіденційності. Крім того, використання цих інструментів вимагає попереднього дослідження, щоб дізнатися, хто їх створив, чи проходив їх незалежний аудит, і чи вони є стійкими. Усі три аспекти можуть підірвати достовірність розслідування. Зокрема, інструменти можуть бути проблематичними в юридичному контексті, якщо справа переходить до судового розгляду, а інструмент оскаржується протилежною стороною. Крім того, ці програмні системи та інструменти вимагають плану резервного копіювання та системи міграції та резервного копіювання даних на випадок, коли вони застаріють або розробники стануть недоступними. Хоча інструменти у відкритому доступі можуть бути привабливими для організацій, частково через те, що ними користуються інші

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

групи однодумців, слідчі повинні проводити повну, незалежну оцінку того, як вони працюють, і наслідки, які їх використання може мати в певному контексті.

139. Приймаючи рішення про те, чи створювати спеціальний інструмент, використовувати безкоштовну пробну версію або програмне забезпечення у відкритому доступі або купувати продукт, слідчі повинні дотримуватися вказівок щодо належної перевірки, наведених у додатку V нижче.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

VI

ПРОЦЕС РОЗСЛІДУВАННЯ

РЕЗЮМЕ ГЛАВИ

- Існує шість основних етапів процесу розслідування. Це (a) онлайн-запити; (b) попередня оцінка; (c) збір; (d) збереження; (e) перевірка; та (f) слідчий аналіз. У сукупності це частина циклу, який може повторюватися багато разів протягом всього розслідування, оскільки нововиявлена інформація веде до нових напрямків дослідження.

- Слідчі повинні документувати свою діяльність на кожному етапі. Це допоможе зрозуміти та забезпечити прозорість їхніх розслідувань, включаючи ланцюги забезпечення збереження, а також ефективність та дієвість їхніх розслідувань, включаючи повноту та комунікацію між членами команди.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

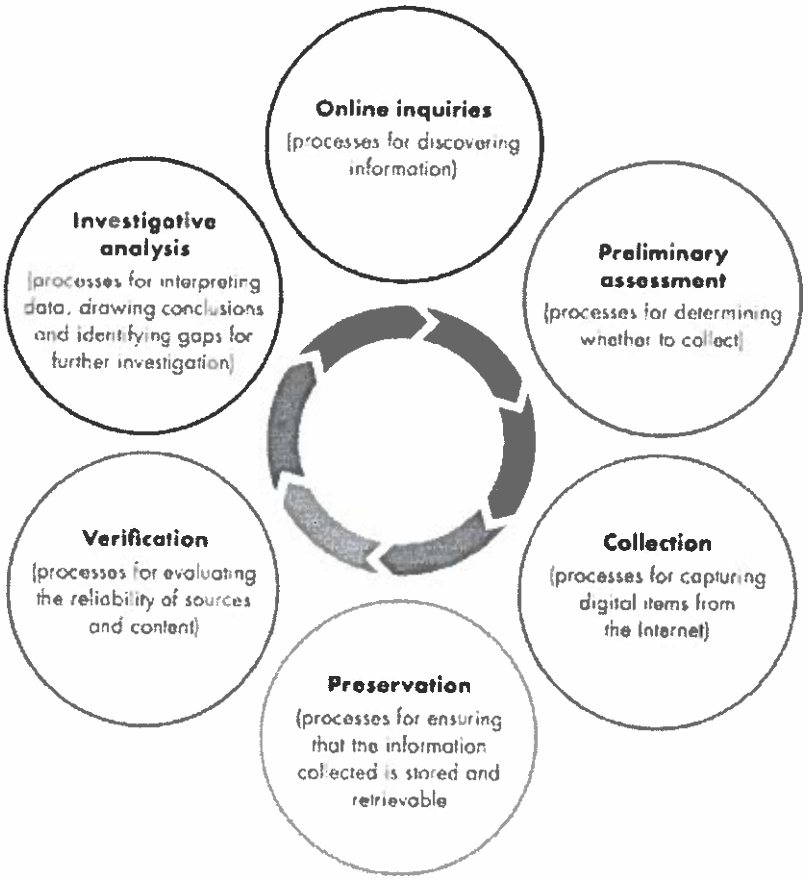
Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

140. Розслідування з використанням даних у відкритому доступі вимагають ретельного спостереження та систематичних запитів для встановлення фактів у складному та динамічному цифровому середовищі. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні використовувати критичний погляд, щоб перевіряти онлайн-контент та вміти оцінювати способи спотворення чи маніпулювання цифровими матеріалами. Вони також повинні застосовувати структурований підхід до запитів в Інтернеті, враховуючи алгоритмічну упередженість та нерівність щодо наявності інформації у відкритому доступі, що стосується певних груп, та динамічного характеру інформації в Інтернеті. Кожен передбачуваний факт слід ретельно вивчити. У цій главі представлено структурований підхід до розслідувань з використанням даних у відкритому доступі. На рисунку нижче зображено цикл розслідування з використанням даних у відкритому доступі. Важливо відзначити, що розслідування з використанням даних у відкритому доступі рідко бувають лінійними і часто вимагають повторення цього процесу з огляду на циклічність побудови. Також можуть виникнути вагомі причини для відступлення від цього порядку.

Цикл розслідування з використанням даних у відкритому доступі



Онлайн-запити
(процеси виявлення інформації)

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Слідчий аналіз
(процеси інтерпретації даних, висновків та виявлення прогалин для подальшого дослідження)

Попередня оцінка
(процеси визначення необхідності збирання)

Перевірка
(процеси оцінки надійності джерел та контенту)

Збір
(процеси захоплення цифрових елементів з Інтернету)

Збереження
(процеси забезпечення зберігання та можливості повторного зберігання зібраної інформації)

A. Онлайн-запити

141. Є два основні процеси для онлайн-запитів: (a) пошук, тобто виявлення інформації та джерел інформації за допомогою загальних або розширених методологій пошуку; і (b) моніторинг, тобто виявлення нової інформації шляхом послідовного та наполегливого огляду набору постійних джерел.

1. Пошук

142. Інтернет-пошук – це діяльність, орієнтована на завдання, спрямована на виявлення нової інформації, що стосується визначеної мети або досліджуваного питання. Пошуки мають бути структурованими та систематичними, включаючи чітке досліджуване питання та параметри пошуку, а також ключові слова та операторів.[137] Різні пошукові системи, інструменти пошуку, пошукові терміни та оператори нададуть різні результати; тому слідчі повинні проявляти певний творчий потенціал та наполегливість у слідуванні різними шляхами та каналами для пошуку відповідної інформації. Окрім пошукових систем, які використовуються для пошуку інформації на індексованих веб-сайтах, структурований пошук також може використовуватися на платформах соціальних медіа та в базах даних. Через необхідність застосування різноманітного та конкретного підходу, слідчі повинні ретельно документувати свої процеси, щоб їх можна було пояснити у розділі методології звітів або надати свідчення в судовому процесі. Це може бути зворотний процес, а не обов'язково той, що триває паралельно з самим дослідженням. Однак документацію завжди слід складати максимально одночасно. Документація структурованих пошуків повинна містити таку інформацію:

---

[137] Логічні оператори – це прості слова, такі як «і», «або» і «ні», які можна використовувати «для об'єднання або виключення ключових слів у пошуку, що призводить до більш цілеспрямованих і продуктивних результатів». Див. Alliant International University Library, «Що таке логічний оператор?» Доступно на сторінці https://library.alliant.edu/screens/boolean.pdf.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(a) Об'єктивні та дослідницькі запитання: сформулюйте питання, на які необхідно знайти відповідь за допомогою пошуку в Інтернеті, маючи на увазі принцип об'єктивності, наведений вище;

(b) Факти, припущення та невідомі: починати з того моменту, коли факти відомі, якщо такі факти були встановлені. Також може бути корисно працювати на основі інформації про потенційних клієнтів або логічних припущень, навіть якщо вони ще не перевірені. Однак важливо, щоб будь-які припущення записувалися як такі. Нарешті, може бути цінним сформулювати прогалини у знаннях або інші «невідомі» на початку розслідування. Розмежування цих категорій інформації допоможе запобігти упередженим або перекошеним результатам, уточнивши терміни пошуку та їх основи;

(c) Пошукові терміни та ключові слова: для проведення цілеспрямованого пошуку слідчі повинні створити списки ключових слів, які відповідають принципу об'єктивності, заснованому на теорії чи кількох теоріях справи. В ідеалі слідчі використовуватимуть ключові слова усіма відповідними мовами та сценаріями та будуть обережними щодо потенціалу надмірного чи недостатнього включення результатів пошуку. Незважаючи на варіації у справах, існують певні загальні теми, які слід включити до списків ключових слів, такі як значні місцезнаходження, назви, організації, дати та відповідні хештеги. Також може бути корисно визначити, що може кваліфікуватися як обвинувачувальна та виправдовувальна інформація в контексті конкретного розслідування;

(d) Пошуки та пошукові системи: слідчі повинні відстежувати їхні пошуки та записувати шляхи до відповідного матеріалу, включаючи терміни, операторів та пошукові системи, які призвели до такого контенту. Слідчі не повинні фіксувати всі результати пошуку, оскільки це буде надмірно обтяжливим і не матиме доказової сили.

2. Моніторинг

143. Моніторинг передбачає відстеження встановленого джерела інформації, наприклад, певної теми, з плином часу. Метою є відстеження змінного контенту, що генерується постійним джерелом. Онлайн-моніторинг має бути структурованою діяльністю, яка використовує списки відомих та попередньо оцінених онлайн-джерел, таких як веб-сайти чи облікові записи в соціальних мережах, а також пошукові запити, які постійно виконуються щодо визначених цілей. Дивіться, наприклад, такі джерела:

(a) Веб-сайти та облікові записи в соціальних мережах: слідчі повинні вести робочі списки веб-сайтів та профілів, які підлягають моніторингу, які повинні містити обґрунтування того, чому вони контролюються; особа, відповідальна за моніторинг; хто здійснює моніторинг; та періодичність моніторингу;

(b) Хештеги та ключові слова: слідчі також повинні вести та регулярно оновлювати робочий список хештегів та ключових слів, які контролюються;

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(c) Автоматизація: моніторинг може включати використання автоматизованих інструментів, які можуть, наприклад, періодично проводити пошук на певних сайтах або за допомогою певних параметрів. Використання таких інструментів, включаючи їх назви та версії, а також введену до них інформацію слід завжди записувати.

3. Упередженість

144. Проводячи структуровані пошукові та моніторингові заходи, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, завжди повинні пильно стежити за упередженням – як власним когнітивним упередженням, так і властивим упередженням у інформації, доступній в Інтернеті. Наприклад, якщо слідчий шукає інформацію про зґвалтування, більшість наданих даних або проблеми, що обговорюються в Інтернеті, ймовірно, стосуватимуться зґвалтування жінок репродуктивного віку, вчиненого поза шлюбними відносинами. Результати пошуку можуть недооцінювати менш помітні або зареєстровані види зґвалтування, такі як сексуальне насильство проти чоловіків і хлопчиків, лесбіянок, геїв, бісексуалів, трансгендерів та інтерсексуалів, а також літніх жінок та випадків зґвалтування у шлюбі.

145. Інший приклад – розслідування насильства, спричиненого мовою ворожнечі в Інтернеті, оскільки таке мовлення часто включає та залежить від кодованої мови та символів, які нелегко розпізнаються слідчими чи машинами. Особливо, коли слідчі приходять з-за меж спільнот, на які вони спрямовані, вони можуть не знати про культурне та конкретне використання термінів та символів, що використовуються для розпалювання ненависті чи насильства. Це ускладнюється тим, що онлайн-мова ворожнечі часто навмисно розроблена, щоб уникнути виявлення машинними або людськими моніторами, видалення з онлайн-платформ, хоча насправді спрямована на розпалювання насильства або дискримінацію щодо цільової групи населення. Для того, щоб допомогти подолати труднощі виявлення підбурювання до дискримінації, ворожнечі чи насильства, слідчі повинні застосувати перевірку на основі прав людини, як це, наприклад, передбачено у Плані дій Рабат щодо заборони пропаганди національної, расової чи релігійної ненависть, яка є підбурюванням до дискримінації, ворожості чи насильства.[138]

146. Зрештою, найкращий спосіб для слідчих протидіяти «упередженості в машині» разом з їх упередженням – це усвідомлювати потенціал такого упередження, визнавати ризики та вживати активних заходів, коли це можливо, щоб врівноважити упередження, досліджуючи відповідну термінологію та символи, що є релевантними для певного контексту чи сукупності злочинів чи інцидентів, а також розширюючи та урізноманітнюючи онлайн-розслідування. У справах, що стосуються сексуального та гендерного насильства, а також будь-яких інших злочинів, у яких жертви стигматизовані та використовуються кодовані мови, слідчі повинні проконсультуватися з експертами, які можуть виявити та поділитися кодованою мовою та практикою спілкування, якою

---

[138] Див. УВКПЛ, «Свобода вираження поглядів проти розпалювання ненависті: УВКПЛ та План дій Рабату». Доступно на сторінці www.ohchr.org/EN/ Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

користуються такі жертви та злочинці часто використовують під час спілкування в Інтернеті.[139]

B. Попередня оцінка

147. Перш ніж збирати контент з Інтернету, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні провести попередню оцінку будь-якого матеріалу, який вони ідентифікують, щоб уникнути надмірного збору та дотримання принципів мінімізації даних та цілеспрямованого розслідування, а також для забезпечення того, щоб збір матеріалу не порушував право на приватне життя приватних осіб. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні врахувати наступні фактори, щоб визначити, чи слід збирати цифровий елемент з Інтернету.

1. Релевантність

148. Розслідування з використанням даних у відкритому доступі має визначити, чи є цифровий елемент prima facie відповідним для конкретного розслідування. Релевантність будь-якого елементу залежить від його змісту та джерела, а також від цілей розслідування та того, що відомо про ситуацію. На ранніх стадіях розслідування може бути важко дізнатися, що має значення, що може призвести до помилок слідчих, а саме надмірного збирання. Тим не менш, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні мати можливість чітко сформулювати, чому вони вважають, що той чи інший елемент є потенційно релевантним, і цю оцінку слід записати (наприклад, за допомогою простої та зручної системи тегування або зберігання, яка пов'язує зібрану інформацію з, наприклад, місцем, датою, інцидентом, особою чи типом порушення, яке розслідується).

2. Достовірність

149. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні визначити, чи є інформація чи претензії щодо цифрового контенту prima facie достовірними, переглянувши та оцінивши контент, а також контекстну інформацію, що міститься у файлі. Це може включати перевірку вбудованих метаданих, пов'язаної інформації та джерела.[140] Цей процес має включати спробу виявлення першоджерела матеріалу, що може вимагати відстеження онлайн-походження даних, завантажувача чи автора.

3. Видалення

150. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні оцінити, чи є ймовірність видалення цифрового елемента з Інтернету чи загального доступу. Якщо видалення контенту є ймовірним, слід зібрати найнадійнішу відому версію

---

[139] Див., наприклад, Кеніг (Koenig) та Еган (Egan), «Приховування на простому веб-сайті: використання інформації з відкритого джерела в Інтернеті для розслідування сексуального насильства та злочинів на гендерній основі».

[140] Див. главу VI.E нижче щодо перевірки.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

контенту , навіть під час подальшої перевірки та розслідування щодо більш ранніх або кращих версій. Ймовірність видалення контенту можна оцінити на основі ряду факторів, включаючи передбачувану особистість джерела, розташування контенту та сумісність контенту з умовами користувацької угоди з постачальником послуг. Наприклад, графічний або образливий контент, який міг би мати високу доказову силу для встановлення злочинів чи порушень, є одним із найбільш ймовірних контентів, які будуть видалені.

4. Безпека

151. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні визначити, чи безпечно збирати цифровий елемент, чи можна і потрібно вжити додаткових запобіжних заходів. Занепокоєння, швидше за все, виникне у разі збору з веб-сайту, який може містити пошкоджені елементи, які можуть пошкодити внутрішню систему.

5. Подальші обов'язки

152. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні визначити, які обов'язки можуть виникнути, якщо взяти під опіку цифровий елемент, наприклад, обов'язок зберігати його в безпечному порядку відповідно до законів про захист даних.[141]

C. Збір

153. Збір – це акт заволодіння інформацією в Інтернеті за допомогою знімка екрана, конвертації у PDF, експертного завантаження чи іншої форми захоплення. Після того, як цифровий контент буде ідентифіковано та визнано відповідним для розслідування, та prima facie відповідним та надійним для своєї мети, слідчий повинен визначити належний метод збору. Методи збору можуть змінюватись залежно від того, чи має онлайн-контент потенційну доказову силу в судових процесах, чи буде він використовуватися для прийняття рішень, чи він буде сприяти лише внутрішньому продукту роботи. У випадках, коли мова йде просто про робочий продукт, може бути достатньо скріншоту або перетворення в PDF, тоді як вміст, що має потенційну доказову силу, може вимагати більш ретельного та обґрунтованого методу збору (наприклад, шляхом призначення значення хешу – див. нижче).

154. Збір онлайн-контенту може здійснюватися вручну за стандартною операційною процедурою або бути автоматизованим за допомогою різноманітних інструментів або сценаріїв. Незалежно від процесу, перелічена нижче інформація в ідеалі повинна бути зібрана в момент збору. Ця інформація може бути корисною для встановлення справжності цифрового елемента. Це може бути особливо важливим у разі судового розгляду, в якому елемент пропонується як доказ, особливо якщо автор чи творець не ідентифіковані, не знайдені чи не доступні для надання свідчень. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні збирати онлайн-контент у його

---

[141] Див. главу VI.D нижче щодо збереження.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

рідному форматі або в стані, максимально наближеному до його вихідного формату. Будь-які зміни, перетворення або конвертації, спричинені процесом збору, повинні бути задокументовані.

155. Нижче наведено вказівки щодо того, що збирати та як збирати. Існує кілька інструментів, які допомагають зафіксувати наведену нижче інформацію, або це можна зробити вручну. Тоді як збирання всієї наведеної нижче інформації вважається найкращою практикою, перші три пункти (єдиний локатор ресурсів (URL), вихідний код мови розмітки гіпертексту (HTML) та захоплення всієї сторінки) служать мінімальним стандартом для надання доказів у суді. Звичайно, такі стандарти будуть відрізнятися в різних контекстах, але захоплення всіх перерахованих нижче елементів забезпечить міцну основу в будь-якому контексті:

(a) Цільова веб-адреса: веб-адресу зібраного контенту, також відому як єдиний локатор ресурсів (URL) або ідентифікатор (URI), слід записати;

(b) Вихідний код: слідчі повинні захопити вихідний код HTML веб-сторінки, якщо це можливо. Вихідний код HTML містить набагато більше інформації, ніж видима частина веб-сайту. Вихідний код HTML сприятиме автентифікації зібраного матеріалу;

(c) Захоплення всієї сторінки: слідчі повинні спочатку зробити знімок екрана цільової веб-сторінки із зазначенням дати та часу. Причина цього процесу полягає в найкращому уявленні того, що було побачено під час збору;

(d) Вбудовані мультимедійні файли: наприклад, якщо завантажують веб-сторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з веб-сторінки;

(e) Вбудовані метадані: слідчі повинні зібрати додаткові метадані цифрового елемента, якщо вони є та застосовні. Метадані можуть змінюватися залежно від джерел, але загальні метадані включають ідентифікатор користувача завантажувача; ідентифікатор публікації, зображення чи відео; дату та час завантаження; геотег; хештег; коментарі; та анотацію;

(f) Контекстуальні дані: контекстний контент також слід збирати, якщо він має значення для розуміння цифрового елемента. Вони можуть включати коментарі до відео, зображення чи публікації; передбачати завантаження інформації; та/або інформацію про завантажувача/користувача, таку як ім'я користувача, справжнє ім'я чи біографію. Необхідність збору навколишньої інформації слід визначити, виходячи зі специфіки випадку та цифрового матеріалу;

(g) Дані збору: слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні записати всі відповідні дані, що стосуються збору, такі як ім'я збирача, IP-адреса машини, яка використовується для збору інформації, віртуальна особистість, за наявності, та мітка часу. Слідчі повинні переконатися, що системний годинник точний, бажано, шляхом його синхронізації з сервером мережевого протоколу часу. Причиною цього кроку є забезпечення того, щоб метадані, пов'язані з часом, були точно представлені

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

у зібраних файлах. Якщо для доступу до зібраної інформації використовується віртуальна особистість, це слід зазначити;

(h) Хеш-значення: хеш-значення – це унікальна форма цифрової ідентифікації, яка за допомогою криптографії підтверджує, що зібраний контент є унікальним і не змінювався з моменту збору. На момент збору слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вручну додати – або інструмент збирання – автоматично додати – значення хешу. Існує безліч різних типів хешів, і стандарти з часом змінилися. Слідчі повинні оцінити, який хеш використовувати, виходячи з прийнятого на даний момент стандарту.[142]

156. У випадках автоматизованого збору деякі описані процеси можуть бути виконані засобами, призначеними для збору відповідного контенту та метаданих. Для кожного зібраного матеріалу слід скласти технічний звіт, що містить вищезазначену інформацію з метою встановлення автентичності елементу пізніше. Контекстна інформація та всі типи метаданих завжди повинні зберігатися разом із цифровим елементом, як пояснюється у наступному розділі.

D. Збереження

157. Постійність та доступність інформації в Інтернеті часто є нестабільною. Платформи соціальних медіа можуть видаляти контент зі своїх платформ відповідно до своїх умов використання, або користувачі можуть вибирати видалення або редагування власного завантаженого контенту. Крім того, інформацію в Інтернеті можна легко деконтекстуалізувати, втратити, стерти або пошкодити.[143] Щоб цифровий матеріал залишався доступним та використовуваним для цілей забезпечення юридичної відповідальності, його слід зберігати як у короткостроковій, так і в довгостроковій перспективі.[144] Як правило, метою цифрового збереження є підтримка доступності.[145] Однак, займаючись збереженням цифрових даних для цілей забезпечення юридичної звітності, мета полягає в тому, щоб керувати та підтримувати цифрові матеріали таким чином, щоб допомогти забезпечити їх доступність, достовірність та потенційне використання механізмами підзвітності, включаючи їх допустимість у судових розглядах. Таким чином, цифрове збереження в контексті розслідування передбачає збереження інформації протягом тривалого часу, щоб зібраний елемент залишався незалежно зрозумілим для передбачуваних користувачів з достатнім підтвердженням його справжності.

---

[142] Національний інститут стандартів і технологій Сполучених Штатів є однією організацією, на яку слід звернути увагу щодо діючого стандарту. Див. www.nist.gov.

[143] Ng, «Як ефективно зберігати інформацію з відкритим доступом».

[144] У тому самому місці, стор. 143. Див. Організація ООН з питань освіти, науки та культури, «Концепція збереження цифрових даних». Доступно на сторінці www.unesco.org/new/en/communication-and-information/access-to-knowledge/preservation-of-documentary-heritage/digital- heritage/concept-of-digital-preservation.

[145] Ng, «Як ефективно зберігати інформацію з відкритим доступом».

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

158. Для довгострокового збереження обладнання та формати зберігання можуть потребувати оновлення, щоб забезпечити доступність матеріалів за допомогою сучасних пристроїв.

1. Властивості цифрового елемента, які необхідно захищати та зберігати з плином часу

159. На думку архівістів, властивості цифрового елемента, які необхідно охороняти та зберігати з плином часу, включають його автентичність, доступність, ідентичність, стійкість, можливість відображення та зрозумілість, як коротко описано нижче.

(a) Автентичність

160. Автентичність – це здатність продемонструвати, що цифровий елемент залишається незмінним з моменту його збирання. Це вимагає, щоб цифровий елемент залишався незмінним під час перебування в архіві або будь-які зміни до нього були задокументовані.[146]

(b) Доступність

161. Доступність – це наявність цифрового елемента у простому значенні, що постійно існує та може бути відновленим, а також у юридичному сенсі забезпечення відповідних прав інтелектуальної власності на доступ та використання цього елемента.[147]

(c) Ідентичність

162. Ідентичність відноситься до здатності цифрового елемента бути предметом посилання. Цифровий елемент має бути ідентифікованим та відрізнятись від інших цифрових елементів, наприклад шляхом реєстрації за допомогою ідентифікатора, такого як унікальний ідентифікаційний номер.[148]

(d) Стійкість

163. Стійкість відноситься до цілісності та життєздатності цифрового елемента в технічному плані. Бітові послідовності цифрового елемента повинні бути неушкодженими, оброблятися та вилучатися.[149]

(e) Можливість відображення

---

[146] З того самого джерела. Зауважимо, що використання терміну «автентичність» у цьому контексті відрізняється від його використання в юридичному контексті.
[147] З того самого джерела.
[148] З того самого джерела.
[149] З того самого джерела.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

164. Можливість відображення означає здатність людей або машин використовувати або взаємодіяти з цифровим елементом за допомогою відповідного обладнання та програмного забезпечення.[150]

(f) Зрозумілість

165. Зрозумілість – це здатність передбачуваних користувачів інтерпретувати та розуміти цифровий елемент.[151]

2. Питання, що стосуються розслідування

166. Слідчі також повинні розглянути та спланувати конкретні питання розслідування, які можуть виникнути або виникнуть під час процесу збереження.

a) Ланцюг забезпечення збереження

167. Ланцюг забезпечення збереження – це хронологічна документація послідовності зберігачів інформації чи доказів, а також документація контролю, дати та часу, передачі, аналізу та розпорядження такими доказами. Після збору ланцюг забезпечення збереження цифрового елемента слід підтримувати шляхом встановлення належної системи цифрового збереження.

(b) Доказова копія

168. Доказова копія – це цифровий елемент, зібраний слідчим у його первісному вигляді, який не слід змінювати. Цифрові елементи слід зберігати в оригінальному вигляді. Це означає збереження чистого оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний.

(c) Робочі копії

169. Копію або копії цифрового елемента слід створити для цілей аналізу та зберігати окремо, щоб слідчі могли працювати з копією, а не з оригіналом. Це дозволяє мінімально обробляти оригінал і зменшувати ризик його компрометації або зміни. Будь-які зміни до елементу, включаючи виготовлення копій, повинні бути задокументовані. Якщо можливо, слід використовувати окремі системи зберігання для доказових копій та робочих копій.

(d) Зберігання

170. Зберігання допомагає забезпечити довготривалість цифрових елементів та можливість їх пошуку та відновлення. Зберігання слід розглядати не пасивно, а як активний процес, що включає поточні, керовані завдання та відповідальність. Він включає постійне сховище, в якому носії даних відіграють роль, а також управління ієрархією сховища,

---

[150] З того самого джерела.
[151] З того самого джерела.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

заміну носія, перевірку помилок, перевірку виправлень (перевірка, щоб переконатися, що елемент не був змінений), відновлення після аварії, а також виявлення та повернення збережених об'єктів.[152] Цифрова інформація може зберігатися на місці (онлайн чи офлайн) або поза його межами (онлайн чи офлайн).[153] Варіанти зберігання цифрового контенту включають локальний жорсткий диск або локальний знімний носій інформації; або мережевий диск, який є частиною локальної мережі або віддаленого сервера чи системи зберігання даних у хмарі. Міркування, пов'язані з вибором сховища, включають ємність сховища (простір); доступ та контроль; резервні копії; відповідний закон; та інформаційну безпеку і захист даних. Вибір сховища також повинен враховувати швидкість, доступність, вартість, стійкість, системи зберігання та пошуку.[154]

(i) Резервне копіювання

171. Якщо трапляються втрати даних або помилки, архівіст або технік може спробувати відновити дані. В ідеалі в окремому місці необхідно створити резервну копію чи дублікат даних. Експерти з інформаційних технологій рекомендують мати принаймні три копії даних принаймні у двох різних типах сховищ, при цьому принаймні одна копія має бути географічно відокремлена від інших копій.

(ii) Погіршення якості

172. Однією з проблем зберігання є те, що якість носіїв з часом погіршується. Архівісти можуть зменшити ризик виходу з ладу сховища за допомогою особливо міцних типів носіїв; проте будь-який запам'ятовуючий пристрій з часом стане дефектним, зношуватиметься або випадково вийде з ладу. Навіть без повного збою, під час розкладання збереженого носія можуть виникати помилки даних або пошкодження файлів. Тому важливо підтримувати резервні копії та регулярно контролювати інфраструктуру зберігання та постійність збережених файлів, наприклад, регулярно перевіряючи хеш-значення випадкових вибірок, щоб переконатися у відсутності погашення якості.

(iii) Застарілість

173. Цифрові файли стають застарілими, коли апаратне забезпечення, необхідне для доступу до даних, більше недоступне або не може належним чином обслуговуватися. Незалежно від того, наскільки довговічним може бути будь-який носій інформації, він також ризикує застаріти, ускладнюючи або унеможливлюючи отримання збережених даних. Таким чином, розслідування повинно гарантувати, що вони підтримують та, у разі необхідності, оновлюють носії даних, щоб підтримувати можливість відтворення та доступність даних.

(iv) Відновлення

---

[152] У тому самому місці, стор. 154.
[153] Шира Шейндлін (Shira Scheindlin) та Даніель Дж. Капра (Daniel J. Capra), Електронні відкриття та цифрові докази в двох словах (Сент-Пол, West Academic Publishing, 2009 рік), стор. 21-22.
[154] Ng, «Як ефективно зберігати інформацію з відкритим доступом», стор. 156.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

174. Цифрові файли можуть бути випадково або цілеспрямовано видалені. Коли користувач «видаляє» файл на комп'ютері, контент видаленого файлу залишається на носії даних, доки поверх нього не буде записаний інший файл.[155] Тому, чим більше активності на комп'ютері або на іншому носії інформації, тим швидше він буде перезаписаний і стане невідновлюваним. Більшість комп'ютерів мають вбудовані в операційну систему утиліти програмного забезпечення для відновлення видалених файлів. Крім того, можна придбати програмне забезпечення для відновлення даних і іноді використовувати його для «скасування видалення» файлів. Слідчим, що ведуть розслідування з використанням даних у відкритому доступі, може знадобитися допомога фахівців з інформаційних технологій для доступу до видалених даних.

(v) Оновлення

175. Оновлення передбачає копіювання контенту з одного носія інформації на інший. Воно націлене лише на застарівання ЗМІ і не є всеосяжною стратегією збереження. Оновлення, однак, слід розглядати як невід'ємну частину більшої стратегії збереження.[156]

E. Перевірка

176. Перевірка відноситься до процесу встановлення точності чи достовірності інформації, зібраної в Інтернеті. Перевірка інформації у відкритому доступі може бути здійснена як частина загальнодоступного аналізу – включаючи інформацію із закритих та конфіденційних джерел – або спиратися виключно на відкриті джерела. Перевірка ділиться на три окремі міркування: джерело, цифровий елемент або файл та контент, які слід разом розглядати та порівнювати для узгодження.

1. Аналіз джерел

177. Аналіз джерел – це процес оцінки надійності та достовірності джерела. Інтернет-середовище створює труднощі для аналізу джерел, оскільки багато джерел є анонімними або псевдонімними. Для того, щоб належним чином проаналізувати джерела інформації, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні спочатку визначити правильне джерело або джерела для аналізу, що означає віднесення інформації до її першоджерела. Аналіз віднесення означає визначення джерела цифрової інформації, яким може бути конкретний веб-сайт, передплатник чи користувач певного облікового запису чи платформи, або особистість осіб, які склали, створили чи завантажили певний контент. Аналіз віднесення не завжди можливий і може потребувати додаткових розслідувань в Інтернеті та реальному світі або розширених методів пошуку та аналізу. Хоча визначення авторства є корисним, його відсутність, як правило, не є критичним для встановлення автентичності онлайн-елемента, оскільки існують інші способи автентифікації інформації у відкритому доступі.

---

[155] Шейндлін і Капра (Scheindlin and Capra), Електронні відкриття та цифрові докази в двох словах, стор. 24.

[156] Бібліотека Університету Корнелла, «Підручник з цифрових зображень». Доступно на сторінці http://preservationtutorial.library.cornell.edu/tutorial/preservation/ preservation-03.html.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

(a) Походження

178. Походження відноситься до походження чи найдавнішого відомого існування чогось. Що стосується онлайн-контенту, то походження може позначати найпершу появу в Інтернеті або вихідний елемент до його завантаження в Інтернет. У разі онлайн-контенту краще звертатися до «першої копії, знайденої в Інтернеті», а не до «першої копії в Інтернеті», оскільки оригінал, можливо, був видалений. Навіть якщо слідчі впевнені, що вони знайшли першу версію, наприклад, відеозапису чи іншої інформації з відкритих джерел у мережі, вони не можуть бути впевнені в її походженні через наявність закритих каналів, таких як електронні листи та групи приватних повідомлень, які, можливо, були використані для обміну елементом до його публічного виходу в Інтернет.[157]

(b) Надійність

179. Історія публікацій джерела, активність в Інтернеті та присутність в Інтернеті можуть містити відповідну інформацію, яка свідчить проти чи на користь достовірності джерела. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вивчити наявність джерела в Інтернеті та історію публікацій, що може навіть допомогти виявити навмисну спробу обману. Наприклад, у разі публікацій про події в певній країні, чи вказують публікації навколо джерела на те, що він чи вона дійсно перебувають у цій країні?

(c) Незалежність та неупередженість

180. Розслідування має перевірити неупередженість джерела. Це можна зробити, переглянувши будь-які групи, організації чи асоціації, з якими пов'язані окремі особи, а також те, як вони заробляють гроші та від кого вони отримують фінансування. Чи є зв'язки чи стосунки з будь-якою зі сторін, які беруть участь у справі чи інциденті, що розслідується? Розглядаючи незалежність джерел, необхідно перевірити, чи можуть вони бути пов'язані з відповідними суб'єктами (наприклад, сторонами конфлікту). Ідеологія джерела та будь-яка групова приналежність також може мати значення. Щодо всіх джерел, слідчі повинні вивчити та виявити їх основні мотиви, інтереси чи плани, а також ступінь того, наскільки це може вплинути на їх достовірність.

(d) Специфіка

181. Чим точніша інформація та твердження, тим легше їх буде довести або спростувати. Широкі та невизначені претензії, як правило, важче критично оцінити.

(e) Згасання

---

[157] Наприклад, один користувач може надіслати фотографію електронною поштою іншому користувачу, який потім завантажує її у соціальні мережі. Таким чином, фотографія виникла у відправника електронного листа, а не у особи, що її розмістила.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

182. Тексти, складені одночасно з подіями, на які вони посилаються, вважаються більш надійними, ніж тексти, написані задовго після того, як події сталися.[158] Цей фактор може бути складним для слідчих, що ведуть розслідування з використанням даних у відкритому доступі, коли незрозуміло, коли був створений цифровий текст.

2. Технічний аналіз

183. Технічний аналіз – це аналіз самого цифрового елемента, будь то документ, зображення чи відео. Для перевірки цілісності файлу, тобто того, чи був він змінений у цифровому вигляді, маніпульований чи модифікований, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, можуть вважати за доцільне піддати його цифровій судовій експертизі, яку іноді називають цифровим слідчим аналізом. Нижче наведені складові такого аналізу.

(a) Метадані

184. Метадані – це дані, які описують та надають інформацію про інші дані. Вони можуть бути створені користувачем, який створив елемент, іншими користувачами, постачальником послуг зв'язку або будь-яким пристроєм, на якому дані створюються, передаються, отримуються або переглядаються. Метадані мають значення для опису елемента та обставин його створення, розповсюдження або зміни. Метадані можуть включати автора файлу, дату його створення, дані завантаження, зміни, розмір файлу та геодані. Метадані можуть бути вбудовані у файл, відображені на веб-сторінці або міститися у вихідному коді. Деякі метадані можуть бути видалені до або під час завантаження, або в результаті використання програм у соціальних мережах, але якщо вони доступні, їх слід переглянути, якщо вони допоможуть встановити достовірність. Оригінальні метадані можуть бути втрачені, оскільки платформи часто перекодують завантажені носії, щоб оптимізувати їх для перегляду, обміну чи відтворення в Інтернеті. У таких випадках метадані будуть відображенням нового файлу, а не оригіналу. Якщо метадані були вилучені, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні шукати інші способи перевірки елемента.

(b) Дані формату файлу зображень, що обмінюються

185. Формат файлу зображень, що обмінюються – це тип метаданих, що визначає формати зображень, звуку та допоміжних тегів, які використовуються цифровими камерами, сканерами та іншими системами, що обробляють зображення та звукові файли, записані цифровими камерами.

(c) Вихідний код

---

[158] Інститут міжнародних кримінальних розслідувань, Посібник для слідчих, 5-е вид. (Гаага, 2012 рік), стор. 88.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

186. Вихідний код – це програмування за будь-якою веб-сторінкою або програмним забезпеченням. Що стосується веб-сайтів, цей код може переглядати будь-хто, використовуючи різні інструменти, навіть сам веб-браузер.

Вихідний код веб-сайту легко переглянути за допомогою ряду вільно доступних інструментів. Він може містити метаконтент або прихований або змінений контент, а також відображатиме структуру посилань та непрацюючі посилання.

3. Аналіз контенту

187. Аналіз контенту – це процес, за допомогою якого оцінюється достовірність та справжність інформації, що міститься у відео, зображенні, документі чи заяві. Аналіз контенту так само багатогранний і включає аналіз візуальних підказок або, наприклад, підтвердження зображення метаданими. Характеристики Інтернет-середовища породжують численні проблеми, які можуть вплинути на фактичну чи уявну достовірність чи справжність інформації з відкритих джерел у мережі. До них належать кругові звіти, деконтекстуалізація інформації та неправильне тлумачення. Дані контенту – це дані, що містяться в цифровому елементі, такі як відео, зображення, аудіозапис, документ або неструктурований текст.

(a) Унікальні ідентифікатори

188. У разі отримання завдання про перевірку візуального контенту слідчі повинні почати з пошуку унікальних чи ідентифікуючих ознак. Такі особливості можуть включати будівлі, рослинний і тваринний світ, людей, символи та знаки розрізнення. Особливу обережність слід застосовувати при аналізі людських особливостей з метою ідентифікації конкретної особи.[159] Практики ідентифікації зазвичай вимагають специфічних навичок, таких як ті, що набуваються з плином часу та шляхом спеціалізованої підготовки судового експерта. Непрофесійний аналіз може бути неточним, завдати шкоди та/або в інший спосіб бути проблематичним, якщо його проводитимуть непідготовлені фахівці.

(b) Інформація, що об'єктивно перевіряється

189. Часто може бути корисно почати з визначення того, що може кваліфікуватися як «інформація, що об'єктивно перевіряється». Наприклад, погода в певний день, прізвище та звання командира чи місцезнаходження будівлі можуть бути об'єктивно перевіреними.

---

[159] Судовий аналіз та ідентифікація людських особливостей за допомогою інструментів або людського аналізу (наприклад, розпізнавання обличчя, аналіз ходи тощо) потребують навичок судового експерта. Див. Ніна М. ван Мастрігт (Nina M. van Mastrigt) та ін., «Критичний огляд використання та наукових основ криміналістичного аналізу ходи», Forensic Sciences Research, том 3, № 3 (2018 рік), стор. 183-193 (доступно за посиланням www.tandfonline.com/doi/full/10.1080/20961790.2018.1503579); Royal Society and Royal Society of Edinburgh, «Криміналістичний аналіз ходи: буквар для судів» (Лондон, 2017 рік) (доступно за посиланням: https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf). Див. також Європейська мережа судових експертиз, Посібник з найкращої практики порівняння зображень обличчя (2018 рік) (доступний за посиланням http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf); Національний центр аудіо та відео криміналістики, «Аналіз висоти відеоспостереження» (доступно за посиланням https://ncavf.com/what-we-do/forensic-height-analysis).

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Оцінка матеріалу у відкритому доступі повинна включати перевірку його змісту щодо такої інформації, яка має об'єктивно перевірятися.

(c) Геолокація

190. Геолокація – це ідентифікація або оцінка розташування об'єкта, діяльності чи місця, з якого створено елемент. Наприклад, можна визначити місце, з якого було знято відео чи фотографію, завантажену з Інтернету, за допомогою методів геолокації. Такі методи можуть включати, наприклад, визначення унікальних географічних об'єктів на фотографії та їх фактичного розташування на карті.

(d) Хронолокація

191. Хронолокація – це підтвердження дат і часу подій, зображених у частині інформації, як правило, у візуальному образі. Наприклад, можна визначити час доби, коли була зроблена фотографія, вивчивши довжину тіней, зроблених сонячним світлом, разом з іншими показниками.

(e) Повнота

192. Неповний документ або відеокліп все ще можуть бути доказовими, однак розрив(и) може вплинути на вагу, яка може бути привласнена елементу. Тому при зборі інформації у відкритому доступі важливо повністю захопити цільовий файл і, коли це необхідно, захопити навколишній контекст.

(f) Внутрішня узгодженість

193. Оцінка внутрішньої узгодженості може бути здійснена стосовно однієї інформації з відкритого джерела в Інтернеті або стосовно масиву інформації з певного джерела (та/або джерел з однаковим походженням чи авторством). Оцінка внутрішньої узгодженості окремої інформації в Інтернеті має на меті встановити, чи є інформація послідовною на її власних умовах. Внутрішньо послідовна частина або сукупність інформації не повинна суперечити сама собі.

(g) Зовнішнє підтвердження

194. Зовнішнє підтвердження забезпечується інформацією, яка лежить за межами самого цифрового елемента, але збігається з його контентом і, таким чином, підтверджує достовірність контенту елемента.

F. Слідчий аналіз

195. Слідчий аналіз – це практика перегляду та інтерпретації фактичної інформації для опрацювання істотних висновків, що мають значення для прийняття рішень або розробки справ. Обсяг та різна якість інформації у відкритому доступі вимагає добре структурованого підходу до аналізу.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

196. Перш ніж пройти певні види аналізу, можливо, спочатку потрібно обробити інформацію у відкритому доступі. Обробка може включати переклад іноземних мов або сукупність різних наборів даних для аналізу поведінки окремих осіб, місцезнаходжень та об'єктів, а також відносин чи мереж, рухів, діяльності чи транзакцій. Це також може включати зміну характеру або формату цифрового елемента, щоб зробити його сумісним із певним програмним забезпеченням. Поширені типи обробки даних включають:

(a) Переклад: якщо дані складені мовою, якою не розмовляють слідчі або яка не обробляється програмним забезпеченням, необхідним для ознайомлення з матеріалом, дані можуть бути перекладені перед подальшими кроками;

(b) Агрегування: слідчим може знадобитися об'єднати різні набори даних в один більший набір даних для їх аналізу;

(c) Переформатування: для полегшення пошуку або повторного використання даних слідчим може знадобитися змінити формат цифрового елемента.

197. Доцільно обробляти лише робочі копії цифрового елемента, на відміну від оригіналу або доказової копії. Будь-яка обробка цифрового елемента повинна бути задокументована. Якщо дослідники використовують цифрові технології для обробки даних, наприклад, аналізу даних за допомогою алгоритмів, включаючи обробку природної мови та глибоке вивчення, вони повинні усвідомлювати ризик упередженості при обробці таких даних.

198. Після обробки інформація може бути проаналізована. Продукти аналітичної роботи з відкритою інформацією будуть змінюватися залежно від мети, типу та обсягу вихідної інформації, що лежить в основі, строку виробництва та аудиторії. Вони будуть розроблені відповідно до потреб розслідування і можуть включати схеми, резюме, глосарії, словники та наочні посібники, включаючи карти та навчання.[160]

199. Слідчі повинні застосовувати жорсткі стандарти для забезпечення об'єктивності, своєчасності, актуальності та точності даних та висновків, що містяться в аналітичних продуктах, а також для захисту конфіденційності та інших міркувань щодо прав людини, особливо при роботі з особистою інформацією. Така інформація повинна бути включена лише до продуктів, на які слідчі отримали згоду залучених осіб, і вона служить прямій меті розслідування. Її також слід розглядати у світлі юридичних та етичних обмежень, що стосуються його використання.[161]

200. Наступні розділи містять загальні типи аналізу, які можуть бути використані для подальших цілей розслідування з використанням інформації у відкритому доступі.

1. Аналіз порівняння зображень/відео

---

[160] Див. главу VII нижче про звітність про результати.
[161] Див. главу III вище про нормативно-правову базу.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

201. Порівняльний аналіз або наука порівняння – це процес порівняння ознак об'єктів, осіб та/або місцезнаходжень з іншими невідомими та/або відомими об'єктами, коли хоча б один із предметів, про які йде мова, є зображенням. Це аналіз змісту зображень та відео, включаючи елементи порівняння між різними предметами та функціями, а також їх якість зображення та візуальні налаштування (світло, перспектива тощо). Хоча зараз багато мирян знають основи аналізу порівняння зображень, допомога експерта, який має кваліфікацію та сертифікацію судово-відеоаналізу та/або цифрової криміналістики, може допомогти у наданні наукового аналізу, включаючи висновок експерта. Для розслідувань у сфері прав людини та інших видів розслідувань також може використовуватися така експертиза для надання додаткової ваги їхнім висновкам.

2. Аналіз інтерпретації зображень/відео

202. До порівняння зображення/ відео відноситься аналіз інтерпретації зображення/ відео, який передбачає аналіз цифрового елемента, щоб зрозуміти його візуальний контент. Наприклад, аналіз пострілів, поранень, крові, транспортних засобів, зброї та військових засобів або аналіз швидкості руху транспортного засобу або віку окремої особи – це частина аналізу інтерпретації зображення/відео. Це може бути зроблено аналітиками для цілей розслідування або судово-медичними експертами у разі встановлення фактів у судовому процесі або висновків щодо прав людини.

3. Просторовий аналіз

203. Просторовий аналіз або геопросторовий аналіз може включати візуальний аналіз контенту та аналіз метаданих для елементів, які пропонують географічні координати або назви місць. Просторовий аналіз передбачає вивчення різних об'єктів та ландшафтних об'єктів з належною роздільною здатністю та перевірку на основі супутникових чи інших зображень, геоданих та карт, належного знання випадку та контексту та інструментів геоінформаційної системи.[162]

4. Відображення суб'єктів

204. Відображення суб'єктів – це техніка для розуміння ключових суб'єктів та визначення відносин влади та каналів впливу.[163] Таким чином, воно починається з визначення ключових суб'єктів, а потім – визначення стосунків між ними.

5. Аналіз соціальних мереж

205. Подібно до відображення суб'єктів, аналіз соціальних мереж – це відображення та вимірювання відносин між людьми, групами, організаціями, комп'ютерами, URL-адресами та іншими пов'язаними об'єктами інформації/знань.[164] Люди та групи часто згадуються як вузли, тоді як посилання показують зв'язок між вузлами. Аналіз соціальних мереж

---

[162] Геоінформаційна система – це комп'ютеризована база даних для управління та аналізу просторових даних.

[163] УВКПЛ, Посібник з моніторингу прав людини, глава 8 про аналіз, стор. 24.

[164] Orgnet, «Аналіз соціальних мереж: вступ». Доступно на сторінці www.orgnet.com/sna.html.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

використовує зв'язки в соціальних медіа та інших мобільних чи веб-платформах для встановлення та розуміння стосунків між окремими людьми. Аналіз даних про з'єднання або посилання може проводитися дослідником вручну або за допомогою програмного забезпечення для аналітики.

6. Відображення інцидентів

206. Відображення інцидентів – це аналітичний прийом, що використовується для встановлення часових та географічних зв'язків між різними інцидентами, який у контексті міжнародних кримінальних порушень та прав людини може стосуватися місця таких порушень чи злочинів, включаючи попередні та наступні події. Він також може включати в себе відображення інших відповідних подій, наприклад, де і коли були зроблені заяви передбачуваних злочинців.

7. Аналіз картини злочину/порушення

207. У контексті національних правоохоронних органів, картина злочину – це група з двох або більше злочинів, про які повідомляється або які виявляються правоохоронними органами, які є унікальними, оскільки вони мають принаймні одну спільність у типі злочину; поведінка правопорушників або жертв; характеристики злочинців, жертв чи цілей; вилучене майно; або місця події.[165] Аналогічно, злочини та порушення можуть бути встановлені у міжнародних кримінальних справах та справах у сфері прав людини на основі інформації у відкритому доступі.

---

[165] Міжнародна асоціація аналітиків злочинності, «Визначення картин злочинів для тактичного аналізу», Біла книга Комітету зі стандартів, методів та технологій 2011-01, стор. 1.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

VII

ЗВІТУВАННЯ ПРО ВИСНОВКИ

РЕЗЮМЕ ГЛАВИ

- Результати розслідування з використанням даних у відкритому доступі, що стосуються або зібраних даних, або висновків, зроблених із цих даних, можна повідомляти усно, візуально або письмово.

- Слідчі повинні враховувати, які формати є найбільш прийнятними для їхніх мандатів та цільової аудиторії – беручи до уваги такі фактори, як технологічна грамотність аудиторії та доступність, об'єктивність, прозорість та безпека – при прийнятті рішення щодо (a) форматів, які будуть використовуватися, та (b) даних, які потрібно включити.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

208. У цій главі описуються способи, за допомогою яких можуть бути представлені або повідомлені результати розслідувань з використанням даних у відкритому доступі, включаючи методології, необроблені дані та аналітичні результати. У багатьох випадках інформація у відкритому доступі буде представлена разом з іншою інформацією, зібраною за допомогою інших методів розслідування. Презентації можуть мати різні форми, включаючи письмові, усні або візуальні звіти, або будь-яку комбінацію цих форм. Звіти можуть бути призначені для внутрішнього використання або для зовнішньої публікації і можуть розглядатися як експертні чи неекспертні залежно від ряду факторів. Звіти повинні забезпечувати такі елементи:

(a) Точність: звіти повинні точно відображати зібрані дані.[166] Необхідно включити виправдовувальну інформацію, а також пояснення щодо будь-яких виправлень або прогалин;

(b) Віднесення: у звітах слід чітко розрізняти вміст, що знаходиться у суспільному надбанні, або загальну некласифіковану інформацію, інформацію, яка є засекреченою чи іншим чином обмеженою, та контент, що відображає судження чи думку слідчих та/або інших фахівців. Слідчі або інші особи, які повідомляють про інформацію у відкритому доступі, також повинні пройти належну перевірку та отримати належні дозволи на використання вмісту, який може належати іншим, наприклад, шляхом забезпечення будь-яких необхідних прав інтелектуальної власності;

(c) Повнота: результати повинні вказувати на повноту базових даних, особливо якщо дані навмисно виключені;

(d) Конфіденційність: незважаючи на те, що вони знаходяться у відкритому доступі, у звітах слід враховувати, які матеріали слід залишити або відредагувати, щоб захистити конфіденційність або іншим чином мінімізувати ризики, зокрема потенційні ризики для джерел, свідків, жертв та членів спільнот, пов'язаних із інформацією у відкритому доступі;

(e) Мова: у звітах слід використовувати нейтральну мову та уникати емоційної мови. Вони повинні чітко викладати факти, не зловживаючи прикметниками чи наголосами. Звіти повинні бути написані гендерно чутливою мовою. В ідеалі публічні звіти мають бути доступними мовами постраждалих громад на додаток до будь-яких офіційних мов, якими користуються слідчі або слідчі органи;

(f) Прозорість: у звітах має бути чітко зазначено, як слідчі виконували свою роботу, їх цілі, процеси та методи. Як правило, це буде включено до розділу методології звіту, але воно також повинно направляти описи у всьому тексті. Описи повинні бути максимально прозорими, не створюючи вразливостей безпеки, наприклад, шляхом розкриття конфіденційної інформації.

A. Письмова звітність

---

[166] Див. главу II.B вище про методологічні принципи.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

209. Розслідування з використанням даних у відкритому доступі може бути представлене у письмовій формі, яке може включати внутрішні звіти та звіти для клієнтів, а також публічні звіти. Одним із способів передачі аналітичних висновків є письмовий звіт, який може включати звіти громадських організацій, слідчих комісій, місій з встановлення фактів та Організації Об'єднаних Націй, а також звіти експертів для суду чи трибуналу.[167] Цифрова інформація у відкритому доступі часто буде інтегрована з іншими формами відкритих та закритих вихідних даних та аналізу. У письмових звітах слід аналізувати зібрану інформацію, щоб зробити логічні висновки, оцінки та прогнози. Звіти повинні відображати обґрунтовану методологію та мати можливість пояснити цю методологію цільовій аудиторії. Достовірність та цілісність основної інформації у звіті має вирішальне значення. Неправильні дані призведуть до поганих висновків.[168]

210. Письмові звіти повинні містити наступні розділи, якщо немає обґрунтованої та чітко сформульованої причини, щоб, наприклад, не зберігати конфіденційність деяких методів, технологій та джерел розслідування в Інтернеті:

(a) Слідчі цілі: звіти повинні містити цілі розслідування та основні повноваження чи вказівки клієнта, включаючи чітко визначені, чітко сформульовані запитання дослідження;

(b) Методологія: звіти повинні включати методи дослідження, щоб забезпечити повторність та дозволити аудиторії зрозуміти та оцінити достовірність інформації та результатів розслідувань, включаючи те, що охоплюється;

(c) Виконана діяльність: звіти повинні містити резюме виконаної діяльності, яка є суттєвою для висновків або оцінки якості аналізу, включаючи заходи щодо виявлення основних даних, того, що було зібрано та що проаналізовано;

(d) Основні дані та джерела: звіти повинні містити опис базових даних, включаючи джерела та їх якість;

(e) Прогалини або невизначеності: звіти повинні визначати будь-які прогалини або невизначеності в базових даних або аналізі, які можуть бути істотними для висновків;

(f) Результати та рекомендації: звіти повинні містити тлумачення дослідниками даних або висновків на основі аналізу даних, з огляду на застереження та нові підказки.

B. Усна звітність

211. Якщо висновки розслідування з використанням даних у відкритому доступі потраплять до зали суду, слідчим, можливо, доведеться дати свідчення як свідкам; таким

---

[167] Приклад письмового звіту про цифрові дані у відкритому доступі див., наприклад, у Human Rights Investigations Lab, «Хімічні удари по Аль-Латаміні: 25 і 30 березня 2017 року – дослідження з використанням даних у відкритому доступі під керівництвом студентів» (Берклі, Центр з прав людини, Каліфорнійський університет, Берклі, Юридична школа, 2018 рік).

[168] Виходячи з обставин та вимог конфіденційності, рекомендується експертна перевірка для забезпечення точності та якості даних, а також аналізу та висновків, отриманих із цих даних.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

чином, представляючи свої розслідування через усні свідчення. Інші форми усного звітування можуть включати доповіді перед комісіями з встановлення правди, форумами громадських організацій, народними трибуналами або на заходах у засобах масової інформації.

212. Кожен, кому потрібно усно представити результати свого розслідування з використанням даних у відкритому доступі, повинен мати можливість чітко і точно пояснити роботу, включаючи застосовану методологію та використані інструменти. Це забезпечить належне врахування усних свідчень та описаних висновків.

213. Що стосується судових розглядів, то часто саме керівники розслідувань мають надавати свідчення, і вони повинні мати можливість говорити про роботу своїх команд. Це, звичайно, вимагає, щоб вони знали, що зробили їхні команди, і могли відповідати на запитання про виконувану роль та обґрунтування, що лежать в основі прийняття будь-яких рішень щодо обсягу розслідування, його методів, використаних інструментів тощо. Слідчі можуть бути або свідками-експертами або звичайними свідками. Свідки-експерти – свідки, які вважаються експертами через їх досвід, знання, вміння, підготовку, освіту або пов'язані з ними повноваження – можуть свідчити про висновки, до яких вони дійшли, та інші результати аналітичної роботи. Звичайні свідки, як правило, обмежуються свідченнями про факти і, зокрема, ті, які вони особисто спостерігали.

C. Візуальна звітність

214. Візуалізація даних – це графічне представлення інформації у вигляді, наприклад, діаграм, графіків, таблиць, карт та інфографіків, які забезпечують доступний спосіб побачити та зрозуміти тенденції, відмінні риси та закономірності у даних.[169] Вона може включати діаграми та інші графічні зображення даних у просторі та часі; графіки (у тому числі ті, що демонструють математичні зв'язки, тенденції чи взаємозв'язки); мережеві графіки, які демонструють відносини між різними людьми; та статистичні діаграми та схеми. Двовимірні та тривимірні карти для візуалізації об'єктів у просторі та часі та тривимірна реконструкція різних місць, включаючи місця злочину, також є частиною репертуару візуалізації даних.[170] Ці інструменти можуть бути корисними для розуміння

---

[169] Приклади візуальної звітності в різних контекстах включають цифрові платформи, які використовуються як показові докази у справі «Прокурор проти Ахмада Аль Факі Аль Махді (Ahmad Al Faqi Al Mahdi)» у Міжнародному кримінальному суді та Прокурор проти Саліма Джаміля Айяша (Salim Jamil Ayyash) та ін. у Спеціальному трибуналі по Лівану; звіт детальних висновків незалежної міжнародної комісії з розслідування протестів на окупованій палестинській території (доступно за посиланням www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf); BBC Africa Eye, «Звірство Камеруну: те, що сталося після того, як «Африканське око» знайшло, хто вбив цю жінку», BBC News, 30 травня 2019 року (доступно за посиланням www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman). Дивіться також, загалом, роботу Forensic Architecture and SITU Research.

[170] Див., наприклад, Цифрову платформу Міжнародного кримінального суду: Тімбукту, Малі (розроблено SITU Research як актив для справи Аль-Махді (Al Mahdi) у Міжнародному кримінальному суді). Доступно на сторінці http://icc-mali.situplatform.com. Дивіться також різноманітні онлайн-розслідування з використанням даних у відкритому доступі та їх візуальні звіти в Forensic Architecture. Доступно на сторінці at https://forensic-architecture.org/methodology/osint.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

великої кількості даних, що часто трапляється у розслідуваннях з використанням даних у відкритому доступі, або для кращого розуміння складних фактичних сценаріїв.

215. Інші види візуалізації даних включають:

(a) Інтелект-карти: інтелект-карта – це графічний засіб представлення ідей та концепцій та їх співвідношення один з одним. Інтелект-карти структурують інформацію таким чином, що полегшує її аналіз, синтез та розуміння. Інтелект-карти часто включають пояснення того, як були виявлені основні дані;

(b) Блок-схеми: блок-схема – це графічне зображення послідовності подій, таких як етапи, вбудовані в алгоритм, робочий процес або подібні процеси;

(c) Інфографіка: інфографіка – це ілюстроване зображення ідеї чи концепції; його можна використовувати для представлення статистичної інформації.

216. Інформація у відкритому доступі може бути представлена різними способами, починаючи від аудіовізуального відображення окремого відео чи веб-сайту до інтерактивних, цифрових та сукупних мультимедійних презентацій.[171] Візуальні демонстрації та ілюстрації, або цифрові платформи, можуть бути використані для відображення інформації таким чином, щоб полегшити розуміння цільовою аудиторією основних фактів. Приклади включають часові шкали, складені фотографії (наприклад, 360-градусний вигляд місця злочину) та відредаговані відео.

217. У разі представлення візуалізації даних та мультимедійних доказів у залі судового засідання або іншим публічним аудиторіям слідчі повинні розуміти, які технічні проблеми можуть виникнути, зокрема, які платформи можуть знадобитися для того, щоб їх презентації були максимально корисними для тих, хто встановлює факти. При виборі оптимальної форми представлення базових даних слід враховувати цілий ряд факторів. Такі фактори включають передбачувану аудиторію та її рівень комфорту з можливими форматами та їх здатність розуміти інформацію, що передається.[172] Зрештою, усі презентації мають сприяти досягненню мети висвітлення фактів, що мають значення у

---

[171] Незважаючи на те, що вони не передбачені для суду, Команда візуальних розслідувань New York Times підготувала ряд візуальних пояснювачів, призначених для узагальнення інформації у відкритому доступі в Інтернеті, підтримки аналізу складних інцидентів та звітування про ці висновки. Див., наприклад, Ніколас Кейсі (Nicholas Casey), Крістоф Кеттл (Christoph Koettl) та Дебора Акоста (Deborah Acosta), «Кадри суперечать твердженню США про те, що Ніколас Мадуро (Nicolas Maduro) спалив конвой з допомогою», New York Times, 10 березня 2019 року (доступно за посиланням www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html); Малахі Браун (Malachy Browne) та інші, «10 хвилин. 12 пострілів. 30 відео. Картографування розправи в Лас-Вегасі», New York Times, 21 жовтня 2017 року (доступно за посиланням www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

[172] Див. Алекса Кеніг (Alexa Koenig), «Докази у відкритому доступі та випадки у сфері прав людини: сучасна соціальна історія», у Digital Witness: Використання інформації у відкритому доступі для розслідування, документації та підзвітності в області прав людини, Сем Дабберлі (Sam Dubberley), Алекса Кеніг (Alexa Koenig) та Дараг Мюррей (Daragh Murray), ред. (Оксфорд, Oxford University Press, 2020 рік), стор. 38-40.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

справі, у спосіб, який є доказовим та не завдає шкоди і має відповідати юридичним та етичним вимогам юрисдикції, в якій подається інформація.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

VIII

ГЛОСАРІЙ

РЕЗЮМЕ

■ Терміни та визначення, що використовуються у розслідуваннях з використанням даних у відкритому доступі, або ті, які можуть виникнути у відповідних чи пов'язаних ресурсах.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

218. Ця глава містить терміни та визначення, які можуть бути корисними для слідчих, що ведуть розслідування з використанням даних у відкритому доступі. Не всі терміни використовуються у Протоколі, але включені, оскільки вони можуть виникати у відповідних або пов'язаних ресурсах.

Повітряний проміжок: коли цифровий пристрій не має прямого підключення до Інтернету або будь-якої мережі, що забезпечує безпеку інформації, яка зберігається на цьому пристрої.

Алгоритм: чітко визначена процедура або набір інструкцій, що дозволяє комп'ютеру вирішити проблему або реагувати на заздалегідь визначений сценарій.

Анонімізація: процес унеможливлення ідентифікації конкретної особи.

Інтерфейс прикладного програмування (API): код, який дозволяє програмним комп'ютерним програмам спілкуватися між собою.

Штучний інтелект (ШІ): галузь інформатики, присвячена розробці програмування для машин, щоб навчитися реагувати на невідомі змінні та адаптуватися до нового середовища.

Маячок: механізм відстеження активності та поведінки користувачів. Маячки зроблені з невеликого і ненав'язливого (часто непомітного) елемента на веб-сторінці (розміром лише одного прозорого пікселя), який, коли він відображається браузером, повідомляє деталі про браузер та комп'ютер, що використовується, третій стороні.

Великі дані: великі набори даних, які можна проаналізувати, щоб виявити кореляції між точками даних та виявити закономірності, які можуть допомогти у прогнозуванні. Ключовими характеристиками великих даних є обсяг і складність.

Блокчейн: технологія, заснована на криптографії, за допомогою якої відкрита, розподілена книга, що складається з «блоків», може бути використана для ефективного та перевіреного та постійного запису транзакцій між двома сторонами чи організаціями.

Логічний пошук: техніка пошуку в Інтернеті, що дозволяє користувачам поєднувати ключові слова з операторами або модифікаторами (тобто І, НІ, АБО), щоб звузити результати пошуку і тим самим надати більш релевантні та конкретні результати пошуку.

Captcha: абревіатура повністю автоматизованого публічного тесту Тьюринга для розрізнення комп'ютерів та людей – це тип перевірки відповіді на виклик, який використовується в обчисленні для визначення того, чи є користувач людиною.

Чат-кімната: веб-сайт в Інтернеті, що дозволяє користувачам вести онлайн-розмови в режимі реального часу.

Хмарні обчислення: модель операцій, яка дозволяє зберігати, обробляти та аналізувати дані через інтрамережу або Інтернет. Існує три типи хмар: приватна, загальнодоступна та гібридна.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Cookie: невеликий фрагмент даних, який надсилається веб-сайтом і зберігається в пам'яті комп'ютера користувача або записується на диск комп'ютера для використання браузером. Файли cookie часто необхідні для ефективного функціонування веб-сайту – вони дають можливість зберігати налаштування веб-сайту користувача та дані про особисті дані, усуваючи необхідність постійного введення даних користувачами під час їх наступних відвідувань.

Криптографічний підпис: математичний процес перевірки справжності цифрового елемента. За допомогою алгоритму можна створити два ключі, які математично пов'язані: один приватний та один відкритий. Для створення цифрового підпису використовується програмне забезпечення для створення хешу електронних даних. Потім приватний ключ використовується для шифрування хешу.

Криптографія: практика цифрового кодування або декодування інформації.

Тіньовий Інтернет: та частина Інтернету, яка доступна лише за допомогою спеціального програмного забезпечення, що дозволяє користувачам та операторам веб-сайтів залишатися анонімними та не підлягати відстеженню.

Видобуток даних: практика вивчення та вилучення даних з баз даних з метою отримання знань або нової інформації.

Цифровий архів: колекція документів, веб-сторінок або електронних записів. Цей термін також може стосуватися офіційної чи неформальної організації, яка бере на себе відповідальність за збереження інформації та надання її доступним авторизованим користувачам.

Цифрове збереження: політика та стратегії, необхідні для управління та підтримки цифрової інформації з постійною цінністю з плином часу, щоб цифрова інформація була доступною та корисною для її цільових користувачів у майбутньому.

Доменне ім'я: мітка, яка ідентифікує мережевий домен. В Інтернеті доменні імена формуються за правилами та процедурами Системи доменних імен (DNS). Загалом, доменне ім'я являє собою ресурс Інтернет-протоколу (IP), такий як персональний комп'ютер, що використовується для доступу до Інтернету, сервер, на якому розміщено веб-сайт, сам веб-сайт або будь-який інший сервіс, що передається через Інтернет.

Реєстрант доменного імені: особа, компанія чи інша організація, яка має або володіє доменним іменем.

Система доменних імен (DNS): система, за допомогою якої регулюється призначення доменних імен.

Dragnet: у контексті онлайн широка автоматизована система збору чи спостереження.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Вбудовані дані: дані, що зберігаються у вихідному файлі або на веб-сторінці.

Шифрування: процес унеможливлення доступу до даних без ключа дешифрування.

Хеш або значення хешу: обчислення, які можна виконати для будь-якого типу цифрового файлу для створення буквено-цифрового рядка фіксованої довжини, який можна використовувати як доказ того, що цифровий файл не був змінений. Цей рядок залишатиметься незмінним під час кожного обчислення, поки файл не зміниться.

Мова розмітки гіпертексту (HTML): мова програмування, яка використовується для створення веб-сторінок, доступ до яких здійснюється за допомогою браузера.

Протокол передачі гіпертексту (HTTP): протокол, що лежить в основі Інтернету та визначає спосіб передачі та прийому даних.

Орган з присвоєння номерів в Інтернеті (IANA): організація, яка контролює глобальне розподіл IP-адрес, номерів автономних систем та систем доменних імен.

Інтернет-корпорація з присвоєння імен та номерів (ICANN): організація, відповідальна за забезпечення стабільної та безпечної роботи Інтернету шляхом координації обслуговування та процедур кількох баз даних, пов'язаних із іменами та числовими просторами Інтернету.

Інтернет-форум (також відомий як дискусійний клуб): веб-сайт, за допомогою якого користувачі можуть розміщувати повідомлення та вести бесіди. Форуми зазвичай містять довші повідомлення, ніж ті, що зустрічаються в чат-кімнатах, і мають більшу ймовірність архівації контенту.

Адреса Інтернет-протоколу (IP): будь-який цифровий пристрій, що підключається до Інтернету, має IP-адресу. Існує два типи IP-адрес: IPv4 (32-бітне число) та IPv6 (128-бітове число). IP-адресу можна використовувати для ідентифікації комп'ютерів та інших пристроїв в Інтернеті.

Постачальник послуг Інтернету (ISP): організація, яка надає користувачам Інтернету послуги для доступу та використання Інтернету.

Інтранет: приватна комп'ютерна мережа, яка використовує протоколи Інтернету та підключення до мережі для створення власної версії Інтернету.

Локальна мережа (LAN): сукупність цифрових пристроїв, підключених до однієї мережі в певному фізичному місці.

Машинне навчання: тип штучного інтелекту, який використовує статистичні методи, щоб надати комп'ютерам можливість «вчитися» на основі даних, без явного програмування.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Шкідливе програмне забезпечення: шкідливе програмне забезпечення, призначене для заподіяння шкоди цифровому пристрою, мережі, серверу чи користувачеві. Існує багато різних типів шкідливих програм, включаючи віруси, трояни, програми-вимагачі, рекламне та шпигунське програмне забезпечення.

Метадані: це дані про дані. Вони містять інформацію про електронний файл, який або вбудований у файл, або пов'язаний з ним. Метадані часто містять характеристики та історію файлу, такі як його назва, розмір та дати створення та модифікації. Метадані можуть описувати, як, коли і ким було зібрано, створено, доступно, змінено та відформатовано цифровий файл.
Редаговний файл: файл у вихідному форматі.

Портативний формат документів (PDF): формат файлу з фіксованим макетом, який зберігає формат документа (включаючи шрифти, інтервали та зображення) незалежно від програмного забезпечення, обладнання та операційних систем, що використовуються для відкриття та перегляду цього документа. Перетворення файлу з вихідного формату в PDF видаляє його метадані, забезпечуючи статичне зображення документа.

Діагностичне програмне забезпечення: програмне забезпечення, яке використовує алгоритми прогнозування та машинне навчання для аналізу даних для прогнозування майбутнього чи невідомих подій чи поведінки.

Псевдонімізація: обробка персональних даних у такий спосіб, щоб інформація більше не могла бути віднесена до певного суб'єкта даних без використання додаткової інформації.

Скрейпінг: метод вилучення масової кількості даних з веб-сайтів.

Соціальна інженерія: психологічна маніпуляція людиною з метою отримання несанкціонованого доступу до інформації. Це схоже на хакерство, але передбачає використання людської вразливості, а не технічної. Існує багато різних типів соціальної інженерії, включаючи фішинг та цільовий фішинг.

Стрипінг: технологічний процес видалення метаданих з файлу без перетворення цього файлу в інші формати.

Структуровані дані: дані або інформація, що відповідає жорсткому формату у сховищі (зазвичай це база даних, але також може бути набором заповнених форм), щоб її елементи були легко доступні для обробки та аналізу.

Поверхневий Інтернет: та частина Інтернету, до якої можна отримати доступ за допомогою будь-якого браузера та здійснювати пошук за допомогою традиційних пошукових систем.

Трекер: тип файлу cookie, який використовує здатність веб-браузера зберігати записи про те, які веб-сторінки були відвідані, які критерії пошуку введені тощо.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Дані про трафік: будь-які дані, оброблені з метою передачі інформації в мережі електронних комунікацій або для виставлення рахунків за цей зв'язок. Такі дані включають дані, що стосуються маршрутизації, часу або тривалості зв'язку.

Єдиний локатор ресурсів (URL): розташування веб-сторінки в Інтернеті. Це те саме, що і веб-адреса.

Неструктуровані дані: дані та інформація, які надходять у різних формах, які не впорядковані у жорсткому форматі і тому їх нелегко обробляти та аналізувати. Зазвичай вони є текстовими, але можуть також включати файли зображень, аудіо та відео.

Віртуальна машина: програмне забезпечення, яке імітує комп'ютерну систему.

Віртуальна приватна мережа (VPN): захищена мережа або система захищених вузлів, які використовують шифрування та інші процеси безпеки, щоб забезпечити доступ до мережі лише авторизованим користувачам. VPN маскують IP-адресу і запобігають перехопленню даних.

Постачальник веб-послуг: організація, що надає послуги та продукти в Інтернеті, наприклад, компанія соціальних медіа.

Веб-сканер (також відомий як веб-павук або павук-робот): програма, яка систематично переглядає Інтернет відповідно до автоматизованого скрипта для завантаження та індексування відвідуваних веб-сайтів.

WHOIS: запис, який ідентифікує, кому належить певне доменне ім'я на основі організації, яка його зареєструвала. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, можуть використовувати інструмент пошуку WHOIS як частину процесу аналізу та перевірки джерел.

Всесвітня павутина (WWW): інформаційний простір, у якому документи та інші веб-ресурси ідентифікуються за URL-адресами, які можуть бути пов'язані між собою гіпертекстом і доступні через Інтернет. Користувачі можуть отримати доступ до ресурсів Всесвітньої павутини за допомогою програмного забезпечення під назвою веб-браузер.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

ДОДАТКИ

РЕЗЮМЕ

- Шаблон плану онлайн-розслідування
- Шаблон оцінки цифрових загроз та ризиків
- Шаблон оцінки цифрового середовища
- Онлайн-форма збору даних
- Міркування щодо перевірки нових інструментів

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Додаток І

Шаблон плану онлайн-розслідування

Довідковий номер розслідування:

Дата оцінки:

Короткий опис розслідування: *предмет, територіальний та часовий обсяг розслідування*

1. Цілі та заплановані заходи

Сюди входять цілі та стратегія онлайн-розслідування, а також конкретні заходи зі строками їх реалізації.

2. Резюме оцінки цифрового середовища

Сюди входить оцінка цифрового середовища на географічній території, що є предметом розслідування, наприклад, популярних соціальних медіа, мобільних додатків та інших технологій, а також того, хто має доступ до цих технологій та використовує їх.

3. Стратегія зменшення ризиків та заходи захисту

Сюди входять основні висновки оцінки цифрової загрози та ризиків, а також стратегія виявлення, управління та реагування на такі загрози.

4. Відображення відповідних суб'єктів

Сюди входить перелік осіб, що приймають перші відповідні заходи, які, можливо, зібрали потенційно відповідний онлайн-контент, який зник з тих пір, цифрові архіви та постачальники Інтернет-послуг та веб-послуг, які можуть мати оригінальні версії або додаткові метадані для онлайн-контенту, які можна отримати через запит на допомогу. Хоча несудові слідчі можуть не мати законних повноважень запитувати інформацію з закритого джерела, контакти між постачальниками Інтернет-послуг все ж можуть бути цінними для відповіді на запитання та допомоги користувачам у навігації на їх платформах.

5. Ролі та обов'язки

Сюди входить визначення ролей та обов'язків членів команди, а також визначення координатора, який буде координувати діяльність в Інтернеті. Сюди також має входити оцінка того, хто потенційно нестиме відповідальність, якщо він буде викликаний для дачі свідчень у суді.

6. Ресурси

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Сюди входить оцінка потреб у персоналі (кількість слідчих, різноманітність та інклюзивність персоналу), а також будь-яка спеціалізована підготовка та обладнання, необхідне для слідчої діяльності в Інтернеті.

7. Документація

Сюди входять конкретні вказівки щодо того, як і де члени групи повинні документувати свою слідчу діяльність в Інтернеті.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Додаток II

Шаблон оцінки цифрових загроз та ризиків

Довідковий номер розслідування:

Дата оцінки:

Короткий опис розслідування: *предмет, територіальний та часовий обсяг розслідування*

Слідчі цілі:

1. Які ваші активи?

Люди (у розрізі за статтю):

Матеріальне майно:

Нематеріальне майно (наприклад, дані):

2. Які ваші вразливі місця?

3. Які види загроз можуть скористатися цими вразливими місцями та завдати шкоди вашим активам?

4. Хто є потенційними суб'єктами загрози?

A. Які їх інтереси?

B. Які їх можливості?

C. Яка ймовірність нападу?

5. Які заходи щодо зменшення ризиків є можливими/доцільними? Чи потрібно реагувати на різні ризики, з якими стикаються різні статі?

Слід враховувати наступне:

- Фізична шкода
- Цифрова шкода
- Психосоціальна шкода

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Додаток III

Шаблон оцінки цифрового середовища

Довідковий номер розслідування:

Дата оцінки:

Короткий опис розслідування: *предмет, територіальний та часовий обсяг розслідування*

Слідчі цілі:

Зірочка (*) означає, що слідчі повинні враховувати різні фактори, такі як вік, стать, місцезнаходження та іншу відповідну демографічну інформацію.

1. Відповідні сторони (тобто конкретні громади, збройні групи тощо). Вкажіть, чи є будь-яка різниця у використанні технологій або представленні в Інтернеті за статтю, віком чи інвалідністю між кожною зі сторін.

2. Відповідні мови (включаючи сленг та інші інсайдерські мови)*

3. Часто використовувані пошукові системи*

4. Популярні платформи соціальних медіа*

5. Популярні веб-сайти*

6. Використання Інтернету/проникнення (у розрізі за статтю, віком тощо)

7. Налаштування мобільного телефону/операційної системи (у розрізі за статтю, віком тощо

8. Популярні мобільні додатки (у розрізі за статтю, віком тощо)

9. Постачальники телекомунікаційних послуг

10. З'єднання: Розташування Wi-Fi/стільникової вежі

11. Відповідні закони (свобода вираження поглядів, доступ до інформації, конфіденційність)

12. ЗМІ та репортери (присутність в Інтернеті)

13. Відкриті бази даних (наприклад, урядові дані, дані НУО/дослідників)

14. Платні бази даних (наприклад, державні дані, дані приватних компаній/дослідників)
15. Репрезентативність онлайн-контенту (включені проти виключених груп)

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Додаток IV

Онлайн-форма збору даних

1. Інформація про збирача

Розслідування:

Збирач:

IP-адреса збирача:

Початок збору (відмітка дати/часу):

Кінець збору (відмітка дати/часу):

2. Цільова інформація

Веб-адреса (URL):

Вихідний код HTML:

Скріншот:

Захоплені дані:

IP-адреси:

3. Інформація про пакет збору

Назва файлу пакета збору:

Хеш-список пакета збору:

Файл хеш-списку хеш-файлів пакета збору:

4. Використовувані сервіси

Програмний продукт(и):

Сервіс часу:

IP-сервіс:

Сервіс WHOIS:

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

Додаток V

Міркування щодо перевірки нових інструментів

Особливості

Відкритий код проти закритого коду

Платно проти безкоштовного

Особистість власника (фізичної особи чи компанії), належність чи інтереси

Фінансування (як і наскільки добре фінансується інструмент? Яка ймовірна тривалість життя продукту?)

Питання безпеки

Кому належить інструмент або базовий код?

Чи є базовий код відкритим чи закритим?

Чи проводиться незалежний аудит інструменту?

Де зберігатимуться зібрані дані?

Хто матиме доступ до будь-яких зібраних даних?

Що таке інфраструктура безпеки інструменту?

Які юридичні зобов'язання можуть вплинути на безпеку використання інструменту?

Якщо є порушення закону, чи є право на його усунення?

Оперативні питання

Яка функціональність інструменту?

У чому зручність використання інструменту?

Які можливості підтримки користувачів власника, постачальника чи інструменту?

Як часто інструмент оновлюється?

Наскільки сумісний інструмент з іншими системами?

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*

ЦЕНТР З ПРАВ ЛЮДИНИ
Юридична школа Каліфорнійського університету в Берклі

Каліфорнійський університет, Центр з прав людини (ЦПЛ)
2224 Piedmont Avenue
Berkeley, CA 94720 (Берклі)
Електронна пошта: hrc@berkeley.edu
Веб-сайт: https://humanrights.berkeley.edu/

ОБ'ЄДНАНІ НАЦІЇ
ПРАВА ЛЮДИНИ
УПРАВЛІННЯ ВЕРХОВНОГО КОМІСАРА

Управління Організації Об'єднаних Націй
Верховний комісар з прав людини
Палац Націй (Palais des Nations)
CH 1211 Женева 10 – Швейцарія
Електронна пошта: InfoDesk@ohchr.org
Веб-сайт: www.ohchr.org

Попередня версія – спільно опублікована Організацією Об'єднаних Націй від імені Управління Верховного комісара ООН з прав людини та Центру з прав людини Каліфорнійського університету в Берклі, Юридична школа.

Переклад тексту цього документа з англійської мови на українську мову виконано мною, перекладачем Зюзь Оксаною Володимирівною.

Перекладач *Зюзь Оксана Володимирівна*

Я, фізична особа – підприємець Шевченко Людмила Михайлівна, цим засвідчую вірність перекладу з англійської мови на українську мову.

Керівник бюро перекладів *Шевченко Л.М.*