6. Бойко І. В ефірі "Україна 24" показали фейкове повідомлення Зеленського про "капітуляцію", президент його спростував. *УНІАН. Інформаційне агентство.* 16 березня 2022. URL: https://cutt.ly/1w31HpoV. (дата звернення 03.01.2024 р.).

7. Інститут Масової Інформації. Хакери зламали рухомий рядок каналу «Україна 24» та транслюють фейк про «капітуляцію». 2022. URL: https://cutt.ly/Yw31HYc4. (дата звернення 03.01.2024 р.).

Ліцук Богдан Вікторович
Здобувач кафедри національної безпеки.
Волинський національний університет імені Лесі Українки
Стрелков Владислав Володимирович
Ph. D., старший викладач кафедри національної безпеки.
Волинський національний університет імені Лесі Українки

ГАЛУЗІ ЗАСТОСУВАННЯ РОЗВІДКИ ВІДКРИТИХ ДЖЕРЕЛ ДАНИХ (OSINT)

Розвідка відкритих джерел даних (з англ. – Open Source Intelligence, далі – OSINT) може бути помічною для різних організацій, включаючи: уряди, бізнес, наукові установи; а також може допомогти журналістам та фахівцям із кібербезпеки отримувати важливу інформацію про конкурентів, партнерів, клієнтів, ринки, загрози, можливості тощо. OSINT також може допомогти звичайним людям перевіряти факти, захищатися від дезінформації, підвищувати свою обізнаність та навички. Проте OSINT також може бути використаний для зловмисних цілей, таких як соціальна інженерія, шпигунство, крадіжка даних тощо. З огляду на це, дослідження теми OSINT викликає значну зацікавленість у вчених, які працюють у різних галузях: військовій, політичній, соціологічній, психологічній та ін., задля підвищення наукового рівня та якості його застосування.

Збір, аналіз та поширення інформації, доступної для громадськості та не захищеної грифами секретності, становлять основу OSINT. У сучасний час цей метод використовується різними установами, включаючи урядові структури, бізнес та неприбуткові організації. OSINT може бути використаний задля гарантування різноманітних інтересів тих чи інших суб’єктів, таких як забезпечення кібербезпеки, проведення досліджень ринку, підтримка журналістської діяльності, а також для потреб розвідки тощо. На ринку існує велика кількість інструментів та ресурсів для застосування OSINT у різних галузях, таких як OSINT Framework, OSINT Dojo та інші. Для успішного

здійснення збору та аналізу даних з відкритих джерел необхідно мати відповідні навички та дотримуватися відповідних принципів та підходів [1].

OSINT – це захоплива та важлива тема, яка знаходить своє застосування в різних сферах життя:

– Урядове та військове використання. OSINT дозволяє отримувати інформацію щодо політичної, економічної та військової ситуації в різних країнах, виявляти можливі загрози та конфлікти. Цей інструмент також допомагає виявляти та протидіяти дезінформації, пропаганді та кібератакам;

– Бізнес. OSINT є важливим для дослідження ринку, конкурентів, клієнтів та партнерів. Він також допомагає виявляти нові можливості та ризики, а також забезпечує захист від шахрайства, крадіжок даних та репутаційних збитків;

– Журналістика. OSINT є незамінним для журналістів у пошуках та перевірці фактів, джерел та свідків. Він також допомагає виявляти нові теми та історії, а також розкривати корупцію, злочинність та факти порушення прав людини;

– Наука та освіта. OSINT є важливим інструментом для науковців та студентів, який допомагає знаходити та аналізувати дані з різних галузей знань. Він сприяє співпраці з колегами та експертами, а також сприяє розвитку критичного мислення, навичок пошуку та оцінки інформації [2].

OSINT та кібербезпека тісно переплетені, оскільки використовують інформацію для досягнення своїх цілей. OSINT є ефективним інструментом у забезпеченні кібербезпеки. Проте може бути присутній і зворотній ефект: кіберзлочинці можуть ефективно використовувати публічну інформацію для виявлення слабких місць у системах безпеки організацій та для проведення втручання у їхню діяльність. З іншого боку, експерти з кібербезпеки можуть успішно застосовувати OSINT для виявлення потенційних загроз та розробки стратегій захисту:

– Виявлення та аналіз кібератак. OSINT допомагає виявляти джерела, методи, мотивації та наслідки кібератак, а також ідентифікувати та відстежувати зловмисників. Використання OSINT також полегшує аналіз вразливостей, шкідливого програмного забезпечення, команд та контрольних серверів, а також інших аспектів кібератак;

– Збір та перевірка інформації про цілі. OSINT допомагає збирати та перевіряти інформацію про потенційні цілі кібератак, такі як організації, особи, системи, мережі, домени, адреси IP, електронні адреси, паролі, сертифікати, ключі та інше. За допомогою OSINT можна виявити зв’язки, залежності, конфігурації, версії, протоколи, порти, служби, процеси, файли та інші деталі;

– Оцінка та підвищення рівня безпеки. OSINT дозволяє провести

оцінку та підвищити рівень безпеки власних або клієнтських систем, мереж, даних та програм. Використання OSINT також допомагає виявити та усунути потенційні ризики, слабкі місця, помилки, конфлікти, невідповідності та порушення [4].

OSINT також грає важливу роль у соціальній інженерії – процесі використання інформації для маніпулювання або впливу на людей, організації або системи. Використання OSINT для соціальної інженерії включає в себе знаходження потенційних цілей, дослідження їхніх вразливостей та створення переконливих сценаріїв. OSINT стає у пригоді соціальним інженерам для знаходження потенційних цілей, дослідження їхніх інтересів, звичок, контактів, вразливостей, слабких місць тощо. OSINT також може допомогти соціальним інженерам створювати переконливі сценарії, повідомлення, веб-сайти, документи, зображення тощо, які будуть викликати довіру або спонукати цілі до певних дій. Однак, OSINT також може бути використаний для захисту від соціальної інженерії, наприклад, шляхом перевірки джерел інформації, використання сильних паролів, застосування шифрування, оновлення програмного забезпечення, освіти та підвищення обізнаності користувачів [3].

OSINT – це процес збору, аналізу та використання публічної інформації для різних цілей. OSINT може бути використаний для розвідки, журналістики, забезпечення кібербезпеки, дослідження ринку, в освітніх цілях тощо. OSINT вимагає засвоєння відповідних навичок, підходів та етики. Це невід'ємна частина життя сучасного освіченого суспільства не лише у площині державної чи політичної діяльності, а й у контексті більш буденних практик, адже навички OSINT можуть бути застосовані і у повсякденному житті. Перспективи подальшого розвитку та дослідження OSINT полягають у застосуванні штучного інтелекту, покращенні якості та достовірності джерел, а також розробці нових методів та засобів аналізу й пошуку відкритої інформації.

Список використаних джерел

1. What is OSINT (Open-Source Intelligence?). *SANS Institute. Cyber Security Training.* URL: https://www.sans.org/blog/what-is-open-source-intelligence/ (date of access: 16.01.2024);

2. OSINT – що це таке, суть, визначення та приклади, види, методи та інструменти розвідки на основі відкритих джерел. *Termin.in.ua.* URL: https://termin.in.ua/osint-rozvidka-na-osnovi-vidkrytykh-dzherel/ (дата звернення: 16.01.2024)

3 Базовий OSINT курс від Molfar. *OSINT-спільнота Molfar*. URL: https://www.udemy.com/course/osint-molfar/ (дата звернення: 16.01.2024);

4. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник / Зоренко Д., Лех Р, Кулик Д.,

Червяков О. Харків : ІПЮК для СБУ, 2023. 36 с.

Гончар Аліна
Здобувач другого рівня вищої освіти.
Черкаський національний університет імені Богдана Хмельницького

РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Реалізація державної інформаційної політики - це процес впровадження та виконання стратегій, програм, законів та інших нормативних актів, спрямованих на управління інформаційним простором держави з метою забезпечення національної безпеки, розвитку суспільства та забезпечення прав та інтересів громадян. Цей процес включає в себе розробку стратегій та планів дій, створення відповідної інфраструктури, впровадження технологічних інновацій, контроль за дотриманням законодавства у сфері інформаційної безпеки та інші заходи, спрямовані на ефективне управління інформаційними ресурсами держави [1].

Реалізація державної інформаційної політики враховує внутрішні та зовнішні фактори, політичні, економічні, соціальні та технологічні аспекти, а також потреби та інтереси різних суб'єктів суспільства. Розглянемо детально кожен із них:

1. Внутрішні та зовнішні фактори. Це означає, що вплив на реалізацію державної інформаційної політики може відбуватися як зсередини країни (внутрішні фактори), так і ззовні (зовнішні фактори), такі як міжнародні стандарти, технологічний прогрес тощо.
2. Політичні аспекти. Включає в себе рішення та стратегії, які приймаються політичними органами, законодавство, політичні пріоритети та цілі, а також міжнародні відносини.
3. Економічні аспекти. Реалізація інформаційної політики може бути обмежена або сприяти економічному розвитку країни. Витрати на розвиток інформаційних технологій, забезпечення кібербезпеки та інші аспекти можуть бути важливими в економічному плані.
4. Соціальні аспекти. Включає в себе питання медіаграмотності, свободи слова, захисту прав людини, доступ до інформації для різних соціальних груп тощо.
5. Технологічні аспекти. Розвиток технологій, зокрема інформаційних та комунікаційних, штучного інтелекту, кібербезпеки, також має великий вплив на реалізацію державної інформаційної політики.