МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

© ОДУВС, 2023

Ефективність кримінального аналізу у виявленні корупційних злочинів полягає в ретельному розгляді фінансової документації та моделей легалізації неправомірно набутих прибутків. Застосування системи електронних декларацій в даний час дозволяє аналізувати заявлене майно та реальний рівень доходів певних осіб, що сприяє успішному розслідуванню злочинів.

Методологія кримінального аналізу розслідування корупційних злочинів, скоєних з використанням інформаційних технологій під час досудового розслідування, базується на докладному вивченні електронних доказів та цифрових слідів, які можуть вказувати на корупційні схеми. Разом із наведеним вище, дана методологія включає аналіз електронних документів, веб-сайтів, електронної пошти та інших цифрових слідів з метою виявлення ознак корупційних дій. Вона також орієнтована на використання спеціалізованих програмних засобів для пошуку аномалій, виявлення незвичайних фінансових транзакцій та збирання доказів для підтримки розслідування. Такий підхід вимагає ретельного аналізу цифрових слідів та використання сучасних технологій кібераналізу з метою ідентифікації та виявлення корупційних дій, які відбуваються через використання інформаційних технологій.

Крім того, методологія кримінального аналізу базується на поєднанні кібераналітики з ретельним моніторингом та аналізом онлайн-активності, що може вказувати на корупційні практики. Вона включає в себе вивчення великих обсягів даних, щоб виявити нестачі або непослідовності в деклараціях, недоречності в фінансових операціях чи інші ознаки, що вказують на корупційну діяльність. Додатково, ця методологія покликана сприяти співпраці між правоохоронними органами, аналітиками, кіберекспертами та іншими фахівцями з метою ефективного виявлення, аналізу та припинення корупційних схем, що використовують інформаційні технології.

Узагальнюючи, методологія кримінального аналізу у виявленні корупційних дій, скоєних з використанням інформаційних технологій, ґрунтується на комплексному аналізі цифрових слідів та електронних документів для виявлення ознак корупційних схем разом документальними джерелами інформації. Використання кібераналітики, спеціалізованих програмних засобів та співпраця різних фахівців із суміжних галузей грають важливу роль у виявленні та припиненні корупції, яка використовує сучасні технології для своєї діяльності. Такий підхід дозволяє виявити нестачі в деклараціях, фінансові недоречності та інші ознаки корупції, що може сприяти більш ефективному розслідуванню та припиненню корупційних дій, вчинених за допомогою інформаційних технологій.

***Література*:**

1. Офіційний сайт Національного антикорупційного бюро України. URL: https://nabu.gov.ua/about-the-bureau/struktura-ta-kerivnitctvo/struktura/osnovni-funkciyi-strukturnyh-pidrozdiliv/upravlinnya-analityky-ta-obrobky-informaciyi/
2. Офіційний сайт Державного бюро розслідувань. URL: https://dbr.gov.ua/news/prezident_zatverdiv_novu_organizaciynu_strukturu_dbr
3. Калиновський О. В., Школьніков В. І. Використання методу кримінального аналізу для протидії організованій злочинності. Часопис Київського університету права. 2017. № 1. С. 300-303
4. Кримінальний кодекс України. Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2898

ОСНОВНІ МЕТОДИ OSINT, ЩО ВИКОРИСТОВУЮТЬСЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

У сучасному світі кримінальний аналіз є однією з найважливіших складових кримінального процесу. Він дозволяє правоохоронним органам отримувати інформацію про злочин, його учасників, а також мотиви та цілі злочину.

За статистичними даними Офісу Генерального прокурора станом на 26 березня 2023 р. в Україні зареєстровано 76 518 злочинів агресії та воєнних злочинів, 16 885 злочинів проти національної безпеки. За даними ювенальних прокурорів, 1 407 дітей постраждало в Україні внаслідок повномасштабної збройної агресії РФ. При цьому, 465 дітей загинуло та понад 942 отримали поранення різного ступеню тяжкості [1; 3]. За даними Офісу Генерального прокурора, за рік повномасштабної війни Росія 8 цілеспрямованими атаками зруйнувала або пошкодила понад 81 тисячу цивільних об'єктів: понад 62 тисячі житлових будинків, понад 450 медичних закладів [2].

Одним із методів кримінального аналізу є розвідка на основі відкритих джерел (OSINT). OSINT – це метод збору інформації з відкритих джерел, таких як Інтернет, со

Пошуковик OSINT – є ключем до нових можливостей для сектору безпеки і оборони, особливо під час війни. Він допомагає не тільки зібрати, перевірити, проаналізувати інформацію про потенційних злочинців (події, явища, підприємства, установи, організації тощо), але й автоматизувати робоче місце кожного представника сектору безпеки і оборони. Оскільки допомагає в отриманні доказової бази, знаходженні потенційних ризиків та визначенні оцінки захищеності відповідних процесів і явищ, мінімізуванні трудової активності військовослужбовця та підвищенні рівня збереження його здоров'я, прийнятті управлінських рішень. соціальні мережі, ЗМІ та інші. [3,18-21]

Використання OSINT в ході кримінального аналізу має ряд переваг. По-перше, OSINT дозволяє отримувати інформацію про злочин, яка не є доступною в рамках традиційних методів розслідування. По-друге, OSINT дозволяє отримувати інформацію оперативно, що може бути критично важливим для успішності розслідування. По-третє, OSINT дозволяє отримувати інформацію з різних джерел, що може допомогти отримати більш повну картину злочину.

Однак, використання OSINT в ході кримінального аналізу також має ряд обмежень. По-перше, OSINT не завжди може забезпечити достовірну інформацію. По-друге, OSINT може бути трудомістким і вимагати значних навичок і знань. По-третє, OSINT може бути обмежений законами про захист персональних даних.

Основними методами OSINT, які використовуються в кримінальному аналізі, є такі:

- Пошук інформації в Інтернеті – це один з найпоширеніших методів OSINT. Він дозволяє отримувати інформацію з різних джерел, таких як веб-сайти, форуми, соціальні мережі та ін.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи, такі як Google, Bing та Yahoo.
- Соціальні медіа-сканери, такі як Maltego та Social Mention.
- Інструменти аналізу веб-сайтів, такі як Screaming Frog та DeepCrawl.
- Аналіз соціальних мереж – це ще один важливий метод OSINT. Соціальні мережі можуть містити цінну інформацію про злочин, його учасників та мотиви злочину.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи соціальних мереж, такі як Twitter Search та Facebook Graph Search.
- Інструменти аналізу соціальних мереж, такі як Crimson Hexagon та Radian6.
- Аналіз ЗМІ – це також важливий метод OSINT. ЗМІ можуть надавати інформацію про злочин, яка не є доступною в інших джерелах.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи ЗМІ, такі як Factiva та LexisNexis.
- Інструменти аналізу ЗМІ, такі як Meltwater та Cision.
- Аналіз відкритих баз даних – це метод OSINT, який дозволяє отримувати інформацію з відкритих баз даних, таких як реєстри, кадастрові карти та ін.

Пошук інформації в Інтернеті дозволяє отримувати великі обсяги інформації, але може бути трудомістким і вимагати значних навичок і знань.

Аналіз соціальних мереж може бути ефективним способом отримання інформації про злочинців і їх діяльність, але може бути обмежений доступом до приватних даних.

Аналіз ЗМІ може бути ефективним способом отримання інформації про злочин, який нещодавно стався, але може бути обмежений доступом до інформації, яка не була опублікована.

Для підвищення ефективності використання OSINT в ході кримінального аналізу аналітики повинні враховувати такі фактори:

Належне планування. Перед початком розслідування аналітики повинні розробити план, який визначатиме цілі розслідування, джерела інформації, які будуть використовуватися, та методи аналізу інформації.

Співпраця з іншими фахівцями. Аналітики OSINT повинні співпрацювати з іншими фахівцями, такими як поліцейські, прокурори та експерти, для отримання більш повної і точної інформації.

Контроль якості. Аналітики OSINT повинні постійно перевіряти достовірність інформації, яку вони отримують.

OSINT є потужним інструментом, який може допомогти правоохоронним органам у розслідуванні злочинів. Однак для ефективного використання цього інструменту аналітики повинні мати необхідні навички та знання. В OsintFlow впевнені, що для розвитку OSINT-фахівця важлива насамперед практика. Але ще треба мати особливий талант і чуття мисливця.

Також фахівець у галузі розвідки за відкритими джерелами має знати менталітет, психологію ворога – так само добре, як і військову складову. Позаяк це не тільки знання ботів або запитів, але насамперед аналітичний склад розуму, що дозволяє з дрібних пазлів викладати реальну картину.

При цьому, не треба забувати, що українські осінтери протидіють ворогові, і вони ж є пріоритетними цілями для нього. Відповідно, потрібно бути підкованим і щодо особистої безпеки, враховувати можливість відстеження та піклуватися про власну інформаційну гігієну.

Література:

1. Офіс Генерального прокурора. URL: https://www.gp.gov.ua.
2. Офіс Генерального прокурора. URL: https://m.facebook.com/ 1000064585280174.
3. 3.Орел О. В.OSINT як ключ до нових можливостей у правовому полі під час війни *Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності* : зб. матер. круглого столу (м. Київ, 31 березня 2023 р.) : у 2-х ч. Ч. 1. Київ : НА СБУ, 2023. 75 с. 18-21
4. Гусаков О. П., Гусакова О. В. Застосування розвідки на основі відкритих джерел (OSINT) у правоохоронній діяльності Науковий вісник Національного університету "Львівська політехніка". Серія "Право"2023
5. OSINT в Україні: хто і як допомагає фронту під час війни? URL:https://www.pravda.com.ua/columns/2023/01/23/7386112/

ВИКОРИСТАННЯ ІНФОРМАЦІЇ З СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖ У РОЗСЛІДУВАННЯХ КІБЕРЗЛОЧИНІВ

Пукас Ярослав Володимирович
здобувач вищої освіти
Прокопов Сергій Олександрович
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ

У сучасних умовах розвитку інформаційних технологій та побудови інформаційного суспільства взаємодія користувачів Інтернету соціальні мережі стає не лише засобом спілкування, а й новою сферою життя. Користувачі активно та повноцінно взаємодіють один з одним у соціальних мережах Інтернету, що призводить до накопичення великого обсягу інформації, яка може мати, в тому числі, протиправний характер.