INFOlight.ua

ФОНД СПРИЯННЯ ДЕМОКРАТІЇ

Проект Infolight.ua здійснюється за підтримки Фонду Ганнса Зайделя в Україні

Фонд Ганнса Зайделя
Київський офіс

Інструменти інформаційної боротьби: ОСІНТ, ІПСО та протидія дезінформації

Словник:

OSINT (Open source intelligence/ розвідка з відкритих джерел) – технологія збору даних з відкритих джерел інформації. В умовах широкого розповсюдження інтернету OSINT перетворився із вузькоспеціалізованого в загальнодоступний інструмент. Сьогодні його застосовують як комерційні структури, так і звичайні користувачі.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ (ІПСО) – сплановані дії по роботі з іноземними аудиторіями. Мета ІПСО – вплив на почуття, мотиви, критичне мислення цільової аудиторії.

ВІДКРИТІ ДЖЕРЕЛА (open sources) – на відміну від секретних джерел та джерел з обмеженим доступом, ВД є загальнодоступною інформацією, якою може скористатися кожен на безкоштовній основі або за плату.

АДЖЕНДА – порядок денний. В OSINT-розслідуваннях слово означає певний протокол, порядок дій, якого дотримується розслідувач.

АВТЕНТИФІКАЦІЯ – процедура встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.

АНАЛІТИЧНА РОЗВІДКА – особлива форма інформаційно-аналітичної роботи, яка заснована на органічній єдності всіх форм цієї роботи і полягає у набутті нових знань про об'єкт чи явище на основі аналітичної обробки здобутої інформації про осіб, події, предмети, що становлять інтерес розслідувача.

Інструменти інформаційної боротьби:

ОСІНТ, ІПСО та протидія дезінформації

Київ 2022

Історична довідка

Засновником технології OSINT можна вважати Шермана Кента, професора Єльського університету, який тривалий час працював в ЦРУ та під керівництвом якого було створено так званий «Єльський звіт», розсекречений тільки наприкінці 1990-х років.

«Єльський звіт» – це документ від 1 вересня 1951-го року на 627 сторінках, щодо боєготовності збройних сил Сполучених Штатів. У певному сенсі це був особливий вид національного розвідувального дослідження, що був призначений оцінити можливості армії США у перші дні корейської війни. А саме – що ворог може знати про армію США та її боєздатність з відкритих джерел: радіо, телебачення та газет – основних джерел інформації тих часів.

Звіт справив вибуховий ефект. Бо, як виявилося, у відкритих джерелах можна було знайти дані про чисельність, дислокацію, озброєння американських військових частин, навіть частково – про розміщення крилатих ракет та іншої надсекретної інформації. Також було встановлено, що понад 90% зібраної інформації відповідало дійсності.

Цей світ допоміг виявити вразливості американської системи секретності, за його підсумками було кардинально змінено класифікацію та захист певної інформації. І саме з нього веде свій відлік OSINT-технологія.

Наступний поштовх розвитку цієї технології стався після терористичних актів 11 вересня 2001 року.

У 2004 році президент США Джордж Буш підписав закон «Про реформування розвідки та протидію терористичній загрозі» (Intelligence Reform and Terrorism Prevention Act of 2004), що містить вказівки про включення OSINT-розвідки як повноцінного і рівноправного виду в діяльність Розвідувального співтовариства, а також про формування національного центру розвідки на основі аналізу відкритих джерел.

Згідно відкритих даних на сьогодні розвідувальні служби США здійснюють OSINT-аналіз та збір даних 25-ма мовами.

За американським зразком поступово усі крани світу почали тією чи іншою мірою використовувати OSINT.

В Україні до 2014 року OSINT періодично використовувався здебільшого журналістами-розслідувачами.

Початок російської збройної агресії дав суттєвий поштовх розповсюдженню OSINT-технологій у світі, зокрема й в Україні.

В Україні після початку російської агресії виникли InformNapalm та «Миротворець». У світовому масштабі Bellingcat став широковідомим саме після розслідування збиття росіянами літака MH17.

Більшість журналістських розслідувань про корупцію в Україні після 2014 року в той чи інший спосіб використовують технології OSINT. Зокрема, отримуючи дані про спосіб життя родин чиновників з інстаграм-акаунтів їх родини чи коханок, відстежуючи польоти приватних літаків через спеціальні сервіси, вивчаючи дані з реєстрів тощо.

Хібікі Сато

OSINT також використовують і злочинці. Найбільш гучним у світі став випадок, коли японець Хібікі Сато, фанатичний прихильник співачки Ени Мацуоки, вистежив її, ідентифікувавши залізничну станцію, що була відображена в її очному яблуці на одному з її селфі в соціальних мережах. Збільшивши зображення її ока та за допомогою Google Street View, він зміг розпізнати назву станції, звідки вона їздила.

Він сказав поліції, що прискіпливо вивчав, здавалося б, тривіальні деталі відео, які жінка знімала у своїй квартирі, як-от розташування штор і напрямок природного світла, що потрапляє у вікно, щоб визначити, у якому будинку вона живе.

Етапи OSINT-планування

Розширені можливості пошукових систем

Розширені можливості пошуку Google

site:	Обмежує результати результатами з певного домену, наприклад **site:apple.com**
“ ”	Лапки вказують на пошук точного вислову, наприклад **“харківська військова операція”**
AND	Показує результати лише для обох умов, наприклад **apple AND orange**
OR	Пошук терміну А, Б чи обох. Символ труби – те саме, що й АБО, наприклад **gun OR rifle = gun | rifle**
*	Підстановковий знак для слів у фразі, яку ви не знаєте, наприклад **wish * a star**
( )	Групує набір слів/операторів окремо, наприклад **(gun | pistol) ammo**
-	Виключає результати, що містить це слово, наприклад **chicago baseball-cubs**
$	Пошук за певною ціною, наприклад **“apple watch” $299**
cache:	Остання кешована версія домену, наприклад **cache:boston.gov**
filetype:	Пошук лише за певним типом файлу, наприклад **ext:** працює так само **filetype:pdf “confidential”** або **ext:pdf “confidential”**
related:	Пошук сайтів, пов’язаних з доменом, наприклад **related:sony.com**
intitle:	Пошук сторінок із умовою в заголовку сторінки, наприклад **intitle:sabotage**
inurl:	Виводить сторінки, що містять вказане слово в URL, наприклад **inurl:private**
around(x)	Сторінки, що містять два слова або фрази на відстані X слів один від одного, наприклад **microsoft (7) surface**
info:	Знайти інформацію про конкретну сторінку, включаючи час останнього кешування, наприклад **info:chicago.gov**

Також просунутий пошук можна здійснювати за допомогою Розширеного пошуку Google https://www.google.com/advanced_search

Розширений пошук DuckDuckGo

На прикладі слів «кіт» та «собака»

Cats dogs	Результати про котів чи собак
«cats and dogs»	Результати для «котів та собак». Якщо результати не будуть знайдені, пошукова система буде намагатись показати відповідні результати.
cats +dogs	Більше собак в результаті пошуку
cats filetype:pdf	PDF файли про котів. Типи файлів, які піддаються пошуку: **pdf, doc(x), xls(x), ppt(x), html**
dogs site:example.com	Сторінки про собак із example.com
Cats -site:example.com	Сторінки про котів, за виключенням example.com
intitle:dogs	Заголовок сторінки має включати слово «собаки»
inurl:cats	Url сторінки включає в себе слово «коти»

Розширений пошук Bing

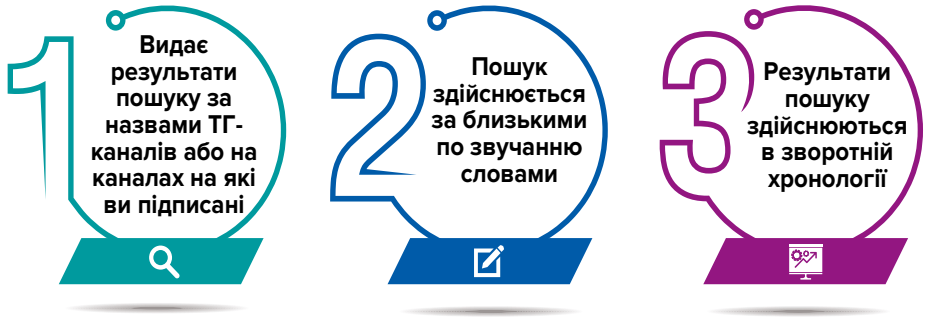
( )	Групує набір слів/операторів окремо, наприклад **(gun | pistol) ammo**
OR	Всі запити Bing розглядаються як І якщо ви не вкажете умови або між ними **goat OR pig OR cow**
NOT	Виключає результати з певним терміном. Також працює символ **–boat NOT (raft OR ship)**
loc:	Пошук сторінок з певного регіону **(loc:GB OR loc:FR)**
prefer:	Надає пріоритет умові пошуку або іншому оператору **prefer:tomato plum apple**
near:x	Пошук слів на відстані X одне від іншого **red near:4 blue**
ip	Знаходить сайти, розміщені на IP адресі **ip:208.43.115.82**
site/domain:	Фільтр для конкретного типа домену **site/.gov confidential**
feed:	Знаходить RSS-канали на основі пошукових запитів **feed:osint**

Додаткові можливості в соцмережах

Telegram

Ця соцмережа має найбільшу динаміку розвитку в Україні, відповідно є найшвидшим засобом інформування.

Пошук за конкретними словами в Телеграм має певну специфіку:



Підбірка найкращих OSINT-ботів Телеграм

@LeakedInfoBot – найпопулярніший бот для пошуку злитої інформації про людину. Знаходить всю доступну інформацію про фізичних та юридичних осіб з державних баз даних, зламаних баз соціальних мереж, з інших джерел. Бот має найактуальніші бази даних.

@UsersSearchBot – бот для пошуку по ПІБ, ніку, номеру телефону, email або профілю в соцмережах. Пошук по Sherlock. Рекомендуємо!

@Quick OSINT bot – інформація про людину за номером телефону, email або профілю в соцмережах, фотографії.

@Search_firm_bot – бот здійснює пошук по організаціям, банкам, поштовому індексу.

@UniversalSearchBot – бот призначений для пошуку виключно відкритої інформації за такими запитами, як номер телефону, адреса електронної пошти, держномер автомобіля, ім'я користувача, IP-адреса, доменне ім'я, геолокація, фотографія, ID Telegram і ВКонтакте. Прекрасно автоматизує OSINT.

@maigret_osint_bot – перевірка username. Maigret перевіряє наявність зареєстрованого користувача з конкретним нікнеймом серед 1366 різних сайтів. За основу взято інструмент Sherlock, який творець бота почав розвивати.

@egrul_bot – безкоштовний швидкий сервіс перевірки контрагентів. Лише легальні дані.

@GetGmail_bot – Пошук облікових записів, прив'язаних до пошти Gmail.

@telesint_bot – дозволяє дізнатися, в яких публічних чатах є користувач. Зараз у базі даних робота знаходиться більше 179 тисяч публічних чатів і записи про більш ніж 45.5 мільйонів користувачів.

@tgscanrobot – так само, як і попередній бот, перевіряє наявність користувача в публічних чатах. Зараз у базі робота міститься більше 709 тисяч чатів, 116 мільйонів унікальних користувачів.

@username_to_id_bot – дозволяє отримати ID користувача, чату, каналу або бота.

@clerkinfobot – пошук за номером телефону та username Telegram.

@creationdatebot – показує дату створення облікового запису.

@SangMataInfo_bot – може показати історію зміни нікнеймів користувача.

@MotherSearchBot – аналог Google, але для Telegram. Допоможе знайти потрібний канал, текст, аудіо чи документ.

@buzzim_alerts_bot – аналіз семантики. Пошук за відкритими повідомленнями в Telegram.

@ChatSearchRobot – пошук подібних за тематикою чатів. У основі робота міститься понад 709 тисяч чатів.

Телефони:

@Real GetContact bot – безкоштовний GetContact

@ Get_Contectredly_bot – бот знайде номер телефону облікового запису, бот приймає username і ID.

@bmi_np_bot – Визначення оператора та інших даних за номером телефону.

@HackContactBot – ще одне робоче дзеркало GetContact

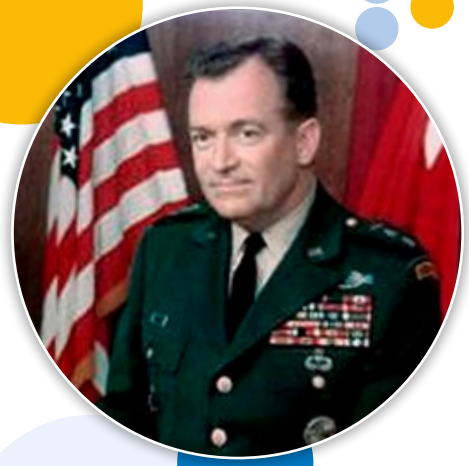
@LBSE_bot – бот-аналізатор розташування мобільного абонента практично будь-якого мобільного оператора в будь-якій країні світу.

Боти по роботі з іншими соцмережами

@InstaBot - завантажує будь-які медіафайли з Інстаграм
@SaveYoutubeBot – шукає та завантажує ролики з YouTube
@getfb_bot – Пошук сторінки у Facebook за номером телефону.

«90% розвідданих приходить із відкритих джерел, і лише 10% – завдяки роботі агентури».

Самуель Вілсон,
колишній керівник РУМО США:



twitter

Розширений пошук	https://twitter.com/search-advanced
Набір тулів	http://tweetbeaver.com/
Поскаржитись	https://tinfoleak.com/
Аналітика	https://socialbearing.com/
Аналітика	https://analytics.mentionmapp.com/
Аналітика	https://foller.me
Аналітика	http://twiangulate.com/search/
Старі пости	http://staringispolite.github.io/twayback-machine/
Пошук	https://snapbird.org/
Підписники	https://doesfollow.com
Відео	https://twdown.net/
Візуалізація	https://treeverse.app/
Зміни профілю	https://spoonbill.io/
Mapping	https://onemilliontweetmap.com
Inteltechniques	https://inteltechniques.com/menu/pages/twitter.tool.html

«Політики отримують із відкритих джерел до 80% інформації, необхідної їм для ухвалення рішень у мирний час»

Шерман Кент, аналітик ЦРУ

TikTok

Пошук	https://tiktokapi.ga/
Пошук	https://www.osintcombine.com/tiktok-quick-search
Завантажувач	https://en.savefrom.net/download-from-tiktok
Захоплення відео	https://airmore.com/watch-tik-tok-pc.html
Юридичні питання	https://www.tiktok.com/en/law-enforcement

Instagram

Пошук користувачів чи тегів	https://www.yooying.com/search
Пошук користувачів чи тегів	https://www.social-searcher.com/
Пошук по #	https://tagboard.com/
Аналіз підписників	https://hypeauditor.com/
Пошук локації	https://www.osintcombine.com/instagram-explorer
Пошук	https://mulpix.com/
Захват медіа	https://downloadgram.com/
Захват медіа	https://instasave.xyz/
Завантаження	https://www.4kdownload.com/products/prod¬uct-stogram
Профіль фотографії	https://instadp.net/
Профіль фотографії	http://izuum.com/
Історії	https://storiesig.com/
Пошук фото	https://imgwonders.com/
Користувач/#	http://picdeer.com/
Користувач/#	https://www.pictame.com/
Inteltechniques	https://inteltechniques.com/menu/pages/instagram.tool.htm

Просунуті OSINT-механізми

ВАЖЛИВО!!! **Цей перелік є актуальним на момент написання тексту. Проте одні сайти зникають, інші з'являються. Перелік сайтів бажано постійно самостійно оновлювати.**

Пошук фото/зображень

Пошук	https://images.google.com/
Пошук	https://tineye.com
Пошук	https://www.bing.com/images/
Пошук	http://www.picsearch.com/
Пошук Росія	https://www.yandex.com/images/
Пошук Азія	http://images.baidu.com/
Twitter Пошук	http://twipho.net/
Flickr	https://www.flickr.com/map
Exif	http://exif.regex.info/exif.cgi

Пошук документів

https://psbdmp.ws	http://www.findpdfdoc.com/
http://cryptome.org	https://www.base-search.net/
http://megasearch.co	https://psbdmp.ws

Пошук фото/зображень

Розширення	https://www.downloadhelper.net/
Youtube-DL	https://github.com/ytdl-org/youtube-dl
Розширення	https://addons.mozilla.org/en-US/firefox/addon/video-downloader-profession/
Знімок екрану	https://www.techsmith.com/screen-capture.html
Архів відео	https://archiving.witness.org/archive-guide/ac-quire/acquiring-raw-video-and-metadata/

Методика пошуку за відео:

Важливо враховувати, що Фейсбук змінює оригінальні дані. В той час як Телеграм здебільшого зберігає ці дані.

ІПСО
Інформаційно-психологічні операції

Інформаційно-психологічні операції (ІПСО, англ. – Psychological Operations, PSYOP) – це спланована дії з передачі конкретної інформації та індикаторів до різних, переважно іноземних аудиторій, щоб вплинути на їхні почуття, мотиви, критичне мислення і, зрештою, на діяльність відповідних урядів, організацій, груп чи індивідів.

Визначення офіційно закріплено в Польовому статуті ЗС США 33-1 – Психологічні операції (англ. Field Manual 33-1 – Psychological Operations) від 1987 року. Втім їх почали використовувати в конфліктах людства набагато раніше під час політичних і релігійних воєн, а до видів ІПСО відносять пропаганду і дезінформацію. Термін виник в 1918 році, під час заснування підрозділу психологічної пропаганди військової розвідки американського експедиційного корпусу.

Інформаційно-психологічні операції складаються з політичних, військових, економічних, дипломатичних і власне інформаційно-психологічних заходів, спрямованих на конкретну людину чи групи людей з метою впровадження в їх середовище чужих ідеологічних і соціальних установок, формування помилкових стереотипів поведінки, трансформації в потрібному напрямку їх настроїв, почуттів, волі.

Основними суб'єктами проведення ІПСО є:

1. **Керівництво іноземної держави**
2. **Спецслужби іноземних держав та її агентура**
3. **Засоби масової інформації** (іноземні та підконтрольні вітчизняні)
4. **Неурядові організації (іноземні й підконтрольні вітчизняні)**
5. **Інтернет-ресурси**

ІПСО можуть бути спрямовані проти населення загалом чи окремих соціальних прошарків і груп; проти політичної, фінансово-економічної, наукової, культурної еліти; проти певних політичних чи військових лідерів; проти релігійних діячів; проти окремих осіб, відповідальних за прийняття тих чи інших суспільно значущих рішень тощо. Також можуть нести вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу – на свідомість і поведінку людей.

Приклади ІПСО з історії:

— В часи військових походів Святослава, перед тим, як іти в похід на ворога, князь посилав йому повідомлення «Іду на ви» – що означало «Йду на тебе війною».
В часи правління Святослава Хороброго Київська Русь була державою з сильною армією, і це повідомлення мало залякати ворогів Святослава ще до того, як він приходив до них з військом.

— Біблійне оповідання про Гедеона. Гедеон зі своїм слугою Фарою пробрався у табір мадіанитян і почув, як один воїн розповідав іншому про свій сон, немовби мадіанитянським табором котився круглий ячмінний хліб і, прикотившись до намету, вдарив по ньому так, що намет упав, перекинувся і розсипався. На це інший воїн зауважив: «Це не що інше, як Гедеонів меч, якому Бог віддасть в руки мадіанитян». Повернувшись у свій табір, Гедеон розбудив своїх воїнів, дав їм до рук труби, порожні глечики і в глечики світильники. Розділив усіх на три загони і наказав їм оточити ворожий табір і робити те, що робитиме його загін, і кричати: «Меч Господа і Гедеона». Коли всі були на місцях, Гедеон наказав своєму загонові розбити глечики і з запаленими світильниками сурмити у сурми і кричати: «Меч Господа і Гедеона!» Те саме вчинили і два інші загони. На мадіанитян напав такий жах, що вони у страшенній паніці в темряві стали вбивати один одного і, урешті-решт, кинулись тікати.

Складові інформаційно-психологічних операцій:

1 ЗМЕНШЕННЯ СПРОТИВУ НАСЕЛЕННЯ
Зміна поведінки громадянського населення на сприятливу.

2 ВВЕДЕННЯ СИЛ ПРОТИВНИКА В ОМАНУ

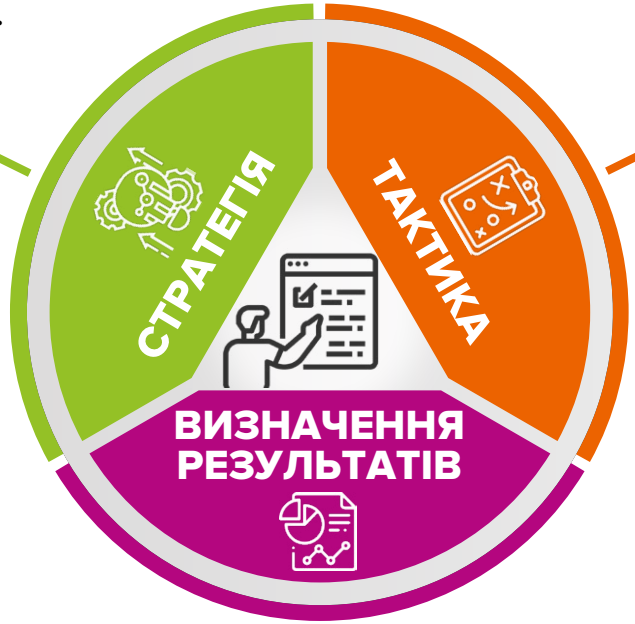
«Вуха російського ІПСО стирчать з матеріалів, де Україну звинувачують у контрабанді, перепродажу, втраті, неналежному використанні озброєння, що постачається нам партнерами. Для цього Росія використовує широкий спектр інструментів інформаційного впливу — афілійованих до неї «лідерів думок», експертів, пресу, політиків не лише в РФ, а й за її межами. Чим більше західна зброя змінюватиме ситуацію на полі бою на користь України, тим істеричніше вестиме себе РФ. Пропаганда — це те, на чому російський тоталітарний режим намагатиметься ще деякий час їхати, тоді як його військова машина розвалюватиметься на ходу.»

Ганна Маляр,
заступниця Міністра оборони України.

Етапи ІПСО-планування

1. Чітке визначення мети, цілей, завдань.
2. Визначення конкретної цільової аудиторії.
3. Оцінка відповідності ІПСО ситуації, яка існує на даний момент.
4. Підготовка детального плану.

1. Вибір каналів донесення інформації
2. Розробка продукту.
3. Тестування на експериментальній групі.
4. Виробництво та розповсюдження матеріалів.



1. Реалізація
2. Посттестування – оцінка відгуків цільової аудиторії
3. В разі потреби – внесення зміни в малюнок реалізації

Послідовність російських ІПСО в ході військових дій 2022 року

Протягом дев'яти місяців російська влада декілька разів змінювала власні пропагандистські наративи. Це пов'язано не лише із спонтанним плануванням, але й зміною цільової аудиторії російської пропаганди.

Якщо з лютого 2022 року цільовою аудиторією для російських ІПСО були громадяни України, то починаючи з квітня стались суттєві зміни. До цільових аудиторій, окрім громадян України, додались громадяни країн-союзників (переважно країни-члени НАТО) та російські громадяни. Путінському оточенню треба було пояснити, що вихід російських військ із північних областей України – це не поразка, а виключно тактичний маневр.

Проте в межах цього матеріалу варто розглянути виключно ІПСО – тобто дії російської пропаганди проти громадян України та країн-членів НАТО.

1 етап

- **Російська армія – друга в світі за потужністю.**
- **ЗСУ як потужної сили не існує.**
- **Чинний президент України втік із Києва в перші дні війни.**
- **Слабкість України є системним наслідком того, що української нації не існує.**

2 етап

- **Вихід російських військ із Київської, Чернігівської та Сумської областей є «актом доброї волі».**
- **Путін має психічний розлад. Отож країнам-партнерам не варто особливо допомагати Україні, щоб уникнути можливої ескалації конфлікту.**
- **Путіну треба допомогти «зберегти обличчя», бо якщо він перетвориться на «щура, загнаного в кут», то застосує ядерну зброю.**
- **Свідченням того, що росіяни та українці є однією нацією, є результати «референдумів» в Луганській, Донецькій, Запорізькій та Херсонській областях.**

3 етап

- **Різниці між агресором та його жертвою немає. Війна є наслідком агресивних дій двох сторін.**
- **Війну треба припинити за столом переговорів.**
- **Проведення мобілізації в РФ може призвести до зміни ситуації на фронті.**
- **Росія вже пішла на можливі максимальні поступки – без особливого спротиву покинула Харківську область та правобережну Херсонщину.**
- **Продовження безглуздої війни в зимовий час потягне за собою значні побутові незручності для українців – відсутність світла, опалення призведе до чисельних жертв.**
- **Українці та росіяни – братні народи, які мають жити в мирі.**

Словник:

ВЕБ-СКРАПІНГ – процес перетворення у структуровані дані інформації з вебсторінок. Як правило проводиться автоматизовано.

ВЕРИФІКАЦІЯ – порівняння даних та параметрів, у тому числі біометричних, для встановлення тотожності особи документам або інформації з Реєстру для підтвердження їх ідентичності.

ЗАГАЛЬНОДОСТУПНА ІНФОРМАЦІЯ – дані, факти, інструкції або інші матеріали, опубліковані або розміщені для широкого використання, доступні для громадськості.

ВІЙСЬКОВА ОПЕРАТИВНО-РОЗШУКОВА ДІАГНОСТИКА – одна із форм інформаційно-аналітичної роботи, спрямована на емпіричне виявлення військових злочинів, сил ворога та пов'язаних з ними предметів, речовин і документів за заздалегідь відомими загальними ознаками, на підставі оцінки об'єктів, які розпізнаються, а також отримання нових знань про ці об'єкти, в інтересах безпеки громадян, суспільства і держави.

ІНФОРМАЦІЙНИЙ ПРОДУКТ – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів.

СКРИНІНГ (screening) – відбір фактів, явищ із багатьох однорідних, які в процесі дослідження виявляють необхідні, шукані властивості.

Інструменти інформаційної боротьби: ОСІНТ, ІПСО та протидія дезінформації

Текст – Юрій Гончаренко, Костянтин Канішев
Літературний редактор, коректор - Катерина Махлай
Комп'ютерний дизайн та верстка - Дмитро Сапон
Концепт художнього оформлення - Дмитро Сапон

Більше по матеріалам ОСІНТ та ІПСО ви зможете дізнатися в авторських лекціях проекту InfoLight_UA

Дмитро Золотухін
«ОСІНТ та робота з джерелами»

Представник Центру національного спротиву
Інформаційно-психологічна операція (ІПСО). Як не стати жертвою чужих маніпуляцій

Проект

INFOlight.ua

сайт Facebook

Проект Infolight.ua здійснюється за підтримки Фонду Ганнса Зайделя в Україні

ФОНД СПРИЯННЯ ДЕМОКРАТІЇ

Фонд Ганнса Зайделя
Київський офіс