

Список використаних джерел

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>.
2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17>.
3. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19>.
4. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.
5. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції : Закон України від 6 лип. 2010 р. № 2438-VI. URL: <https://zakon.rada.gov.ua/laws/show/2438-17>.
6. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3 серп. 2017 р. № 676, зареєстр. у Мін'юсті України 24 серп. 2017 р. за № 1059/30927. URL: <https://zakon.rada.gov.ua/laws/show/z1059-17>.
7. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : наказ МВС України від 16 бер. 2020 р. № 257, зареєстр. у Мін'юсті України 31 бер. 2020 р. за № 319/34602. URL: <https://zakon.rada.gov.ua/laws/show/z0319-20>.
8. Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС України : наказ МВС України від 10 вер. 2009 р. № 390. URL: <https://zakon.rada.gov.ua/laws/show/z0963-09>.
9. Case of S. and Marper v. the United Kingdom (applications nos. 30562/04 and 30566/04) : judgment of the European Court of Human Rights (Grand Chamber), 4 December 2008. URL: <https://hudoc.echr.coe.int>.
10. Шепітько В. Ю. Криміналістика : підручник. Харків : Право, 2019. 456 с.
11. Журавель В. А. Загальна теорія криміналістики: генеза та сучасний стан : монографія / В. А. Журавель ; Нац. акад. прав. наук України. Харків : Право, 2021. 448 с.
12. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. 588 с.

Базиліак Ірина Олегівна, здобувач вищої освіти НАВС

Науковий керівник – **Воробей Олена Вячеславівна**, професор кафедри криміналістичного забезпечення та судових експертиз навчально-наукового експертно-криміналістичного інституту НАВС, кандидат юридичних наук, доцент

OSINT ЯК ІНСТРУМЕНТ ПРОТИДІЇ РОСІЙСЬКІЙ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ

Сучасна війна ведеться не лише на передовій, а й у медійному та інформаційному просторі. Як відомо, російська федерація протягом багатьох років формувала масштабну систему пропаганди й дезінформації, використовуючи фейки та маніпулятивні наративи для впливу на суспільну свідомість і дезорієнтацію аудиторії. Водночас розвиток Інтернету та цифрових технологій надав цивільному суспільству потужний інструмент протидії – OSINT (Open Source Intelligence), тобто розвідку на основі відкритих даних. Сьогодні цей інструмент вийшов далеко за межі діяльності спецслужб і перетворився на глобальний волонтерський та журналістський рух, який допомагає викривати дезінформацію та руйнувати пропагандистські міфи Кремля.

OSINT – це діяльність із пошуку, збору та аналізу інформації, отриманої із загальнодоступних каналів, що не потребує застосування таємних методів збору [1, с. 7]. До джерел можна віднести супутникові знімки, фото та відео з соціальних мереж, публічні реєстри, бази даних, новини, метадані файлів тощо.

Ключова перевага OSINT у боротьбі з пропагандою полягає у посиленні перевірки фактів та доказової бази. Коли пропаганда апелює до емоцій, маніпуляцій, теорій змови та авторитету «офіційних джерел», то відкрита розвідка ґрунтується на точності даних і реальних доказах, доступних для незалежної перевірки. Використовуючи відкриті джерела та аналітичні

методи, OSINT дає змогу кожному, хто має доступ до комп'ютера та володіє критичним мисленням, самостійно перевіряти інформацію та викривати неправдиві наративи.

Російські інформаційні операції переважно спрямовані на приховування власних злочинів, спотворення фактів або дискредитацію України на міжнародній арені. OSINT-спільнота – такі проєкти як OSINT Бджоли, InformNapalm, Molnar, DeepState [2] – використовує низку ефективних інструментів для встановлення реальних фактів. Коли міноборони РФ або пропагандистські ресурси поширюють відео нібито «знищення української техніки» чи «успішних ударів», аналітики перевіряють достовірність цих матеріалів шляхом встановлення точного місця зйомки: досліджуються особливості рельєфу, розташування доріг, ліній електропередачі, будівель та інших об'єктів, які порівнюються із супутниковими знімками. У результаті таких перевірок неодноразово виявлялося, що пропагандистські «переможні сюжети» були зняті далеко від зони бойових дій – на полігонах у Росії або на тимчасово окупованих територіях. В окремих випадках на відео фіксувалася навіть російська техніка, яку намагалися видати за українську [3].

Особливо важливу роль OSINT відіграє у викритті спроб приховування воєнних злочинів. Одним із найвідоміших прикладів стала трагедія в м. Буча. Після звільнення міста російська пропаганда поширювала твердження, ніби тіла загиблих мирних жителів з'явилися на вулицях уже після відходу російських військ, називаючи зазначені жахливі події «постановкою». Проте аналітики та журналісти швидко спростували ці заяви за допомогою супутникових знімків компанії Maxar Technologies, зроблених у середині березня 2022 року, коли місто перебувало в окупації. На знімках було чітко видно тіла людей у тих самих місцях, де їх згодом виявили українські військові та міжнародні журналісти після деокупації Бучі [4].

Ще одним напрямом OSINT є аналіз цифрових слідів та метаданих, що дає змогу викривати інформаційні маніпуляції ще до їх масового поширення. Один із показових прикладів – відеозвернення представників так званих «ЛНР/ДНР», оприлюднених напередодні повномасштабного вторгнення у 2022 році, в яких нібито оголошувалась «термінова евакуація населення через наступ українських сил» [5]. Для перевірки достовірності таких матеріалів аналітики досліджують цифрові файли та їх метадані – дату створення, редагування та технічні параметри запису. Так було виявлено, що відео були записані ще за кілька днів до початку вторгнення та спростовано російську тезу, що агресія була «вимушеним кроком у відповідь».

Одним із аспектів діяльності OSINT є встановлення персональної відповідальності за воєнні злочини. Ворог прагне знеособити наслідки насильства та уникнути конкретизації відповідальності конкретних осіб. Але з використанням інструментів з розпізнавання облич та аналізу злитих у відкритий доступ російських баз даних, спеціалісти знаходять конкретних пілотів, які запускають ракети по українських містах, або солдатів, що займалися мародерством, катуваннями та вбивствами. У низці розслідувань саме завдяки відкритій розвідці вдалося ідентифікувати осіб, які вчиняли воєнні злочини на території України. Надалі, матеріали використовуються журналістами, правоохоронними установами як додаткові джерела для документування подій та потенційного притягнення до відповідальності [6].

На відміну від традиційних механізмів державного спростування, які часто потребують більше часу для збору, перевірки та оприлюднення інформації, OSINT відзначається швидкістю, відкритістю та широким залученням незалежних учасників. Тисячі незалежних аналітиків і журналістів у різних країнах можуть одночасно досліджувати один і той самий матеріал, перевіряючи його з різних позицій та використовуючи різні методи аналізу. Як правило, аналітики демонструють повний алгоритм дослідження, що дозволяє іншим дослідникам повторно перевірити результати. Також дедалі частіше отримані під час досліджень матеріали використовуються як допоміжна доказова база у правозахисній діяльності та судових процесах.

OSINT суттєво змінив сучасний інформаційний простір на той, у якому дедалі більшого значення набувають перевірені дані та доказовість. Нині розвідка на основі відкритих даних уже не є виключно сферою діяльності державних структур чи професійних аналітиків. Завдяки доступу до інформації, цифровим сервісам і розвитку навичок критичного мислення дедалі більше людей можуть долучатися до перевірки фактів та виявлення інформаційних маніпуляцій. У наш час інформаційна безпека суспільства значною мірою залежить від здатності перевіряти першоджерела та відрізняти факти від маніпулятивної інформації.

Список використаних джерел

1. OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. Одеса : Видавництво «Юридика», 2024. 180 с.
2. OSINT в Україні: хто і як допомагає фронту під час війни? Українська Правда. веб-сайт. URL: <https://www.pravda.com.ua/columns/2023/01/23/7386112/index.amp>
3. РФ видала трактор за нібито знищений в Україні танк Leopard. DW: веб-сайт. URL: <https://www.dw.com/uk/rosia-vidala-traktor-za-nibito-znisenij-v-ukraini-tank-leopard/a-65845769>
4. Оприлюднили супутникові знімки з тілами у Бучі до деокупації. *Militaryni* : веб-сайт. URL : <https://militaryni.com/uk/news/oprylyudneno-suputnykovi-znimky-z-tilamy-u-buchi-do-deokupatsiyi/>
5. У «ДНР» і «ЛНР» оголосили евакуацію населення в росію. Україна заперечує наступ. BBC Україна. URL : <https://www.bbc.com/ukrainian/news-60429343>
6. Хто катував херсонців? Журналісти-розслідувачі встановили нові факти. *Radio Свобода* : веб-сайт. URL : <https://www.radiosvoboda.org/a/novyny-pryazovy-a-khto-katuvav-khersonsiv-pid-chas-okupatsiyi/32893929.html>

Balaniuk Bogdan, Cadet of the Kharkiv National University of Internal Affairs

Research Supervisor – **Timoshyn Anatolii**, Associate Professor of Department of Information Systems and Technologies of Kharkiv National University of Internal Affairs, Candidate of Physical and Mathematical Sciences, Associate Professor

DEVELOPMENT OF A SIMPLE WEB RESOURCE RISK ASSESSMENT SYSTEM BASED ON HEURISTIC RULES

In this day and age, with the internet being our go-to for all sorts of information, keeping in touch, and even sorting out our finances, it's no surprise that the more we get online, the more dodgy stuff we bump into. We're talking about all sorts of nasty traps like fake websites designed to nick your details, nasty software lurking about, rip-off online shops, and other risky places. Because of this, sorting out a way to figure out just how risky a website is, and how quickly we can spot potential trouble for a user, has become a pretty pressing job.

One of the most straightforward and effective ways to tackle this is by using what we call heuristic principles. Heuristics is basically a method of looking into something that doesn't rely on hardcore maths, but rather on a collection of common-sense clues and practical observations you pick up along the way. This method is super useful in the world of online security because it lets us react fast to new threats that pop up, even if we don't have a massive list of known malicious sites yet.

Imagine you've got a system for judging website risks, and it's built on these heuristic ideas. It works by looking at what makes a website tick and tallying up special «risk points». The more red flags it spots, the more dangerous that site is deemed to be.

To get a basic system up and running for judging risk, you can pinpoint a few key things to check about a website. First off, is it using that secure HTTPS connection? Having an SSL/TLS certificate means the information zipping between you and the website's server is all scrambled up and safe. On the flip side, if a site's just chugging along on plain old HTTP, it might be a sign that it's either dodgy or just plain old. Still, even with HTTPS, you're not completely in the clear, as those sneaky phishers can get hold of these certificates too.

Another big thing to check is the website's actual address, its domain name. Shady sites often try to trick you by looking *very* similar to the addresses of famous websites, perhaps by swapping out a letter or adding bits and bobs. This trick, often called typosquatting, is a favourite among those running phishing scams. So, instead of landing on the usual site, you might get sent somewhere that looks almost the same, but with a tiny spelling mistake.

You can also get a sense of risk by looking at how long the domain has been around. Websites that have only just been set up are far more likely to be used for scams, simply because the crooks keep ditching them once they get blocked. If a domain's only been live for a few days or weeks, that's a strong hint it could be risky business. To find out how old a domain is, you'd typically have a look at WHOIS records or special databases.

It's also important to peek inside the website's layout. Loads of flashing adverts, pop-ups that appear out of nowhere, automatically sending you off to other sites, or trying to sneakily download files