ПИР-Центр – МГИМО МИД России

МЕТОДОЛОГИЯ И ПРАКТИКА РАЗВЕДКИ ДАННЫХ ПО ОТКРЫТЫМ ИСТОЧНИКАМ (OSINT) ПРИМЕНИТЕЛЬНО К ИССЛЕДОВАНИЯМ В ОБЛАСТИ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ, КОНТРОЛЯ НАД ВООРУЖЕНИЯМИ И НЕРАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ

Серия «Доклады ПИР-Центра. № 44»

ПИР-Центр – МГИМО МИД России

Методология и практика разведки данных по открытым источникам (OSINT) применительно к исследованиям в области международной безопасности, контроля над вооружениями и нераспространения оружия массового уничтожения

Методическое пособие для студентов магистерской программы «Международная безопасность»

С.Д. Семенов

Серия «Доклады ПИР-Центра. № 44»

Москва
2025

Рецензенты:
Бужинский Евгений Петрович, кандидат военных наук, Председатель ПИР-Центра, Вице-президент РСМД, генерал-лейтенант (в отставке)

Цуканов Леонид Вячеславович, кандидат политических наук, консультант (Проекты «Перспективы и потенциал сотрудничества России с государствами Африки в вопросах глобальной безопасности и высоких технологий» и «Перспективы и потенциал сотрудничества России с государствами Персидского залива в вопросах глобальной безопасности и высоких технологий» Блока «Научные исследования и прикладной анализ»), ПИР-Центр

Левицкий Станислав Григорьевич, директор странового офиса госкорпорации «Росатом» в Беларуси, подполковник запаса

Подготовил:
Семенов Сергей Дмитриевич, научный сотрудник, ПИР-Центр

Научный руководитель:
Орлов Владимир Андреевич, директор и основатель, ПИР-Центр; профессор кафедры ПАМП, МГИМО МИД России

Данное методическое пособие подготовлено в рамках реализации совместного проекта ПИР-Центра и МГИМО МИД России «Глобальная безопасность, стратегическая стабильность и контроль над вооружениями» под эгидой Программы стратегического академического лидерства «Приоритет-2030».

Данное методическое пособие (доклад) доступно для скачивания по ссылке:

Серия «Доклады ПИР-Центра» (№ 44)

ОГЛАВЛЕНИЕ

Значительная часть нашей работы либо бесполезна, либо дублируется открытыми средствами информации. Разница и проблема заключаются лишь в том, что спецслужбы призваны не просвещать широкую публику, а обслуживать свои правительства. А правительства, как и мы все, доверяют только тому, за что заплатили, и с подозрением относятся к бесплатному сыру.

Джон Ле Карре[1]

Введение

Функция разведки – вскрывать неизвестное. Разведка данных по открытым источникам (OSINT, от англ. Open Source Intelligence), как следует из названия, использует для этого общедоступные источники информации: газеты и телевидение, Google и социальные сети – всё вплоть до страниц на форумах «доброго времени суток».

Для студента, научного работника, журналиста зачастую иных источников и не предполагается: другие виды разведки (например, HUMINT – от англ. *Human Intelligence*, классическая «человеческая» разведка или SIGNINT – от англ. *Signal Intelligence*, радиоэлектронная разведка) доступны только сотрудникам соответствующих компетентных органов. Для качественного исследования это, впрочем, необязательно. Как следует из приведенной выше цитаты Джона Ле Карре, для точных и выверенных оценок геополитической обстановки в большинстве случаев хватает прессы и журналов.

Вместе с тем, очевидно, что в военно-политической области традиционного подхода – открыть все ссылки на первых пяти страницах выдачи в Google – недостаточно. Поверхностность и компилятивность - недостатки многих работ молодых и не только авторов, специализирующихся на проблематике контроля над вооружениями, разоружения и нераспространения ОМУ (КВРН). Не отрицая значимости качественного обзора уже имеющихся трудов, следует помнить: ценность научного исследования определяется количеством и качеством материалов, впервые введенных в научный оборот.

Это особенно важно для тех студентов, которые рассматривают для себя возможность построения карьеры в госорганах или в аналитике для госструктур. Ключевые экспертные и новостные публикации руководителям уже известны: и по сводкам новостей, и по информации из закрытых каналов. Действительный интерес вызывают те бумаги, где автор может удивить новым поворотом мысли или фактом, который доселе был не на виду.

Преимущество OSINT – в возможности привлекать нестандартные источники информации, в т.ч. для дополнения и перепроверки традиционных: прессы, телевидения, официальных сообщений и т.д. Разведка по открытым источникам предполагает работу с широким массивом сведений, представляющих потенциальный интерес: спутниковыми снимками, фотографиями, видеороликами и социальными сетями.

[1] Дж. Ле Карре. Маленький городок в Германии. Секретный паломник. М.: Аст, С. 166.

Было бы преувеличением назвать OSINT изобретением последних лет. В специальных ведомствах этому направлению издавна уделяется большое внимание. Как отмечал один из самых видных руководителей советской и российской внешней разведки В.А. Кирпиченко, «День разведчика начинается с чтения газет»[2]. Широкую известность получил пример того, как ЦРУ США смогли установить местонахождение советских атомных объектов по фотографии в журнале «Огонёк»[3].

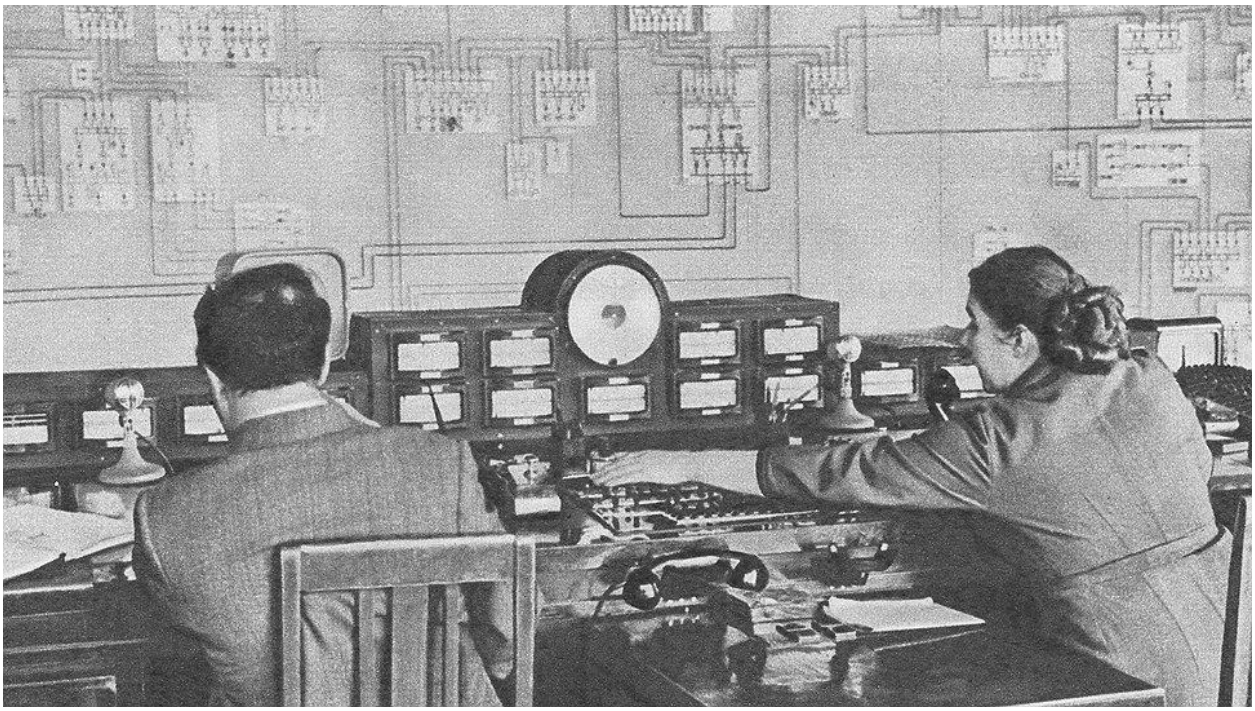

Рис. 1. Фотография диспетчерского пункта Уралэнерго в журнале «Огонёк». На её основе аналитики ЦРУ смогли установить расположение ключевых промышленных объектов в регионе.

В то же время распространение цифровых технологий открыло совершенно новые возможности для ведения разведки по открытым источникам. Как отмечает руководитель консалтинговой компании «Масалович и Партнёры» Андрей Масалович, в современном мире фиксируется каждый шаг человека. Соответственно, это даёт больше возможностей по вскрытию ранее недоступной информации.

Основной фокус негосударственного применения OSINT – что в России, что за рубежом – экономическая безопасность (поиск информации о контрагенте, осуществление т.н. «должной осмотрительности»), маркетинговые исследования и информационная безопасность (профилирование угроз, тестирование на проникновение, и т.д.). Созданы и активно развиваются онлайн-сообщества по интересам, проводятся конференции и учебные курсы. Более подробно эта тема будет освещена в следующем разделе.

Те же инструменты вполне применимы и для аналитики в области КВРН. В США одним из основоположников этой работы стал Центр исследования проблем нераспространения им. Джеймса Мартина (James Martin Centre for Nonproliferation Studies, г. Монтерей, штат

[2]А. Бондаренко. Разведка – дело профессионалов. СВР России. Режим доступа: http://svr.gov.ru/smi/2002/09/krzv20020925.htm (дата обращения 18.12.2024)
[3] Studies in Intelligence. Volume II. Issue: Summer. Year: 1967

Калифорния). В их портфолио – обнаружение потенциальных позиционных районов китайских МБР (на основе спутниковых снимков)[4], анализ ситуации вокруг иранской ракетной программы (на основе спутниковых снимков), вычисление ТТХ северокорейских МБР (на основе фотоснимков с парадов военной техники)[5].

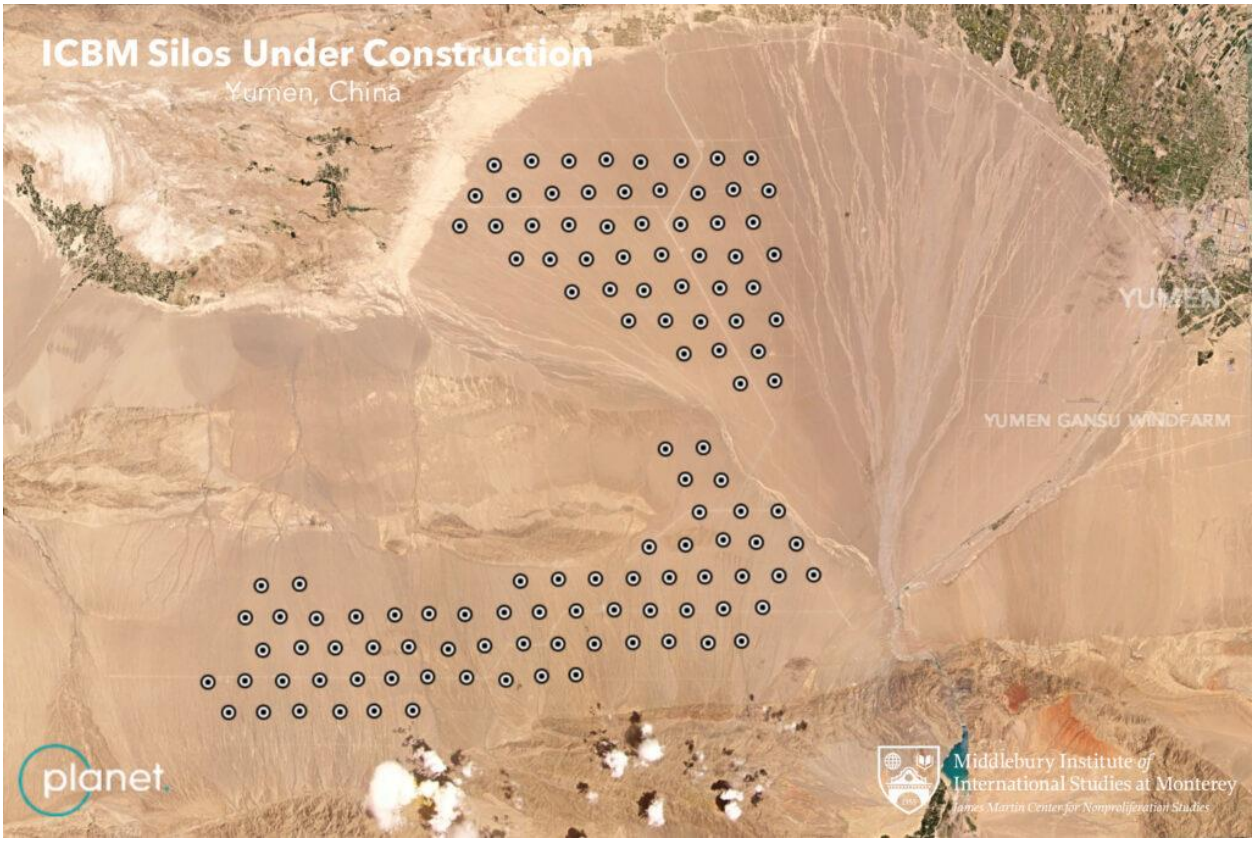

Рис.2. Предполагаемые (по оценкам американских специалистов) позиционные районы МБР в Китае. Источник: armscontrolwonk.com

В числе «передовиков» также можно выделить Федерацию американских учёных (делают упор на стратегическую тематику, флагманский материал – Nuclear Notebook), венскую Open Nuclear Network (финансируется США, акцент на северокорейское ракетно-ядерное досье), Institute for Science and International Security (специализируются на вопросах иранской ядерной программы, отличаются тенденциозной подачей материала в русле политических установок Республиканской партии США), Institute for Study of War (военный ресурс, заметен детальным освещением событий вокруг специальной военной операции с «западной колокольни»), а также Bellingcat (признан в Российской Федерации нежелательной организацией).

[4] Jeffrey Lewis. Chinese ICBM Silos. Arms Control Wonk. URL: https://www.armscontrolwonk.com/archive/1212340/chinese-icbm-silos/ (дата обращения: 18.12.2024)

[55] См. например: Max Fisher, The Hidden Messages in North Korea's Military Parade. New York Times. April 18, 2017. URL: https://www.nytimes.com/2017/04/18/world/asia/north-korea-parade-missiles.html (дата обращения 18.12.2024)

В России при анализе военно-политической проблематики технологии OSINT наиболее активно применяют авторские команды телеграм-каналов «Рыбарь» [6] и «Ватфор»[7]. Вместе с тем, количество авторов, использующих OSINT в научной работе по тематике КВРН пока невелико. Соответственно, существует риск складывания зависимости отечественных исследований от западного прочтения «открытых исходников». Исходя из этого был задуман курс для студентов МГИМО МИД России, который бы дал представление об OSINT как можно большему числу начинающих исследователей.

Это методическое пособие разработано в помощь студентам МГИМО МИД России, изучающим курс «Разведка данных по открытым источникам». Предлагаемый материал ориентирован на решение следующих задач:

1. Дать общее представление об открытых источниках информации, основных принципах и инструментах работы с ними;
2. Показать возможности базовой автоматизации при проведении OSINT-исследований;
3. Продемонстрировать общие принципы анализа информации и написания аналитического доклада по открытым источникам;
4. Предоставить читателю набор правил по обеспечению собственной безопасности при работе с OSINT.

Автор намеренно не приводит историю применения OSINT в годы холодной войны и после, поскольку цель настоящего пособия – подготовить практиков, а не специалистов по феномену OSINT в современном методологическом дискурсе.

[6] Рыбарь. Telegram. URL: https://t.me/s/rybar (дата обращения 18.12.2024)
[7]Ватфор | Автострадный think tank. Telegram. URL: https://t.me/s/vatfor (дата обращения 18.12.2024)

1. Роль и место OSINT в исследовательской работе по вопросам КВРН. Общие правила методологии. Формулирование гипотезы и постановка исследовательского вопроса (ТЗ)

Идея этого пособия возникла при написании аналитического доклада ПИР-Центра «Новая *ядерная девятка*: перспективы ядерного распространения в мире»[8]. При его подготовке авторский коллектив ПИР-Центра столкнулся с ограниченностью источниковой базы для анализа рисков и угроз для режима нераспространения ядерного оружия. Основные сведения черпались из газет и профильных изданий, заявлений политиков и материалов официальных веб-сайтов что, очевидно, оставляло «слепые пятна».

Один из методологических выводов, сделанных по итогам той работы: по газетам и высказываниям можно оценить намерения. Для оценки потенциалов требуются более надёжные и объёмные источники информации.

В сфере нераспространения ядерного оружия и контроля над вооружениями OSINT может использоваться для выявления и мониторинга деятельности по наращиванию ядерной инфраструктуры, разработке и развёртыванию перспективных систем вооружения, определения их тактико-технических характеристик.

Среди ярких случаев применения открытых источников в ракетно-ядерной сфере: обнаружение американскими специалистами потенциальных позиционных районов китайских МБР (на основе спутниковых снимков), анализ ситуации вокруг иранской ракетной программы (на основе спутниковых снимков), вычисление ТТХ северокорейских МБР (на основе фотоснимков с парадов военной техники).

Методология

Как и в любом исследовании, работа с использованием OSINT-инструментария начинается с постановки исследовательского вопроса.

Хорошая методика – выявлять пробелы (gap analysis) в массивах уже имеющейся информации. В соответствии с ней, предварительную работу можно выстроить в четыре такта:

1. Понять, что мы уже знаем;
2. Попытаться сделать предварительные выводы на основе имеющейся информации;
3. Определить вопросы, требующие уточнения;
4. Предположить, где можно найти требуемые данные[9].

Главное правило OSINT-исследования - тщательно документировать процесс и найденные результаты. Неорганизованные заметки или их отсутствие могут привести к тому, что всю

[8] Новая ядерная девятка? Оценка угроз распространения ядерного оружия в мире. Доклад. Издание 2-е (исправленное и дополненное) / Ред. В.А. Орлов, С.Д. Семенов. М.: ПИР-Пресс, 2023. – 230 с. – (ПИР-Библиотека - книжная серия). Режим доступа: https://pircenter.org/editions/new-nuclear-nine-report/

[9] Rae Baker. Exploring the Real-World Value of Open Source Intelligence. Wiley, 2023. P 34

работу придётся переделывать в случае появления вопросов к тому или иному положению исследования. Среди лучших практик:

- Всегда исходить из того, что заметки придётся показывать кому-то ещё (научному руководителю, главе авторского коллектива, редактору и т.д.);
- В случае скриншотов – делать пояснения;
- Всегда записывать ссылки;
- Фиксировать дату и время описываемых событий;
- Отображать конкретные инструменты поиски и зацепки.

2. Литература и источники: как и где учиться OSINT?

В рамках одного методического материала невозможно покрыть всё многообразие тем, связанных с разведкой данных по открытым источникам. На одном только ресурсе OSINT Framework[10] приведено более 100 инструментов, направленных на поиск информации в открытых источниках. Пользователи GitHub[11] и вовсе выделяют 1140 инструментов и ресурсов в этой области.

Основная задача, которую автор методического пособия ставит перед собой – снабдить исследователя общим пониманием методики работы по открытым источникам и предоставить основу для дальнейшего самосовершенствования. В то же время практика остаётся единственно верным критерием истины. При выборе конкретного набора инструментов целесообразно «плясать» от поставленной задачи и идти от простого к сложному.

Ниже приведён список литературы и ресурсов, которые будут полезны при проведении OSINT-исследований, в т.ч. с точки зрения расширения используемого инструментария. Этот перечень не носит исчерпывающего характера и предназначен лишь для сокращения времени на поиск практических руководств.

Отметим, что на момент написания этого методического материала доступ к некоторым из нижеперечисленных ресурсов заблокирован на территории Российской Федерации. Автор упоминает их исключительно в справочных целях и призывает неукоснительно придерживаться требований российского законодательства при проведении OSINT-исследований (см. подробнее раздел 12).

2.1. Литература

Профильный портал OSINT Library[12] насчитывает, как минимум, 184 публикации по вопросу разведки по открытым источникам. Недостаток этого ресурса в том, что упоминаемые там статьи и книги не распределены по годам и темам. При подготовке этой методички автор попытался отобрать наиболее актуальные и нужные работы, сгруппировав их по конкретным сюжетам. При этом, поскольку данный курс ориентировал на российских исследователей, приоритет отдавался книгам и статьям, выпущенным за последние 5-7 лет и находящимся в открытом доступе[13].

[10] Удобен группировкой инструментов поиска по категориям. OSINT Framework. URL: https://osintframework.com/ (дата обращения 15.11.2024)

[11] Awesome OSINT. Github. URL: https://github.com/jivoi/awesome-osint (дата обращения 15.11.2024)

[12] OSINT Library. Blockint: Research, Consulting, Training. URL: https://www.blockint.nl/the-osint-library/ (дата обращения 15.11.2024)

[13] Автор методического руководства и ПИР-Центр ни в коем случае не поощряют использование работ, размещенных в открытом доступе в нарушение авторских прав, в частности, на ресурсах Z-Library и Library Genesis.

Общие руководства и учебники по OSINT:

1. Akhgar, B., Bayerl, P. & F. Sampson (eds.) (2016) Open Source Intelligence Investigation: From Strategy to Implementation. Springer.
2. Bazzell, M. (2020) Extreme Privacy. What it takes to Disappear. (2nd edition. NB: 3rd edition coming soon, already available via Amazon US).
3. Bazzell, M. (2022) Open Source Intelligence Techniques. Resources for Searching and Analysing Online Information (10th edition).
4. Chauhan, S. and N. Panda (2015) Hacking Web Intelligence – Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Syngress.
5. Hassan, N. and R. Hijazi (2018) Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress.
6. Shamaeva, I. and Galley, D.M. (2021) Custom Search – Discover more: A Complete Guide to Google Programmable Search Engines. Taylor & Francis Ltd.
7. Appel, E. (2011). *Internet Searches for Vetting, Investigations, and Open-Source Intelligence*. CRC Press.
8. Ashdown, N. (2022) Public Open Source Analysis and Intelligence: Practice, Terminology, and Ethical Considerations. Stanley Center for Peace and Security.
9. Dubberley, S., A. Koenig and D. Murray (eds) (2019) *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford Public International Law.
10. European Open Source Intelligence Organisations Observatory (2023) *Guidelines for Public Interest OSINT Investigations*. Available at: https://obsint.eu/wp-content/uploads/2023/04/Guidelines-for-Open-Source-Intelligence-Organisations.pdf.
11. Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2020) 'Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence', in *Journal of Applied Security Research*, 16(3), 345–369.
12. Fernandez, M., A. Millington, M. Monday and E. Sarpa (2019) *Elementary… the Art and Science of Finding Information.* BookLocker: St. Petersburg, USA.
13. Joint Military Intelligence Training center (1996) *Open Source Intelligence: Professional Handbook.* Department of Defense.
14. NATO (2002) *Open Source Intelligence Handbook.*
15. NATO (2002) *Open Source Intelligence Reader*.
16. NATO (2002) *Intelligence Exploitation of the Internet*.
17. Pouchard, L., J. Dobson and J. Trien (2007) *A Framework for the Systematic Collection of Open Source Intelligence*. Oak Ridge National Laboratory.
18. Reuser, A.H.P. (2017) 'The RIS Open Source Intelligence Cycle', *Journal of Mediterranean and Balkan Intelligence,* Vol. 10(2): pp. 29-44.
19. Richey, M. and M. Binz (2015) 'Open Source Collection Methods for Identifying Radical Extremists Using Social Media', *International Journal of Intelligence and CounterIntelligence,* 28:2, 347-364.

20. U.S. Army (2006) Open Source Intelligence. Field Manual Interim No. 2-22.9. Washington, DC.

21. U.S. Army (2012) *ATP 2-22.9 Open-Source Intelligence*. Headquarters, Department of the Army.

22. U.S. Army (2013) JP 2-0 Joint Intelligence. Chiefs of Staff, United States Army.

23. Wilson, H., O. Samuel and . Plesh (2024) Open Source Investigations in the Age of Google. World Scientific.

24. Zhang, Y., R. Frank, N. Warkentin and N. Zakimi (2022) 'Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure', in *Journal of Cybersecurity*,8(1): pp. 1–15.

25. OSINT Investigations. We know what you did that summer. By Information Warfare Center.

26. Dale Meredith. The OSINT Handbook 2024.

27. Open Source Intelligence 101: From Novice to Expert 2023.

28. Hassan, N. A., & Hijazi, R. (2018). Open Source Intelligence Methods and Tools. Apress. URL: https://doi.org/10.1007/978-1-4842-3213-2.

29. Wiil, U.K. (2011). Counterterrorism and Open Source Intelligence: Models, Tools, Techniques, and Case Studies. In: Wiil, U.K. (eds) Counterterrorism and Open Source Intelligence. Lecture Notes in Social Networks. Springer, Vienna. URL: https://doi.org/10.1007/978-3-7091-0388-3_1.

Нераспространение:

1. Green, D. (1993) Monitoring Technology Proliferation. An open source methodology for generating proliferation technology. Thesis Naval Postgraduate School, Monterey, CA.

2. Townsend, R. (1993) 'Deception and Irony: Soviet Arms and Arms Control', in American Intelligence Journal, Spring/Summer 1993, pp. 47-53.

3. U.S. Department of Defence (2021) Dictionary of Military and Associated Terms. Washington, DC.

4. Photo Interpretation Student Handbook. Defense Mapping Agency. March 1966. URL: https://bpb-us-e2.wpmucdn.com/sites.middlebury.edu/dist/f/5986/files/2012/07/Photo-Interpretation-Student-Handbook.-Photo-Interpretation-Principles.pdf.

5. Открытый доклад СВР России за 1993 год. Новый вызов после "холодной войны": распространение оружия массового уничтожения. М.: СВР России. 99 с. URL: http://svr.gov.ru/upload/iblock/0a2/ОТКРЫТЫЙ%20ДОКЛАД%20СВР%20РОССИИ%203А%201993%20ГОД.pdf.

6. Новая *ядерная девятка*? Оценка угроз распространения ядерного оружия. в мире. Доклад. Издание 2-е (исправленное и дополненное) / Ред. В.А. Орлов, С.Д. Семенов. М.: ПИР-Пресс, 2023. – 230 с. – (*ПИР-Библиотека* – книжная серия). URL: https://pircenter.org/wp-content/uploads/2023/01/23-01-26-NINE-2nd-edition.pdf

Исторические аспекты OSINT:

1. Bagnall, J. (1958) ‘The Exploitation of Russian Scientific Literature for Intelligence Purposes‘, *Studies in Intelligence,* Vol 2(3): pp. 45-49.
2. Becker, J. (1957) ‘Comparative Survey of Soviet and US Access to Published Information‘, *Studies in Intelligence,* Vol 1(4): pp. 35-46.
3. Block, L. (2023) ‘The Long History of OSINT’, in *Journal of Intelligence History*
4. Calkins, L. (2011) ‘Patrolling the Ether: US–UK Open Source Intelligence Cooperation and the BBC’s Emergence as an Intelligence Agency, 1939–1948’, *Intelligence and National Security* Vol. 26(1): pp. 1–22.
5. Colquhoun, C. (2016) A Brief History of Open Source Intelligence. Bellingcat.
6. Croom, H. (1969) ‘The Exploitation of Foreign Open Sources’, *Studies in Intelligence* (Summer 1969-declassified article): 129–30.
7. Hastedt, G. (2009) ‘Intelligence Estimates: NIEs vs. the Open Press in the 1958 China Strait Crisis’, in *International Journal of Intelligence and CounterIntelligence,* Vol. 23(1): 104–132.
8. Schaurer, F. And J. Storger (2010) *The Evolution of Open Source Intelligence*. International Relations and Security Network (ISN), ETH Zurich.
9. Sibbet, D. (1993) ‘Commercial Remote -Sensing: Open Source Imagery Intelligence’, in *American Intelligence Journal,* Spring/Summer 1993, pp. 37-40.

Использование OSINT спецслужбами:

1. Bureau of Intelligence and Research (2024) *Open Source Intelligence Strategy.* State Department, Washington D.C.
2. Eldridge, C., C. Hobbs & M. Moran (2018) ‘Fusing algorithms and analysts: open-source intelligence in the age of ‘Big Data’, *Intelligence and National Security,* 33(3): pp. 391-406.
3. Flamer, N. (2023). ‘The enemy teaches us how to operate’: Palestinian Hamas use of open source intelligence (OSINT) inits intelligence warfare against Israel (1987-2012). *Intelligence and National Security,*
4. Hatfield, J.M. (2023) ‘There is No Such Thing as Open Source Intelligence’, in *International Journal of Intelligence and CounterIntelligence*.
5. Janjeva, A., A. Harris and J. Byrne (2022) *The Future of Open Source Intelligence for UK National Security*. Royal United Services Institute (RUSI).
6. Miller, B.H. (2018). ‘Open source intelligence (OSINT): An oxymoron?’, *International Journal of Intelligence and Counterintelligence,* Vol. 31(4), pp. 702-719.
7. Murray, D., Y. McDermott and K. Alexa Koenig (2022) ‘Mapping the Use of Open Source Research in UN Human Rights Investigations‘, in Journal of Human Rights Practices, 2022, 1-28.

8. Oakley, D. P. and J. Rogg (2024) ‘Spreading the “smog of war”: the impact of propaganda, social media, and OSINT on U.S. civil-intelligence relations’, in *Journal of Intelligence and National Security.*

9. Oerlemans, J. and S. Langenhuijzen (2024) ‘Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices’, in International Journal of Intelligence and CounterIntelligence.

10. Ogar, S. (2019) *Covert Networks – A comparative study of Intelligence Techniques used by Foreign Intelligence Agencies to Weaponize Social Media*. MA Thesis Johns Hopskins University, USA.

11. Pringle, Robert W. (2003) ‘The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989’, *International Journal of Intelligence and Counterintelligence*, Vol. 16(2): pp. 280-289.

12. Waltz, E. (2003) *Knowledge Management in the Intelligence Enterprise*. Artech House.

13. Ziolkowska, A. (2018) ‘Open Source Intelligence (OSINT) as an element of Military recon’, in *Security and Defence Quarterly,* 19(2).

Правовые аспекты:

1. Block, L. (2021) GDPR essentials for OSINT research.

2. Department of Justice Cybersecurity Unit (2020) *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources*. Washington, Computer Crime & Intellectual Property Section Criminal Division U.S. Department of Justice.

Анализ информации:

1. Director of National Intelligence (2015) *Analytic Standards, Intelligence Community Directive 203*.

2. Irwin, D. and D. Mandel (2019) ‘Improving information evaluation for intelligence production’, *Intelligence and National Security*, Vol. 34(4): pp. 503-525.

3. Kivimäki, V. (2023) ‘Open-source information for intelligence purposes: The challenge of disinformation’, in Arcor, R., I. Chiru and C. Ivan (eds.) *Routledge handbook of disinformation and national security*. New York: Routledge.

4. Lowenthal, M. (2001) ‘OSINT: The State of the Art, the Artless State‘, in *Studies in Intelligence*, 45(3), 61–66.

5. NATO (2018) ‘Communicating Uncertainty, Assessing Information Quality and Risk, and Using Structured Techniques in Intelligence Analysis’, proceedings of the *SAS-114 Workshop* held from 5-7 December 2016 in Copenhagen, Denmark.

6. Omand, D. (2020) *How Spies Think: Ten Lessons in Intelligence*.

7. Pherson R. and R. Heuer (2020) *Structured Analytic Techniques*. Sage, London.

8. Psychology of Intelligence Analysis

Написание текстов:

1. William Strunk, Jr. Elements of Style. New York: Harcourt, Brace and Company. 1918

2. M. Patrick Hendrix and James S. Major. Communicating with Intelligence: Writing and Briefing for National Security, Third Edition. Rowman and Littlefield. 2022. 310 p.

3. Пиши, сокращай: Как создавать сильный текст / Максим Ильяхов, Людмила Сарычева. 2-е изд. – М.: АП, 2017. - 440 с.

2.2. Интернет-ресурсы

1. Learn New Tools. James Martin Center for Nonproliferation Studies. URL: https://learn-new-tools.org/.

2. Awesome OSINT. GitHub. URL: https://github.com/jivoi/awesome-osint?tab=readme-ov-file.

3. Bellingcat Toolbox. GitHub[14]. URL:https://bellingcat.gitbook.io/toolkit.

2.3. Телеграм-каналы и новостные рассылки

1. Open Source. URL: https://t.me/open_source_friend. Полезные инструменты для поиска по открытым источникам.

2. Social Engineering. URL: https://t.me/Social_engineering.

3. Investigation & Forensic TOOLS. URL: https://t.me/forensictools. Инструментарий для проведения расследований, криминалистических исследований, корпоративной разведки, и исследований в области безопасности. NB – очень полезный.

4. Наука и данные. URL: https://t.me/naukaidannye.

5. Северная Пальмира. URL: https://t.me/northern_palmyra.

6. Новости конкурентной разведки. URL: https://t.me/ci_newsblock. Хороший агрегатор.

7. Digital-Разведка & OSINT. URL: https://t.me/Digitalntelligence.

8. T.Hunter. URL: https://t.me/tomhunter.

9. Mycroft Intelligence. URL: https://t.me/mycroftintel. ТГ-канал консалтингового агентства «Масалович и партнёры».

10. Интернет-Розыск I OSINT I Киберрасследования. URL: https://t.me/irozysk.

11. Арсенал Безопасника. URL: https://t.me/arsenal_security. Больше про информационную безопасность.

[14] Bellingcat признана на территории Российской Федерации нежелательной организацией

12. Bafomëd OSINT 🛰 URL: https://t.me/osint_san_framework. Проект по обучению методикам OSINT и созданию разведывательных инструментов.

13. OSINT | Форензика. URL: https://t.me/osintkanal.

14. OSINT mindset. URL: https://t.me/osint_mindset.

15. data.csv. URL: https://t.me/data_csv. Визуализация данных.

16. STEIN: ИБ, OSINT. URL: https://t.me/secur_researcher.

17. Библиотека разведчика | Osint | Книги | Курсы. URL: https://t.me/books_osint. Единственная в своем роде библиотека по OSINT, сбору информации, технологиям конкурентной разведки, разведке в сетях и т.п.

18. Заметки OSINTера. URL: https://t.me/osint_data.

3. Основные правила работы с поисковыми системами

3.1. Гуглить надо с умом: Операторы поиска в Google и Yandex.

Получив задачу, начинающий специалист, как правило, обращается к поисковым системам: Google и Яндекс. Выдача результатов в таком случае позволяет составить общее представление о предмете изысканий.

Вместе с тем нередки случаи, когда искомая информация или отсутствует, или нуждается в проверке и уточнении. В этих ситуациях весьма полезен дополнительный функционал популярных поисковых систем. Ниже приведены основные инструменты, позволяющие «отфильтровать» результаты поиска в соответствии с заданными критериями в Google.

«кавычки» (“”)	Особенно актуально для поиска имён собственных, особенно часто употребимых.
AND	в поиск будут включены только результаты, содержащие оба термина
NOT (-)	исключает из поиска заведомо нерелевантные результаты
OR	расширяет поле поиска за счёт включения нескольких терминов (например, различных вариантов написания одного и того же имени/объекта)
site:	поиск по конкретному сайту или доменной группе (например, gov, edu)
filetype:	позволяет искать только конкретные типы файлов (pdf)
intitle:	поиск в заглавии
inurl:	поиск в адресной строке
link:	поиск страниц, которые ссылаются на определенный URL
cache:	просмотр кэшированной версии страницы

В целом похожие операторы работают и в других поисковиках, включая Яндекс и DuckDuckGo. Сочетание различных поисковых операторов называют “доркингом” (Google dorking). Полный список возможных комбинаций, позволяющих выйти на чувствительную информацию, можно найти на портале Google Hacking Database (ведётся с 2004 года)[15].

Использование таких операторов позволяет сократить время на выполнение рутинных работ, например, при поиске информации о конкретном человеке или организации.[16]

С учётом специфики исследований в области КВРН отдельное направление поиска – научные публикации с тем, чтобы отследить направление изысканий того или иного учреждения. Хрестоматийный пример в этой области – в 1940-х гг. советская внешняя разведка предположила, что в США приступили к военно-прикладной ядерной программе, поскольку из открытой научной печати исчезли материалы по этой теме.

[15] Google Hacking Database. Exploit Database. URL:https://www.exploit-db.com/google-hacking-database (дата обращения: 12.12.2024)
[16] Пример проверки контрагента с использованием доркинга: T.Hunter. Google Dorking. Если ты сотрудник СБ компании. Habr.ru. URL: https://habr.com/en/companies/tomhunter/articles/698568/

Для мониторинга научной активности исследовательских институтов стран коллективного Запада достаточно использовать ресурсы Google Scholar, Scopus, Web of Science и др. Относительно новый ресурс – поисковик на основе искусственного интеллекта Consensus, индексирующий англоязычные научные публикации с применением искусственного интеллекта[17].

Разведка объектов в странах глобального большинства потребует большего тщания и поиска непосредственно по сайтам журналов и страницам указанных институтов.

3.2. Техники работы с поисковой выдачей

Частая проблема – дифференциация выдачи в зависимости от точности поискового запроса. Слова и термины в запросе должны отображать специфику искомой темы. Они должны как можно более однозначно указывать поисковику на область вашего текущего интереса. Не рекомендуется использовать предлоги и союзы: как правило, поисковый движок их просто игнорирует.[18]

Вместе с тем даже использование операторов и точно сформулированный запрос не гарантирует результата. Поисковые системы получают основной доход за счёт продажи рекламы: соответственно, они будут заинтересованы «подсветить» те результаты, которые потенциально могут принести прибыль. В таком случае поисковая выдача может потребовать дополнительной фильтрации.

Существует несколько техник уточнения поиска, которые могут быть использованы на этапе первоначального поиска данных.

Yo-yo *(от англ. yonder – отдаляться).* Результаты, отображаемые на первой странице поисковой выдачи, следует критически оценить. Если они не имеют ценности, перейти на середину выдачи (например, на 10 страницу из 20). Осмотреть результаты там. Если они релевантны запросу, двигаться «вверх»: на предыдущую страницу (т.е. на страницу 9 и т.д.). Если результаты на условной странице 10 нерелевантны, перейти на середину второй половины выдачи. Если они подходят, см. предыдущий шаг. Если же нет, то поисковик для данной задачи следует заменить и попробовать альтернативные поисковые системы, в т.ч. локально используемые в стране поиска (например, Baidu).

Синекдохический подход *(от названия стилистического приёма, предполагающего использование названия части вместо названия целого, частного вместо общего и наоборот)*. В таком случае изначальная выдача используется только в качестве «зацепки» для дальнейшего поиска по тематическим кластерам. Воспользуемся примером интернет-исследователя Fravia по поиску книги о хайку под редакцией Мундаррена[19].

1. Горизонтальный «региональный» срез. Мундаррена могли издавать не только во Франции, но и в издательствах других стран – ищем его там.

2. Горизонтальный «тематический» срез. Ищем издательство, занимающееся темой хайку. Мы можем обратиться к самому первоначальному издательству (в данном случае

[17]Consensus. URL: https://consensus.app/ (дата обращения 18.12.2024)
[18] Фравиа. С 17
[19] Фравиа. Там же. С. 20

международное отделение японской Kodansha) и через него узнать о множестве региональных кластеров.

3. Вертикальный «тематический» срез. Выявляем другие менее популярные слова на нашу тему, которые дадут кластеры результатов.

4. Вертикальный «синтаксический» срез. Во французском языке, которым пользуется наш редактор, слово «хайку» пишется с диэрезисом: haïku. Поэтому если искать именно в таком написании, мы останемся во франкоговорящей среде, однако передвинемся на совсем другой кластер – на сайты, где употребляют именно этот вариант. Использование прикольных спецсимволов, правильного перевода и транслитерации позволяет отрезать много лишнего. Или другой пример: искать по автору "Басё" можно и в транскрипции «Башо».

5. Вертикальный «метонимический» срез. Поиск смежных понятий. Первые найденные кластеры могут быстро вывести вас на новые стрелы-запросы, связанные с более глубокой тематической терминологией. Например: ренга – коллективные хайку, киго – хайку о временах года.

6. Поиск через контекст. Один из самых продуктивных приёмов поиска – вбивать прямые цитаты из источников, связанных с темой или ли же информацию, очерчивающую контекст искомого.

Важный момент – результаты поиска будут заведомо превышать ресурсы по их обработке. Это обуславливает необходимость самодисциплины: в любой момент проведения исследования следует держать в уме главную цель и не отвлекаться на малополезные частности.

3.3. Основы автоматизации поиска

Вышеперечисленные инструменты предполагают ручной поиск информации. Хотя ничто не может заменить человека в аналитическом процессе, поиск может быть автоматизирован с тем, чтобы сэкономить время и ресурсы.

При работе с большими объёмами информации, где предполагается извлечение однотипных данных, целесообразно использовать т.н. «парсеры». Наиболее функциональные из них настраиваются через соответствующие библиотеки на языке Python (например, BeautifulSoup, Scrapy) или Node.js (например, Cheerio). Существуют и более простые версии в формате браузерного расширения, которые не требуют навыков программирования. В их числе – Webscraper[20].

Для организации долгосрочного мониторинга избранных новостных ресурсов, аналитических центров, сайтов интересующих организаций и ведомств можно использовать RSS-ленты. Они позволяют агрегировать новости с различных источников в одном приложении. Для этого можно задействовать сервисы Feedfry[21] (не работает для мониторинга российских и белорусских сайтов) или Feedly[22].

[20] https://webscraper.io/
[21] https://feedfry.com/preview
[22] https://feedly.com/

Рис.3. Пример настройки RSS-ленты

4. Работа с официальными (государственными) базами данных: таможенная информация, поиск юрлиц, судебные дела, данные о собственности

В военно-технической и оборонной сфере ценным источником информации являются государственные порталы закупок, сайты таможенных и налоговых служб, реестры юридических лиц и собственности, онлайн-ресурсы судебных инстанций. На руку OSINT-исследователям играет принимаемое в странах коллективного Запада (и не только) законодательство в области «открытого правительства» и повсеместная цифровизация государственных услуг.

На примере США работу с государственными базами данных можно выстраивать по нескольким направлениям.

4.1. Информация о государственных закупках.

Принцип «следовать за деньгами» более чем актуален в данном случае. В соответствии с Законом о федеральном финансировании и ответственности (Federal Funding and Accountability Act of 2006, FFATA), на сайте USASpending.gov размещается информация о заключаемых государственных контрактах и предоставляемых субсидиях. На портале, в частности, можно найти информацию о стоимости заключаемых контрактов по линии конкретного ведомства или даже конкретной базы с указанием сроков реализации и конкретных субподрядчиков.

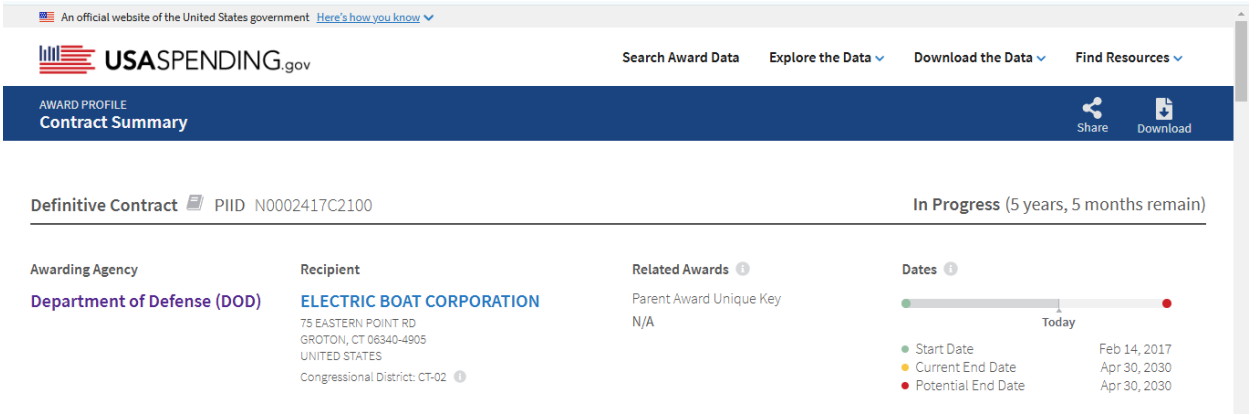

Рис. 4. Так выглядит карточка контракта на строительство АПЛ с ядерной силовой установкой класса «Колумбия». Указаны головной исполнитель, его местонахождение, а также ожидаемые сроки реализации проекта.

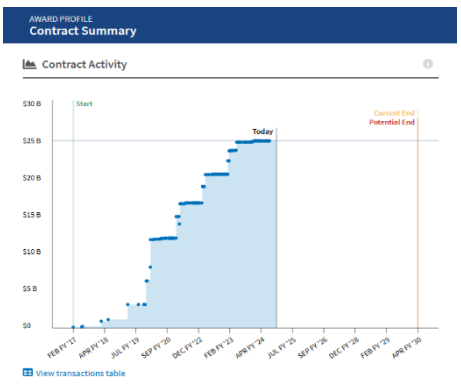

Рис. 5. Посредством портала можно отслеживать динамику выплат по конкретному проекту, производственную кооперацию по контрактам субподряда. В дальнейшем информацию о «смежниках» можно использовать как зацепку для поиска дополнительной информации об изучаемом объекте (в данном случае о головной АПЛ «Колумбия»).

4.2. Информация о судебных процессах

Интерес представляют судебные дела с участием конкретных юридических (или физических) лиц. В США основная информация по этим вопросам держится на уровне штатов. На первом такте целесообразно использовать агрегаторы – например, порталы Public Records Online, Netronline. Существует федеральная платформа PACER, которая, однако, является платной при поиске более 150 страниц в месяц. Обойти это ограничение можно за счёт использования браузерного расширения RECAP, которое позволяет находить документы по тому или иному заседанию, уже выложенные в открытый доступ.

4.3. Поиск по рассекреченным документам

В соответствии с законом о свободе информации (Freedom of Information Act, FOIA)[23] министерства и ведомства США рассекречивают даже чувствительную информацию по запросу граждан или по истечении срока давности. Это, в частности, относится к документам ФБР, ЦРУ, Минобороны, Государственного департамента, Министерства энергетики и других ведомств, принимающих участие в проведении внешней и оборонной политики. Хотя многие из представленных там документов имеют, скорее, историческую ценность, они могут быть полезны для понимания контекста формирования американской политики.

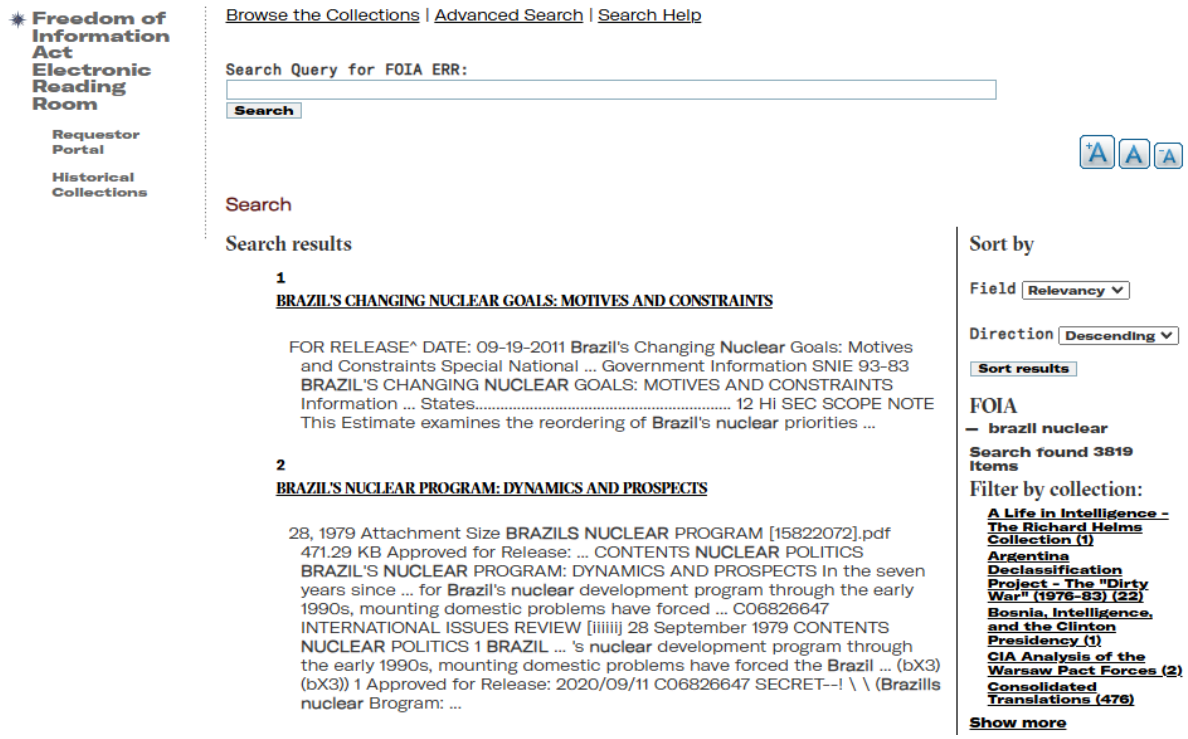

Рис. 6. Пример поискового запрос по FOIA Reading Room ЦРУ США.

[23] Freedom of Information Act Electronic Reading Room. U.S. Government. URL: foia.gov/search.html (дата обращения: 18.12.2024)

4.4. Поиск по юридическим лицам.

Как и в случае с судебными делами, основная информация в части юрлиц хранится на уровне штатов. Она включает данные об учредителе, членах совета директоров и иных аффилированных лицах. Автор книги OSINT Techniques и один из наиболее авторитетных специалистов в этой области Макл Баззелл[24] рекомендует использовать порталы Open Corporates[25], AIHIT[26], Blackbook как наиболее информативные.

4.5. Информация о предвыборных пожертвованиях.

С учётом высокой политизации темы оборонного строительства в США полезно изучить политические «подвязки» крупных компаний. Взносы на нужды предвыборных кампаний в США являются публично доступной информацией. Как правило, для поиска достаточно фамилии кандидата или жертвователя. Ниже приведены три сайта, которые, как представляется, соедржат наиболее подробную информацию в этой связи.

Open Secrets (opensecrets.org)

Money Line (politicalmoneyline.com)

Melissa Data (melissadata.com/v2/lookups/ fee/index)

Отдельного упоминания заслуживает сайте LittleSis, позволяющий выявить связи между крупными организациями и политиками посредством пожертвований, членства в попечительских совета или советах директоров и т.п.

4.6. Поиск по официальным сайтам организаций

Не следует пренебрегать информацией с официальных сайтов изучаемых компаний или государственных структур и, в частности, их годовыми отчётами, которые, как правило содержат систематизированную и актуальную информацию о деятельности за год. При анализе юридических лиц рекомендуется придерживаться следующей структуры, которая позволяет найти «зацепки» для дальнейшего поиска[27].

Организационно-штатная структура. История организации: ключевые даты (для проверки на связь с другими событиями), нынешние и прежние владельцы, переименования, руководство. Ключевые персоналии необходимо изучить на предмет возможных политических связей, прежних мест работы, компрометирующих материалов в СМИ, а также контактов. Схема принятия решений и влияния – составление карты ключевых заинтересованных сторон (по аналогии с проектным управлением)[28].

Основная деятельность. Выпускаемые продукты и потребители, область применения, наличие собственной базы для НИОКР. места производства. Участие в цепочках производственной кооперации. Заключаемые контракты (на основе пресс-релизов, требуют

[24] Базелл. С 401.
[25] opencorporates.com
[26] aihitdata.com
[27] Baker. Там же. С 219-221.
[28] Там же. С 239

анализа на предмет субподряда). Зарубежное присутствие: филиалы, постоянные представительства, имена руководителей зарубежных офисов.

Финансирование. Данные отчётности (в первую очередь инвестиционной), сделки слияния и поглощения. Включена ли компания в санкционные списки иностранных государств?

Государственные базы данных для поиска информации о юридических лицах обширны и разнообразны. Их полное перечисление выходит за рамки настоящего пособия. Для выбора конкретного инструмента можно обратиться к списку баз данных, составленному специалистами консалтингового агентства i-intelligence[29].

[29] Open Sources Intelligence Tools and Resources Handbook. i-intelligence, 2020.

5. Работа с социальными сетями. Особенности поиска информации в Twitter, Facebook, Telegram

В области КВРН социальные сети, очевидно, выступают в роли вторичного, косвенного источника информации. В отличие от человека, по странице в Facebook, Twitter или LinkedIn (запрещен в России), нельзя составить полный профиль, скажем, военно-технической деятельности государства. А вот получить для него несколько «штрихов к портрету» - вполне.

Как и в классической разведке, в исследованиях по открытым источникам человек остаётся главным источником и главной уязвимостью. На фотографии, размещаемые в социальных сетях, могут попасть изображения закрытых объектов или зацепки, позволяющие установить их местонахождение. Внимательное изучение страницы в LinkedIn позволяет понять *оргштатную* структуру разведываемой организации, определить её приоритеты.

При помощи социальных сетей можно выяснить следующую информацию:

Установочные данные пользователя: псевдоним (может быть использован для поиска на других платформах), реальные имя и фамилия, дата рождения, место работы, электронная почта, адрес, родной город, образование, детали внешности (особые приметы, изменения веса и т.д.).

Данные об окружении: часто посещаемые места, упоминания об отношениях, беременности, реабилитации и т.д., отмеченные люди, с которыми объект может общаться, ссылки на людей, которые наиболее активно реагируют на публикации (они могут быть хорошими друзьями и знать, где находится объект), увлечения.

В этой работе не может быть шаблона. Нет и вряд ли возможно представить единый для всех случаев алгоритм работы по социальным сетям. Задача этого пособия в том, чтобы показать минимальный набор инструментов, на основе которых специалист мог бы достраивать свой исследовательский арсенал.

5.1. Facebook

Facebook (запрещен в России как часть экосистемы Meta) – на данный момент самая популярная социальная сеть в мире, количество пользователей – более 2 млрд человек. С 2019 года наиболее полезные инструменты поиска по страницам пользователей этой сети перестали функционировать. Вместе с тем остаётся ряд полезных работающих инструментов.

Начнём со стандартных возможностей. Для поиска конкретного человека можно использовать расширенный поиск с фильтром по городу, дате рождения и месту учёбы. Допустим, нас заинтересовала страница пользователя USERNAME (www.facebook.com/username). За счёт добавления в адресную строку следующих команд мы можем получить дополнительную информацию о его интересах и местонахождении.

Работа	/about?section=work
Образование	/about?section=education
Место жительства	/about?section =living
Контактные данные	/about?section=contact-info
Отношения	/about?section =relationship
События из жизни	/about?section=year-overviews
Друзья	/friends
Подписчики	/following
Фото профиля	/photos
Места	/places_visited
Книги	/books
Понравившееся	/likes
Отзывы	/reviews
Заметки	/notes

Поиск в Facebook посредством адресной строки может быть настроен и на группы пользователей. Для расширения зоны и автоматизации поиска можно использовать кастомизированный механизм поиска, разработанный порталом IntelTechniques: https://inteltechniques.com/tools/Facebook.html.

В отличие от стандартного расширенного поиска в Facebook данный инструмент позволяет:

- находить фото и видео с точной фильтрацией по дате (стандартный поисковик предлагает только опции «на этой неделе», «в этом месяце» и «в этом году»;

- искать фото- и видеоматериалы по месту съёмки;

- выводить публикации в зависимости от даты размещения.

5.2. X (Twitter, запрещён на территории России)

Стандартный расширенный поисковик X включает достаточное количество полей запроса. Вместе с тем, как отмечают специалисты, большая часть результатов в выдаче будет ограничена сроком в 7-10 дней. Те же запросы можно внести в адресную строку вручную, однако с большим охватом.

Следует знать следующие поисковые операторы?

from: - все «твиты» от конкретного пользователя;

to: - «твиты», адресованные заданному пользователю;

filter:replies – включает только «твиты» в ответ другим пользователям;

geocode: *координаты*, lkm – поиск по геолокации (в пределах 1 км от заданных координат). Стоит заметить, что в последнее время пользователи X весьма редко указывают геолокацию в своих публикациях.

min_replies:100 – функция позволяет отфильтровывать наиболее популярные «твиты» по количеству лайков;

since:2021-01-01 until:2024-12-05 – позволяет установить диапазон дат поиска;

Запросы через адресную строку:

https://twitter.com/username/media/ - медиафайлы, размещённые конкретным пользователем;

https://twitter.com/username/lists/memberships – подписки на пользователя;

from:username filter:links – ссылки на медиафайлы на других ресурсах;

Необходимо отметить, что современные поисковые системы позволяют находить даже удаленные «твиты» пользователя. Это можно сделать за счёт поиска по кэшированной версии сайта в Google.

В числе полезных инструментов для работы с X также стоит выделить:

All My Tweets (allmytweets.net) – позволяет вывести все «твиты» пользователя над одну страницу (до 3200 публикаций);

TweetBeaver (tweetbeaver.com) – позволяет получить структурированную информацию о пользователя, его интересах, а также устанавливать связи между несколькими пользователями (за счёт переписок или подписок на одни и те же страницы). Наиболее удобная функция – выгрузка полученных сведений в табличном формате.

Followerwonk (followerwonk.com) – позволяет проводить поиск по биографиям (описаниям профилей) пользователей на предмет установления связей, анализировать список подписчиков и выявлять их примерное местонахождение.

Twitter Biography Changes (spoonbill.io) – позволяет выявлять изменения в биографии пользователя на протяжении времени;

Spark Toro (sparktoro.com/ tools/ fake-followers-audit) – предназначена для выявления фейковых пользователей (ботов);

Twiangulate (twiangulate.com) – может устанавливать близкий круг общения нескольких пользователей за счёт мониторинга подписок и общения.

5.3. Telegram

Telegram в строгом смысле этого слова не является социальной сетью, а относится к категории мессенджеров; имеет свою специфическую систему выдачи и хранения информации. Вместе с тем, с учётом широкого распространения телеграм-каналов, было бы ошибкой игнорировать возможности разведки по этому направлению.

В русскоязычном сегменте интернета в качестве основного инструмента поиска рекомендуют использовать телеграм-боты. В их числе Userbox, Unamer[30], Insight, Глаз Бога и др. Они способны осуществлять поиск по ФИО, никнейму, номеру телефону и электронной почте, а также проверять базы утечек, устанавливать подписки пользователя на группы в телеграм.

[30]Adm1ngmz. Разведка по Telegram ботам — OSINT в телеграм. Habr.com. URL: https://habr.com/en/articles/859360/ (дата обращения 18.12.2024)

В данном пособии их применение детально рассматриваться не будет в связи с законодательными ограничениями. На наш взгляд, использование таких ботов связано с рисками компрометации личной информации, а, соответственно, к их применению следует подходить с большой осторожностью. В частности, не следует оплачивать услуги таких ботов, раскрывая данные банковских карт.

Для этих же целей можно применять надстройки в браузер Google Chrome Telegram Group and Channel Search Tool[31]. Специально для целей поиска в Телеграм были созданы кастомизированные движки Telegago, Comentgram, Osint.me и др.

Для архивации информации из телеграм можно использовать платформу Telethon (Python), которая позволяет выгружать данные и даже вести переписку от имени пользователя[32].

[31] Telegram Group and Channel Search Tool. Google Chrome Store. URL: https://chromewebstore.google.com/detail/telegram-group-and-channe/ilpgiemienkecbgdhdbgdjkafodgfojl
[32] https://docs.telethon.dev/en/stable/

6. Работа с сайтами и их архивными версиями, поиск информации о хостинге и администраторах

Анализ сведений о сайте разведываемой организации (объекта) позволяет добыть массу полезной, а порой, критической информации: начиная от данных владельца и заканчивая внутренними документами компании. Ниже приведены основные автоматизированные инструменты для проведения анализа по этому разделу.

6.1. Составление карты доменов

Карта доменов позволяет установить список доменов и поддоменов, сервисы, что запущены на этих доменах (например, веб-сайты, почтовые серверы, FTP и пр.), их IP-адреса, сертификаты SSL и DNS-записи, владельцы (например, из WHOIS).

Среди наиболее популярных инструментов: DNSdumpster (https://dnsdumpster.com); Amass[33]

Рис. 7. Пример поиска в DNSdumpster: структура поддоменов сайта pircenter.org.

С картой у исследователя уже будет информация, какие домены используются на периметре и какие «светятся» наружу. Подобная инвентаризация позволяет получить дополнительные зацепки для поиска. DNSdumpster «отрисует» карту доменов и укажет все DNS записи, Amass от него отличается тем, что имеет возможность автоматизировать поиск посредством скриптов и сравнивать результаты от разных дат и выявлять произошедшие изменения[34].

[33] https://github.com/owasp-amass/amass?tab=readme-ov-file
[34] Stein_osint. OSINT: Анализ доменов компаний. Habr.com. URL: https://habr.com/en/articles/861560/ (дата обращения: 07.12.2024)

6.2. Анализ истории DNS

История DNS показывает есть ли у целевого сайта незакрытые уязвимости. Например, компания переезжает со старого IP-адреса на новый, когда встает за сервис DDoS-защиты и забывает убрать и заблокировать старый IP-адрес. В таком случае у компании две «входных двери», что создаёт дополнительные уязвимости.

Инструменты для проверки истории DNS: dnshistory[35] и completedns[36]. Чтобы отследить, что было на домене год, два или пять лет назад, можно использовать сервисы wayback machine и stored.website. Как отмечалось в главе по социальным сетям, эти ресурсы в т.ч. позволяют увидеть уже удаленный контент.

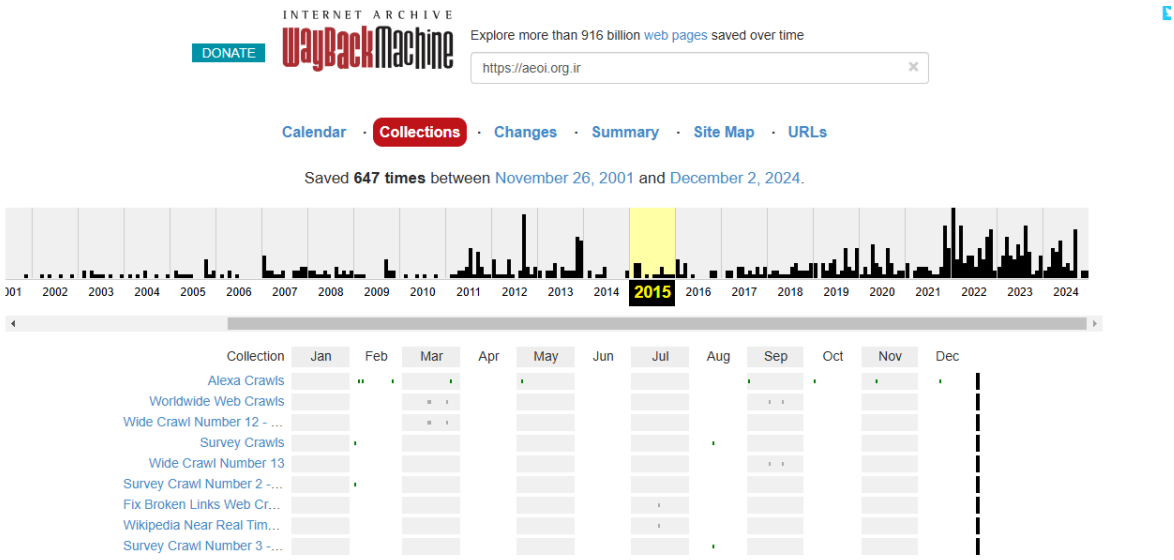

Рис.8 Сохраненные записи сайта Организации по атомной энергии Ирана. Функционал сервиса позволяет отслеживать изменения между версиями, выбирать записи по дате, а также мониторить карту сайта в различных вариантах.

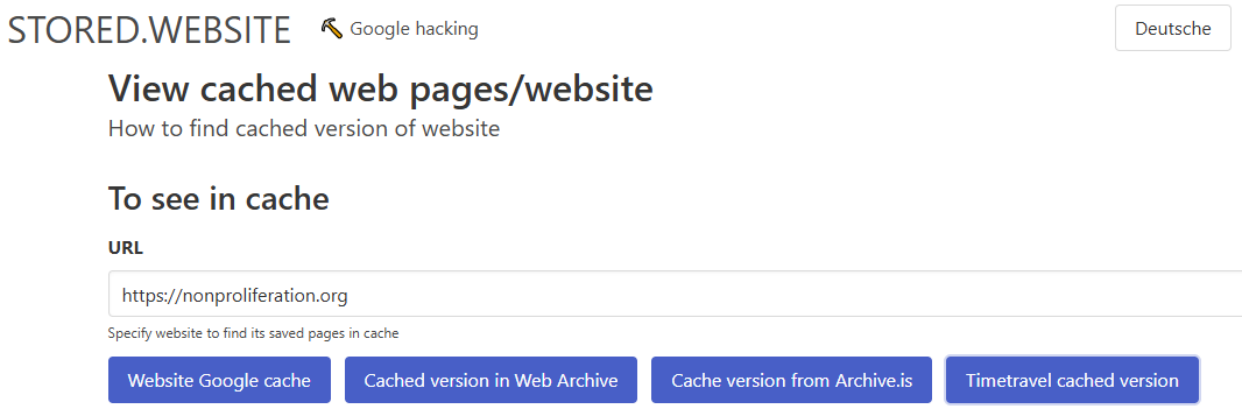

Рис.9. Ресурс Stored.Website позволяет агрегирует архивные версии заданного сайта с четырёх ресурсов: Google Cache, Web Archive, Archive.is, Timetravel

[35] https://dnshistory.org/
[36] https://completedns.com/

6.3. Поиск утёкших корпоративных учётных записей

Не редки случаи, когда сотрудники используют для регистрации корпоративные почты на сторонних ресурсах, а порой – применяют там аналогичные пароли. Для выявления таких пользователей существует сервис WhatsMyName Web. С его помощью удобно искать рабочие e-mail, зарегистрированные на внешних ресурсах.

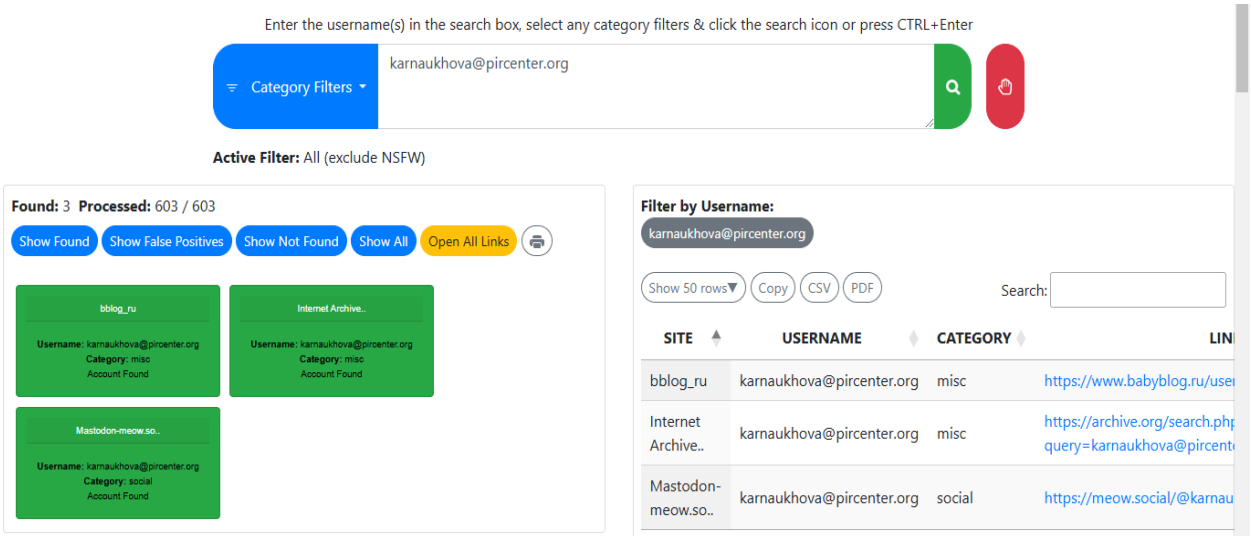

Рис.10. Результаты поиска по одному из электронных адресов в домене pircenter.org

Еще один удобный инструмент — Skymem: он показывает, какие учетные записи зарегистрированы на внешних сервисах. Это особенно важно, когда у компании есть домены только для внутреннего пользования, и аккаунты с этих доменов в принципе не должны использоваться на сторонних ресурсах.

Продвинутый поиск: DorkSearch; Advangle

На этих сервисах с помощью конструктора можно легко создать «прицельный» запрос для поисковых систем и найти: домены и поддомены, email'ы, пользователей, файлы в открытом доступе или на публичных хранилищах.

Альтернативный инструмент — поисковик с расширенными фильтрами Biznar. Он категоризирует выдачу по параметрам (дата, формат и прочее) и помогает фильтровать все, что нашлось. Из «комбайнов» для комбинированного поиска можно посоветовать рассмотреть metabigor — агрегатор данных из разных источников, утилита бесплатная, нужно только установить и запустить ее для поиска информации.

7. Работа с изображениями. Выявление ретуши, работа с метаданными

Любое изображение может сказать больше, чем кажется. Задача аналитика (как в случае и с другими источниками информации) состоит в том, чтобы выжать из фотографии максимум. При рассмотрении следует попытаться ответить на три вопроса (или группы вопросов):

1. Что именно мы видим? В случае, если на фотографии представлены здания, оборудование, системы вооружений – соотносятся ли они с имеющимися сигнатурами? Есть ли отличия? В случае людей – кто именно изображен на снимках?
2. Контекст. Где и когда именно был сделан снимок? Есть ли метаданные? По каким косвенным признакам можно верифицировать место съёмки?
3. Достоверность. Есть ли на фотографии признаки ретуши или видимые искажения? Наблюдаются ли признаки фальсификации (например, генерации нейросетями)?

Исходя из этих задач, предлагается использовать следующие виды инструментов:

7.1. Поиск в интернете по изображению.

Изображения (или их фрагменты) в нём используются вместо поискового запроса. Поиск работает путем загрузки изображения — или его URL—адреса - в систему, которая на основе своих индексов определяет, где еще это изображение появляется в Сети, и отображает все остальные местоположения. Таким образом, можно узнать первоисточник фотографий, мемов и изображений профиля, а также выявить похожие объекты (например, боевую технику конкретного типа).

Ниже приведены наиболее популярные сайты для обратного поиска изображений:

Google (https://www.google.com/imghp): Google имеет специальная поисковая система для обратного поиска изображений; вы можете либо вставить URL-адрес изображения в поле поиска, либо загрузить его в Google.

Reverse-image-search.com: Объединяет выдачу из трёх поисковых систем: Google, Yandex, Bing.

www.imageidentify.com: Использует технологию визуального поиска для распознавания загруженных изображений.

Есть и специализированные сайты, на которых размещаются фотоматериалы основных информационных агентств. В их числе:

• Gettyimages (www.gettyimages.com)

• International Logo List (http://logos.iti.gr/table/)

• Instant Logo Search (http://instantlogosearch.com)

• Reuters Pictures (http://pictures.reuters.com)

• News Press (https://www.news-press.com/media/latest/news)

• Associated Press Images Portal (www.apimages.com)

• PA Images (https://www.paimages.co.uk)

• European Pressphoto Agency (www.epa.eu)

• Canadian Press Images Archive (www.cpimages.com/fotoweb/index.fwx).

В некоторых случаях на фотографиях будет виден текст. Для его анализа следует использовать инструменты оптического распознавания текста, например, FreeOCR[37], Free Online OCR (www.i2ocr.com) или NewOCR (www.newocr.com).

Кроме того, в силу небольшого разрешения или отдалённости изучаемых объектов изображение иногда необходимо увеличить. В таких ситуациях может быть полезна программа Lets Enhance (https://letsenhance.io), позволяющая увеличить фрагменты изображения без потери качества. При этом бесплатный лимит составляет 14 фотографий на пользователя, а использование сетевой инфраструктуры может оказаться неприемлемым с точки обеспечения собственной безопасности.

7.2. Выгрузка метаданных

Анализ изображения начинается с определения исходного устройства (фотоаппарата или мобильного телефона), с помощью которого был сделан снимок. Эта информация является частью метаданных изображения. Метаданные могут содержать множество полезной информации для целей исследования по открытым источникам.

ExifTool (https://sno.phy.queensu.ca/~phil/exiftool): Позволяет читать, записывать и редактировать метаинформацию в самых разных файлах. Он поддерживает различные форматы метаданных, такие как EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP и ID3.

Exif-Search (https://www.exif-search.com): Платный инструмент для поиска изображений с использованием их метаданных.

Geosetter (www.geosetter.de/en): Позволяет просматривать и изменять геоданные изображений.

7.3. Проверка на достоверность

Поиск по мультимедийным файлам в данном случае является одной из областей т.н. «цифровой криминалистики». Не следует доверять всем мультимедийным файлам, которые вы получаете. При наличии сомнений относительно какого-либо мультимедийного файла (изображения или видео), следует тщательно проверить, не был ли он подделан, то есть не был ли подвергнут манипуляциям с целью скрыть или изменить некоторые факты. Для их извлечения и анализа полезными представляются следующие инструменты

[37] www.paperfile.net/index.html

Forensically (https://29a.ch/photo-forensics/#forensic-magnifier): Этот сайт содержит бесплатные инструменты для криминалистического анализа изображений и включает в себя обнаружение клонов, анализ на уровне ошибок (анализ ошибок при сжатии цифровых фотографий), извлечение метаданных и многое другое.

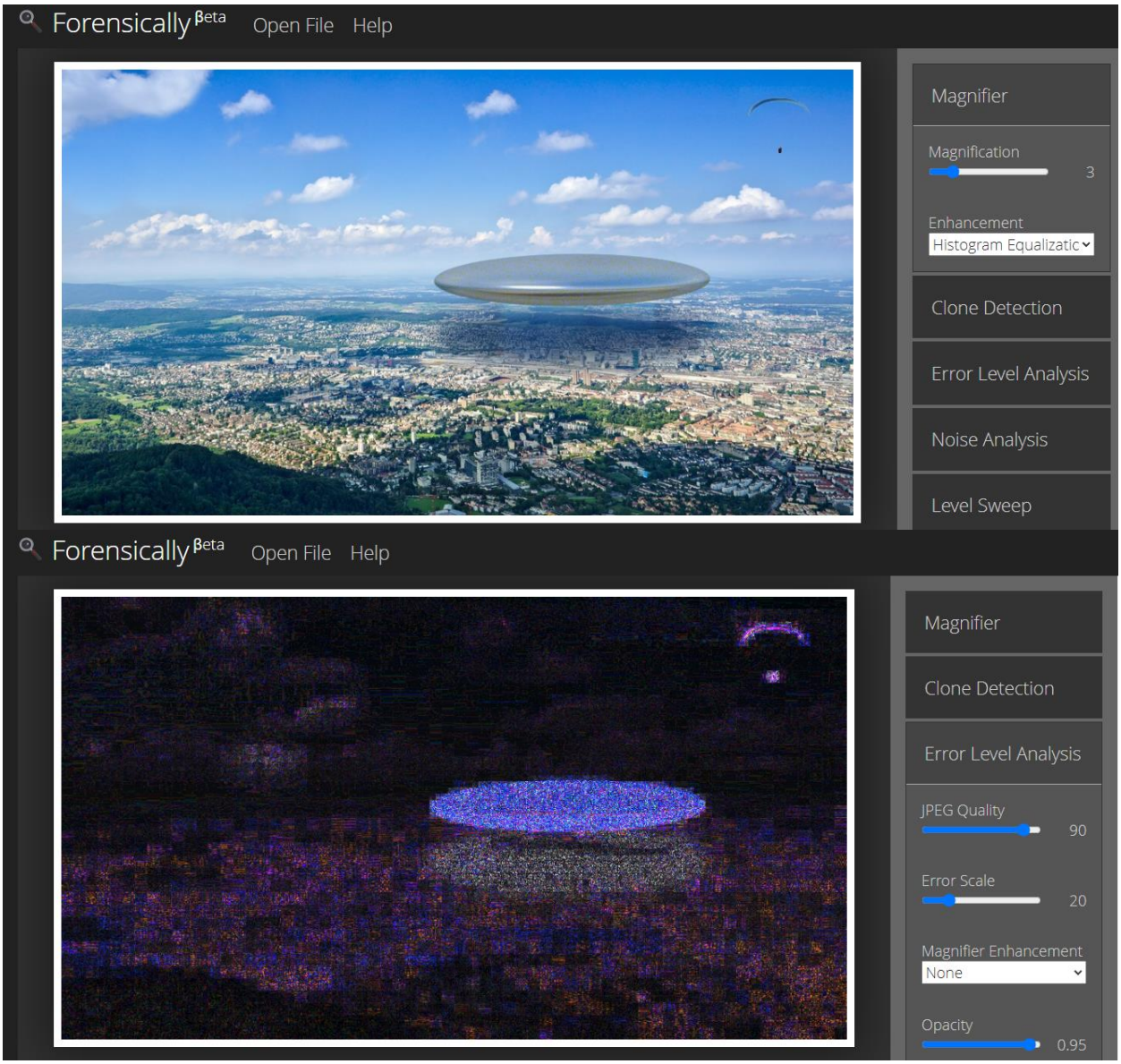

Рис. 11 и 12. *При помощи сервиса Forensically удалось определить, что НЛО и парашютист на фотографии явно лишние.*

Fotoforensics (http://fotoforensics.com): Позволяет проводить криминалистический анализ файлов JPEG и PNG на предмет любых манипуляций с использованием методов анализа на уровне ошибок (ELA).

Ghiro (www.getghiro.org): Это инструмент с открытым исходным кодом, который может массово анализировать изображения и извлекать информацию о метаданных, использовать метаданные GPS для поиска близлежащих изображений и выполнять анализ уровня ошибок для определения того, подвергалось ли изображение манипуляциям.

8. GEOINT. Спутниковые снимки: основные провайдеры и правила работы, сигнатуры объектов по тематике КВРН. Геоинформационные системы: FlightRadar, CruiseShipTracker и др.

Один из важнейших инструментов в арсенале аналитика – спутниковые снимки. Они позволяют сравнительно объективно оценить реальный масштаб событий на конкретном объекте.

При этом использование спутниковых снимков имеет ряд ограничений, о которых следует знать. В частности, в силу низкого разрешения отдельных космических аппаратов изображение может быть искажено, а расстояние – измеряться не вполне корректно.

8.1. Трудности

Наибольшие трудности, впрочем, связаны с актуальностью полученных спутниковых данных. Наиболее интересные результаты можно получить со спутников с высокой «частотой пролёта» (revisit frequency). Это, во-первых, позволяет изучить объект в сравнительной перспективе, а, во-вторых – свести к минимуму фактор погодных условий (например, облачность в рассматриваемом районе). Следует также иметь в виду, что данные могут публиковаться на популярных платформах с задержкой.

Некоторые сервисы (например, Google Earth) намеренно скрывают отдельные объекты и районы по указанию Правительства США. На анализе объектов на территории Китая может сказываться то, что «великий китайский файрволл» искажает работу популярных поисковиков[38].

Стоит также отметить, что многие провайдеры спутниковых услуг ограничивают доступ к своим сервисам с территории Российской Федерации. Приобретению платных снимков высокого разрешения (Maxar, Planet) препятствуют введенные антироссийские санкции.

Ниже приведен краткий перечень доступных ресурсов для работы со спутниковой информацией.

Baidu Maps	Картографический сервис китайского поисковика Baidu. Наиболее детализированные спутниковые снимки и карты КНР. **Недостаток:** сервис на китайском языке, отсутствует детализированное руководство на русском или английском языках.
Earth Explorer	Сервис для запроса и заказа спутниковых снимков, аэрофотоснимков и картографической продукции, разработан Геологической службой США.

[38] Maps & Satellites. Bellingcat Tools. URL: https://bellingcat.gitbook.io/toolkit/categories/maps-and-satellites (дата обращения: 15.12.2024)

	Недостаток: Можно увидеть предварительные просмотры изображений, но часто необходимо заплатить за заказ и загрузку фактического изображения. Некоторые изображения доступны бесплатно.
The European Space Agency (ESA) - Earth Online	Продукт Earth Online от Европейского космического агентства предлагает портал для доступа к спутниковым снимкам и данным об окружающей среде, поддерживая целый ряд приложений — от мониторинга климата до оценки стихийных бедствий. **Недостаток**: Заблокирован для пользователей из России, необходимо использование VPN.
Google Earth Pro	Google Планета Земля — это геопространственный инструмент, который предоставляет подробные глобальные спутниковые снимки, карты, трехмерные модели рельефа, а также возможность интерактивного изучения географических данных. Минус – недостаточный архив снимков, многие локации датированы 2021 годом. По отдельным районам разрешение спутниковых снимков будет недостаточного качества.
NASA Worldview	Разработан НАСА, представляет собой интерактивный онлайн-инструмент с открытым исходным кодом, который позволяет пользователям исследовать земную поверхность, в т.ч. с помощью исторических спутниковых снимков. В основном предназначен для мониторинга атмосферных явлений, погоды и состояния окружающей среды. В числе преимуществ – возможность практически в ежедневном режиме получать изображения в видимом инфракрасном спектре и данные радиоспектрометрии земной поверхности в умеренном разрешении. При использовании этой платформы следует иметь в виду следующие ограничения **Доступность данных**: Не все спутниковые данные доступны в режиме реального времени, большинство наборов данных обновляется реже. Некоторые регионы или типы данных могут быть недоступны с требуемым разрешением для детального анализа. **Низкое разрешение.** Наибольшее оптическое разрешение составляет 10 метров на пиксель для RGB и ближнего инфракрасного диапазонов, 20 метров на пиксель для коротковолнового инфракрасного диапазона. Для сравнения – коммерческие спутники компании Maxar позволяют получать изображения с разрешением порядка 50 см на пиксель, разведывательные спутники США – порядка 27 см на пиксель.

	Сложность в освоении и ограниченные возможности для анализа. Несмотря на то, что Worldview поддерживает визуализацию, он не предлагает обширных встроенных инструментов для анализа данных. Пользователям может потребоваться использовать другое программное обеспечение для детального анализа.
Copernicus Browser and EO Browser (formerly Sentinel Hub Playground)	Удобная платформа для визуализации данных со спутников Sentinel Европейского космического агентства, обновляемая каждые 5-10 дней. Интерфейс включает в себя ряд функций, в том числе встроенные индексы и инструмент временной привязки. Может быть недоступна из России, требуется использовать VPN.
Tencent Maps	Картографическое приложение и технология китайской компании Tencent. Включает спутниковые снимки, карты улиц, обзор улиц (покрытие) и исторические перспективы. **Недостатки**: При работе с IP-адресов за пределами КНР скорость работы будет замедляться из-за брандмауэров, установленных в китайском сегменте интернета. Уровень охвата и детализации картографических данных ограничен и включает карты только материкового Китая, Гонконга, Макао и Тайваня. В некоторых сельских или менее развитых районах данные могут быть скудными или устаревшими.

8.2. Методология анализа спутниковых снимков

Первый шаг при анализе спутниковых снимков – понять, что именно вы ищете. В большинстве случаев разведка будет вестись по заданному объекту или району поиска. В отдельных ситуациях координаты искомого объекта потребуется установить на основе фотографий «с земли» или иных вводных.

***Рис. 13, 14**. На основе фотографии новейшего американского тяжёлого бомбардировщика B-21 Raider российские аналитики смогли установить точное местонахождение производства и испытательной инфраструктуры самолёта. Источник: Stein_osint. OSINT: Нахождение секретной техники ВВС США по фото. Habr.com. URL: https://habr.com/en/articles/837804/ (дата обращения: 18.12.2024)*

Наиболее интересные результаты, как правило, даёт сравнительный анализ снимков одного и того же объекта, снятых в различное время, на предмет изменений. Обратите внимание на изменения в местности, расчистку земли, здания или дороги. Иногда изменения на местности очевидны. В других случаях на спутниковых снимках невозможно четко определить, действительно ли это уже построенное здание или строительство еще продолжается. В этом случае поможет внимательное наблюдение за тенями. Если строится высокое здание или высокий объект, то на снимке появляется тень, которую можно использовать для определения степени развития и даже времени и расстояния.

Частой ошибкой новичков является неправильная интерпретация объектов и элементов на снимках. Чтобы успешно расшифровать спутниковые снимки, необходимо детально изучить многочисленные компоненты, узоры и элементы на изображении. В годы холодной войны ЦРУ США использовало следующую последовательность шагов для анализа снимков промышленных объектов. Как представляется, эти рекомендации сохраняют актуальность и сегодня.

1) Определите местоположение объекта, масштаб и дату съёмки;

2) Определите площадь объекта;

3) Внимательно осмотрите здания и смежные конструкции;

4) Обратите внимание на трубы, дым и пар;

5) Проанализируйте коммуникации и перемещения на объекте;

6) Определите места хранения: склады, запасы, резервуары;

7) Изучите состояние инженерных сетей: ЛЭП, водопровод и другие инженерные коммуникации;

8) Обратите внимание особые признаки (сигнатуры), указывающие на предназначение объекта;

9) Проверьте, нет ли на фотоснимке признаков строительных или демонтажных работ, других признаков эксплуатации;

10) Обратите внимание на меры безопасности и системы физической защиты объекта;

11) Найдите источник рабочей силы;

12) Изучите окрестности на предмет неожиданных факторов[39].

Расшифровка конкретного содержания каждого из этапов приведена в Приложении 1.

Еще один признак развития - изменения в ландшафте или растительности. Если помнить об этих элементах при просмотре спутниковых снимков, это поможет вам увидеть изменения в городской местности, которые могут свидетельствовать о расширении поселения.

[39] Basic Course in the use of Aerial Photography for Intelligence Purporses. Central Intelligence Agency. URL: https://www.cia.gov/readingroom/docs/CIA-RDP80-01333A000300170001-8.pdf (дата обращения: 18.12.2024)

8.3. Инструменты для отслеживания транспорта

Существует ряд онлайн-инструментов, позволяющих отслеживать перемещение авиационного и морского транспорта. При проведении исследований в военно-политической области это может быть востребовано для выявления неафишируемых контактов и визитов делегаций, определения поставок. При этом необходимо понимать, что они работают за счёт информации, собранной волонтёрами по всему миру. Соответственно, содержащуюся в них информацию нельзя воспринимать как достоверную в силу возможных технических искажений и возможных злонамеренных фальсификаций.[40]

8.3.1. Воздушный транспорт

Существует несколько веб-сайтов, которые позволяют отслеживать рейсы, как в режиме реального времени, так и в исторической перспективе. Как и в случае с любым другим инструментом с открытым исходным кодом, рекомендуется проверить несколько веб-сайтов, поскольку на одном может быть больше информации, чем на других.

Flight Radar 24[41] – один из самых известных веб-сайтов для отслеживания полетов. Интерфейс сайта понятен и прост в использовании. Как и на других страницах этого руководства, на Flight Radar 24 есть возможность просматривать исторические записи о полетах. Другими словами, если вы хотите выполнить поиск по регистрации воздушного судна, вы сможете найти на веб-сайте записи о рейсах, совершенных этим воздушным судном в прошлом. На странице также возможно просматривать заданный участок воздушного пространства таким, каким он был в конкретный момент в прошлом. Этот инструмент полезен в тех случаях, когда необходимо отслеживать активность в конкретном аэропорту без данных о воздушном судне.

Рис. 15. Отображение самолётов в сервисе FlightRadar24

[40] Подробнее о принципах работы таких систем: DmitrySpb79. Flightradar24 — как это работает? Habr.com URL: https://habr.com/ru/articles/408003/ (дата обращения: 19.12.2024)
[41] www.flightradar24.com

Radarbox24 На первый взгляд, сервис похож на Flight Radar 24. Одно из небольших отличий в качестве обслуживания заключается в том, что интерфейс Radar Box по умолчанию показывает больше информации при наведении курсора на самолет, чем Flight Radar 24. Эта информация включает логотип авиакомпании, города вылета и прибытия, тип воздушного судна и регистрационный номер.

Наведя курсор на воздушное судно в интерфейсе Radar Box по умолчанию, можно увидеть важную информацию о рейсе, включая тип воздушного судна и города назначения/прибытия.

Flight Aware – сервис для всех коммерческих рейсов, включая удобную информацию о погоде в пунктах назначения по всему миру и карту задержек в аэропортах, доступную на домашней странице. На веб-сайте также есть RSS-лента отраслевых новостей, доска объявлений и даже раздел с фотографиями самолетов. Flight Aware также позволяет получать уведомления всякий раз, когда отслеживаемый самолет подает заявку на полет, вылетает из аэропорта или прибывает в пункт назначения, а также в случаях, если рейс задерживается, отменяется или перенаправляется. Эти оповещения о рейсах позволяют осуществлять пассивный мониторинг рейсов.

Рис. 16. Интерфейс сайта FlightAware.

ADS-B Exchange – это любительский бесплатный проект. ADS-B Exchange подходит для слежения за военными самолетами (хотя, заметьте, не за каждым из них), что делает его особенно полезным инструментом для оперативного мониторинга горячих геополитических точек и последних новостных событий. Оперативная карта веб-сайта (находится на вкладке “Глобальный радарный обзор” на главной странице) содержит удобную функцию фильтрации, которая позволяет отображать только военные самолеты:

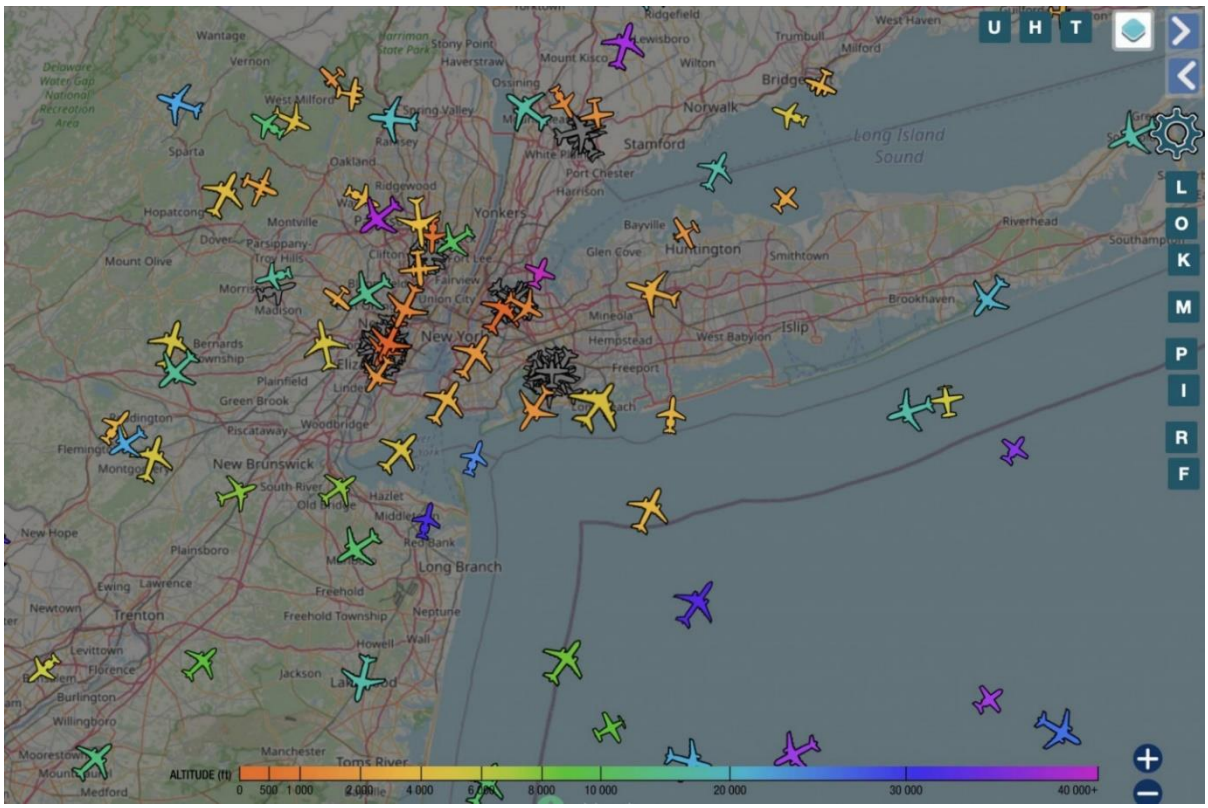

Рис. 17. Интерфейс ADS-B Exchange

8.3.2. Инструменты по отслеживанию морского транспорта

Отслеживание морского транспорта происходит посредством AIS-трекеров - сервисов, которые предоставляют информацию о местоположении и движении морских судов в режиме реального времени. Среди онлайн-сервисов в этой области можно выделить следующие[42]:

1. **Marine Traffic** — аналог Flightradar24 для судов. В режиме реального времени показывает местоположение яхт, рыболовных траулеров, танкеров, контейнеровозов и так далее. Предоставляет массу справочной информации.(зачастую за точное местоположение просят оформить подписку, но есть компании, которые предоставляют это бесплатно, например: Veson Nautical, необходимо лишь написать на почту press@veson.com)

[42]MagisterLudi. OSINT самолетов, пароходов и поездов. Habr.com. URL: https://habr.com/ru/companies/timeweb/articles/665724/ (дата обращения: 16.12.2024)

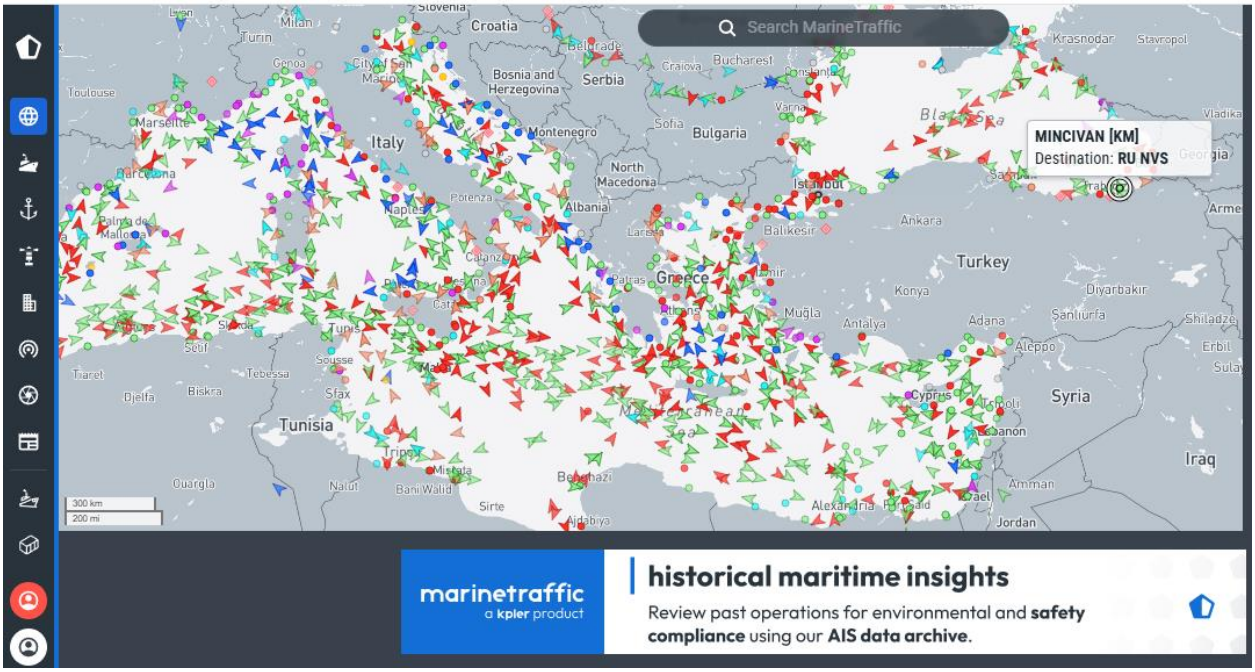

Рис. 18. Интерфейс сервиса Marine Traffic.

2. **VesselFinder** — альтернативный портал для отслеживания маршрутов судов и агрегации данных. Использует большую сеть наземных AIS-приемников и данные спутникового мониторинга.

3. **Marine Vessel Traffic** — сервис использует карты из предыдущих пунктов этого списка, но дополняет их рядом полезных фильтров и возможностью удобного отслеживания отдельных классов судов.[43]

[43] OSINT: подборка инструментов по отслеживанию морского транспорта. STEIN: URL: https://t.me/secur_researcher/512 (дата обращения: 16.12.2024)

9. Анализ. ПО в помощь исследователю

Собранная информация должна быть обработана, систематизирована и должным образом проанализирована. На этом этапе следует решить несколько последовательных задач:

1. Определить, какая именно информация была получена на этапе сбора, соотнести её с поставленным исследовательским вопросом. Полезный совет на данном этапе: отсутствие информации – это тоже информация. В открытых источниках нет и не может быть всех необходимых сведений, особенно в столь чувствительной сфере, как КВРН. Вместе с тем, выявленные пробелы и зазоры могут свидетельствовать о предпринимаемых мерах по засекречиванию, что само по себе ценно и задаёт направление дальнейших поисков[44].
2. Проверить собранные сведения на достоверность и внутреннюю непротиворечивость, определить надёжность каждого из источников.
3. Сделать на основе полученной информации предположения, выявить возможные логические ошибки и неточности;
4. Определить возможные альтернативные точки зрения (гипотезы) относительно причин происходящего и направления дальнейшего развития событий.

Главная ошибка начинающего исследователя – отсутствие правильной систематизации на этапе сбора информации. Из-за этого при анализе зачастую приходится проделывать одну и ту же работу дважды (а то и трижды). Как уже отмечалось во введении, все источники должны быть тщательно задокументированы с указанием ссылок и приложением (там, где это применимо) скриншотов и иной подкрепляющей документации.

Базовый способ – сохранять всё в сводный файл Word. Его недостаток – излишняя громоздкость. Файл Excel в этом отношении будет более удачным выбором, поскольку позволяет сохранять единообразную текстовую информацию в таблице, параллельно указывая источники и степень их надёжности. Вместе с тем, при таком варианте каталогизации сложно сохранять изображения и прочую нетекстовую информацию.

Оптимальным представляется следующий путь.

1. Вся подкрепляющая документацию сохраняется в отдельную (желательно изолированную, см. главу о собственной безопасности) папку. Все текстовые файлы индексируются при помощи программы dtSearch или аналога для последующего полнотекстового поиска.

2. Для текстовой информации (книг, научных статей, публикаций в СМИ) используется библиографический менеджер, на основе которого в итоговом документе будет оформляться справочно-ссылочный аппарат. Наилучшие варианты – Mendeley (есть бесплатная версия, предполагает возможность совместной работы), а также Citavi. При этом в примечаниях к каждой предполагаемом цитате в карточке библиографического менеджера должна быть сделана хотя бы предварительная пометка о надёжности источника.

3. Полученные «зацепки» и узлы связей между различными видами информации визуализируются при помощи специального ПО. По опыту зарубежных OSINT-исследователей, наиболее для этих целей подходят программы Maltego, а также Neo4j

[44] Baker. Там же. С 36

Community Edition и Gephi[45]. Кроме того, помимо выстраивания графов с взаимосвязями между объектами, весьма полезным может оказаться систематизация времени анализируемых событий в форме графика. Для этих целей можно использовать следующее свободное ПО: Draw.io[46], Visual Investigative Scenarios[47], MindMup[48] и NWU[4950].

4. Внимательно изучить используемые источники на предмет дезинформации или непреднамеренного искажения. Как представляется, эта тема заслуживает подробного рассмотрения.

   Так, если речь идёт об авторской публикации или предполагаемом «инсайде», следует задаться вопросом, откуда у источника доступ к такой информации. В этом случае следует сопоставить имеющиеся сведения с известной оргштатной структурой разведываемого объекта/организации.

   В случае работы по материалам СМИ, открытой печати и экспертным публикациям каждому источнику должна быть дана характеристика. Можем ли мы определить первоисточник? Насколько авторитетным является источник? Объективен ли он, есть у него материальная или иная заинтересованность в размещении соответствующей информации? Не содержит ли публикация искажений по сравнению с первоисточником, подтверждают ли другие источники представленную информацию? (идеальный вариант – подтверждение по трём *независимым* источникам). Насколько полно изложена информация?[51]

   Для проверки информации на достоверность можно использовать алгоритм из восьми вопросов:
   1. Кто автор материала?
   2. Что именно вы нашли? Это исчерпывающее объяснение, доказанная концепция, небольшой комментарий или лишь гипотетическое изложение?
   3. Где найден результат. Что это за ресурс?
   4. Ссылается ли на него кто-нибудь?
   5. С чьей помощью информация увидела свет? Кто владелец сервера, где расположен хостинг? Есть ли какие-нибудь ссылки?
   6. Для чего этот материал создали и выложили в сеть?
   7. Как создавался материал. На него потратили годы исследований, или это вброс, состряпанный за полдня?
   8. Когда эту информацию создали, опубликовали, обновляли, когда был создан разместивший её ресурс?[52]

[45] Baker. Ibidem. P. 191
[46] www.diagrams.net/integrations.html
[47] vis.occrp.org/account/metro
[48] mindmup.com
[49] knightlab.northwestern.edu/projects
[50] OSINT Techniques, 2023, p. 519
[51] OSINT Strategies. P. 107
[52] Фравиа. С. 42.

Кроме того, проведение OSINT-исследований сопряжено с двумя потенциальными ошибками. Первая – эффект «эхо», когда информация из одного источника стремительно распространяется. В таком случае есть соблазн считать её достоверной в силу многочисленности публикаций. Следует помнить, что стремление подтвердить уже сформированное мнение – одно из ментальных искажений, свойственных человеческой психике[53].

Вторая ошибка – тенденция к быстрому распространению недостоверной информации, что также «замыливает» информационное пространство. Для выявления такой информации можно использовать следующие инструменты[54] (с оговоркой о том, что многие из них разработаны под политический заказ противодействия российским стратегическим коммуникациям и объективностью не отличаются): Hoaxy, Verification Junkie.

[53]Heuer. Psychology of Intelligence analysis. P. 127
[54] Nihad p. 169-171

10. Принципы написания аналитического текста: советы начинающим исследователям

1. Текст должен быть написан короткими рублеными фразами, без «мусорных» слов, не несущих добавленной стоимости. Вместо оценочных прилагательных «уникальный», «справедливый», «замечательный» и т.п. следует использовать конкретные примеры, иллюстрирующие вашу мысль.

Не пишите ничего «вообще». Старайтесь, чтобы ваши материалы всегда были в точку. Не нужно общих рассуждений там, где можно дать конкретику. Не «будет иметь самые серьёзные последствия для международной обстановки», а «ставит под угрозу принятие Заключительного документа ОК ДНЯО 2026 года». Старайтесь, чтобы у всего того, что вы делаете, была добавленная стоимость. В идеале, чтобы, если Ваш текст прочитают, его захотелось бы скопировать и вставить, как есть, в курсовую или в докладную записку на имя Президента.

Воплощение такого подхода – информационный стиль, разработанный Максимом Ильяховым, чья книга «Пиши, сокращай» рекомендуется к внимательному прочтению[55].

2. Пожалуйста, следите за логикой и структурированностью текста. Старайтесь придерживаться правила «один абзац – одна мысль». Более того, следите, чтобы содержание текста соответствовало заявленной теме и введению. Кажется очевидным, но со многими авторами случается так, что они заявляют одну тему, а потом полёт мысли уносит их в иные степи.

3. Обязательно делайте нумерацию страниц в документе, если он занимает более одной страницы.

4. Старайтесь избегать длинных предложений. Иногда приходится сталкиваться с тем, что автору не дают покоя лавры Льва Толстого и он начинает писать абзацы одним предложением. Это имеет право на существование в классической литературе, но те, кто читает аналитические материалы, не всегда захотят разбираться в хитросплетениях Вашей мысли – особенно, если она долгая и непонятная.

5. Русский язык велик и могуч, как мы помним ещё со школьной скамьи. Пожалуйста, не злоупотребляйте калькой с английского (или любого другого иностранного языка). Слова вроде «актор» не вызывают ничего кроме раздражения. И, поверьте, своими текстами Вы хотите вызвать совсем другие эмоции.

6. Помните про тему-рему. В русском языке смысловой центр предложений – в конце.

7. Вычитывайте ваши труды в обязательном порядке. Если пишете статью, которая может полежать ещё час или день, дайте ей отлежаться, чтобы потом вычитать всё «свежим взглядом». Иногда будете удивляться, сколько всего вы пропустили.

[55] М.Ильяхов, Л.Сарычева Пиши, сокращай 2025: Как создавать сильный текст. М.: Альпина Паблишерз, 2024, 398 с.

11. Контр-OSINT и личная безопасность

Поскольку данное пособие предназначено для начального ознакомления с тематикой разведки по открытым источникам, здесь будут приведены основные правила обеспечения собственной информационной безопасности исследователя. Работа по объектам, где подразумевается активное противодействие со стороны вероятного противника, требует дополнительных мер безопасности. В конце главы будут приведены ссылки на материалы для самостоятельного изучения.

Пункт первый – определите текущее состояние личной информационной безопасности. Используя инструменты, описанные в предыдущих главах, найдите информацию о себе и попытайтесь выявить каналы утечки. В частности, следует проверить используемые вами аккаунты в социальных сетях и основных почтовых клиентах на предмет наличия в базах утечек на портале Have I Been Pwned[56] или на мониторинговом портале Firefox[57].

Пункт второй – установите надёжные пароли на основных сервисах. Главный принцип - никогда не используйте одинаковые или похожие пароли. По двум причинам:

- Имея вашу почту и пароль от сайта А, злоумышленник обязательно попробует зайти с ними на сайт Б;
- Если данные о ваших аккаунтах вместе с паролями всплыли в утечках, то получится сопоставить между собой даже совершенно разные почты и номера телефонов.

При этом необязательно держать в голове сразу все пароли. Вполне надёжный способ – обзавестись менеджером паролей и запомнить основной мастер-пароль к нему. При этом пароль должен соответствовать базовым критериям стойкости: не менее 8 символов, среди них – цифры и знаки. Хороший принцип построения – три случайных слова, часть символов в которых заменяется цифрами.

Для обеспечения дополнительной защищенности структурно пароль можно делить на две части – уникальная часть для сервиса, которая вносится в менеджер паролей, и единая добавка-приписка, которая держится в уме (пример: в менеджер паролей заносится первая часть пароля – «MG1M0o$inT», в уме держится приписка – «Cheburashka»). Таким образом, итоговый пароль – «MG1M0o$inTCheburashka».

Кроме того, на ключевые ресурсы необходимо установить двухфакторную аутентификацию. Важно: привязывать телефон к аккаунту - не всегда хорошая идея. Не используйте подтверждение через номер телефона там, где это необязательно, особенно на ненадёжных ресурсах: иначе в случае утечки в сеть могут попасть данные о номере, который используется для авторизации.

Используйте дополнительный фактор для входа в сайт, когда вы осознаете, что аккаунт на конкретном сайте для вас важен (переписки, покупки, финансы), и что вы сознательно будете подтверждать вход каждый раз.

[56] https://haveibeenpwned.com/
[57] https://monitor.firefox.com/

Пункт третий – следует минимизировать возможные утечки из слабозащищенных сервисов. При размещении фотографий или файлов в социальных сетях или отправке широкому кругу получателей следует зачищать метаданные, которые содержат информацию о месте съёмки и домашнем компьютере (например, при помощи сервисов Adarsus или PDF24).

Полезный совет – указывать минимально необходимое количество информации при оформлении, скажем, доставки. Самый предпочтительный вариант - указать лишь номер дома и встретить курьера снаружи. Всё остальное (этаж/квартира/домофон) пишите в поле дополнительной информации — курьер его легко прочтёт, а вот в базу данных с вашим адресом такая неструктурированная информация попадёт с меньшей вероятностью.

Пункт четвёртый – обеспечить постоянное резервное копирование информации на внешний носитель (предварительно проверив его при помощи антивирусной утилиты).

Резервные файлы в облачных хранилищах следует периодически «подчищать». Проверьте файлы в своих облачных хранилищах, удалите все ненужное. Проверьте доступ к давно забытым документам для совместного редактирования в облаке. Возможно, среди них есть конфиденциальные.

Пункт пятый – по возможности, обеспечить разделение рабочего и личного информационного пространства. В частности, для проведения исследований желательно создать отдельный почтовый ящик. Помимо этого, должен существовать изолированный «мусорный» электронный адрес, на который будут направлять рекламные материалы и т.п.

- Спам-ящик: почтовые рассылки и интернет-магазины, случайные регистрации.
- Личный ящик: текущая переписка, регистрация в сервисах, уведомления от которых важны.
- Облачный ящик: привязки сервисов типа iCloud, Google Drive, мессенджеры.
- Секретный ящик: для финансовых документов и любой иной чувствительной информации рекомендуем использовать почтовый сервис с End-to-end шифрованием.

В случае, если регистрация на сайте осуществляется в единоразовом порядке, целесообразно использовать одноразовые временные электронные адреса. Существует большое количество сервисов, предоставляющих одноразовые почтовые ящики на 10-15 минут. Они хороши для одноразовых регистраций на сайтах, куда вы попадаете в первый раз и больше, скорее всего, не воспользуетесь. Среди наиболее правдоподобных TemporaryMail[58] и MinuteInbox[59].

При этом даже «мусорный» почтовый ящик периодически необходимо зачищать. В этой связи полезными представляются следующие сервисы:

- JustDeleteMe[60] - прекрасный каталог по платформам, даёт ссылки и описание нужных действий, показывает сложность удаления. Также у создателей есть

[58] https://temporarymail.com/
[59] https://www.minuteinbox.com/
[60]https://justdeleteme.xyz/

родственные сайты JustGetMyData[61] и JustWhatsTheData[62] для выполнения вышеперечисленных действий.

Наличие электронной почты само по себе раскрывает о вас некоторую информацию. Прежде всего, это **алиас**, имя ящика, слева от символа собаки "@". Первый и очевиднейший совет -- не стоит выбирать именем ваши инициалы, фамилию и год рождения, если это не сугубо личный или рабочий ящик.

- После алиаса и перед знаком @ вы можете указывать дополнительный суффикс с "+", например nickname+facebook@google.com. Письма на такой электронный ящик будут приходить к владельцу nickname@google.com, но с точки зрения сайтов это будет совершенно другой ящик. У Google, к тому же, существует особенность: любые точки в алиасе рассматриваются как опциональные и работают как суффиксы после "+".
- Существует несколько схем использования: уникальный ящик для каждого сервиса, уникальный ящик для каждой "личности" либо использование только для некоторых сервисов по известной только вам схеме. Строго рекомендуется использовать эту возможность во всех сайтах, где она поддерживается. Таким образом Вы в случае утечек или рассылки спама будете точно знать, откуда была получена почта, а в случае целенаправленного сбора информации по вашему электронному адресу информация с нескольких сайтов с меньшей вероятностью будет объединена в одно досье.

Пункт шестой – к**онфиденциальность в Telegram** (и других мессенджерах).

Telegram даёт возможность гибко управлять белыми и чёрными списками по доступу к вашим данным. Для пунктов в этом подразделе можно скрыть информацию от всех или показать всем либо использовать список ваших контактов. Также возможно добавлять точечно исключения в виде отдельных аккаунтов или всех людей, состоящих в определённых группах.

Контактами в данный момент в Telegram считаются не только те аккаунты, для которых вам известен телефон (так было ранее), но и аккаунты, вручную добавленные в контакты приложения. Поэтому полагаться на список контактов в настройках сильно не следует -- как минимум, в вашей телефонной книге уже могут быть посторонние номера, а контакты внутри приложения легко добавить по ошибке. Поэтому рекомендуется сделать ревизию телефонной книги либо вообще не расшаривать к ней доступ.

Номер телефона

Ставим опцию "Кто видит мой номер телефона" в значение "Никто", иначе любой аккаунт в Telegram в любом чате сможет видеть ваш номер телефона.

Также видим, что есть опция "Кто может найти меня по номеру". Это одна из наиболее ценных настроек приватности Telegram. К сожалению, до сих пор эта опция не имеет значения "Никто". Ставим эту опцию в "Мои контакты", и теперь только аккаунты из ваших контактов смогут добавить вас по номеру телефона. Помним при этом ограниченное доверие к группе контактов (см. выше).

[61] https://justgetmydata.com/
[62] https://justwhatsthedata.github.io/

Последняя активность

В платформе есть особенность -- ограничения на время последней активности (был N минут назад в сети) действует в две стороны. Ставим в значение "Никто", но помним, что при этом и вы не сможете видеть активность других аккаунтов. К счастью, конкретных людей при необходимости можно добавить в исключения и удалить после проверки.

Группы и каналы

Разрешение на добавление вас в группы и каналы имеет ограничение -- нельзя запретить всем, но можно разрешить только своим контактам. Также для опции действуют отдельные точечные запреты.

Ставим опцию в значение "Мои контакты". Помним при этом ограниченное доверие к группе контактов (см. выше).

Звонки

Антиспам в Telegram работает хорошо, поэтому звонки от спамеров довольно редки. Также, к счастью, сам звонок не раскрывает о вас никакой информации, если не включён режим Peer-to-peer. В этом режиме Telegram устанавливает прямое соединение от вашего устройства к устройству собеседника, и становится возможным определить IP-адрес.

Ставим "Кто может мне звонить" в значение "Мои контакты", если вы готовы добавлять вручную аккаунты в контакты и следить за их "чистотой". Ставим опцию "Peer To Peer" в значение "Никто".

Фотография профиля

При включённой опции другие аккаунты теряют возможность видеть ваш аватар. Эта довольно полезная опция тоже ограничена уровнем доступа контактов, но также может быть включена вручную для конкретных аккаунтов.

Ставим опцию в значение "Мои контакты". Помним при этом ограниченное доверие к группе контактов (см. выше).

Пересылка сообщений

С определённой версии Telegram научился для пересланных (forward) сообщений убирать ссылку на автора. Таким образом, даже если ваше сообщение скопируют в другой чат, через него невозможно будет выйти на ваш профиль. Ранее это позволяло отслеживать аккаунты, которые оставили хотя бы одно сообщение в любом чате.

Ставим опцию "Кто может ссылаться на мой аккаунт при пересылке сообщений" в значение "Никто".

Пункт седьмой – использование VPN-сервисов. Начнем с простого: если ваш Wi-Fi-роутер близок к винтажному, самое время его сменить. Незащищенный роутер и беспроводная сеть могут стать точкой входа для соседа, который практикует свои знания в области компьютерной безопасности, или для настоящего злоумышленника.

Все критичные операции выполняйте только через подключение к VPN - проверка личного почтового ящика, работа с конфиденциальной информацией, доступ к интернет-банку и тд. Наши рекомендации: NordVPN, ExpressVPN, Surfshark.

Помните: меры безопасности должны соответствовать реальной ценности данных. Помните, что использование средств криптографической защиты может вызвать повышенный интерес к вам со стороны органов безопасности.

Дополнительные материалы и литература:

- Искусство обмана. К.Д Митник.
- Искусство вторжения. К.Д. Митник.
- Социальная инженерия и социальные хакеры. М. Кузнецов, И. Симдянов.
- Киберпреступник №1, Ник Билтон.
- Расследования компьютерных преступлений, Кевин Мандиа.
- Extreme Privacy Guide, Michael Bazzel.
- Countdown to zero day, Kim Zetter.
- Противодействие OSINT для взрослых. URL: https://github.com/shadawck/awesome-anti-forensic.
- Памятка с инструментами по обеспечению приватности. URL: https://github.com/Lissy93/awesome-privacy/.
- Чек-лист по личной безопасности. URL: https://digital-defense.io/.

12. Нормативно-правовое регулирование OSINT

Важный аспект личной безопасности при проведении OSINT-исследований – неукоснительное соблюдение требований законодательства Российской Федерации. В первую очередь речь идёт о нормативно-правовых актах в сфере защиты персональных данных и сведений, составляющих государственную тайну, защите национальных интересов от внешнего влияния, противодействия дискредитации Вооруженных сил Российской Федерации.

При работе с открытыми данными рекомендуем придерживаться следующих простых правил.

Базовый принцип – работаем только по зарубежным целям, для объектов на территории Российской Федерации используем официальные данные. Каждое утверждение применительно к российским объектам или возможным действиям Российской Федерации должно быть подкреплено ссылкой на достоверный источник.

При этом даже применительно к информации, формально не подпадающей под перечень сведений, составляющих государственную тайну Российской Федерации (подлежащих засекречиванию), органом безопасности может быть установлен особый статус. В соответствии с приказом ФСБ России от 4 ноября 2022 г. № 547[63], определен перечень сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации.

К таким сведениях, среди прочего, отнесены данные о стратегическом планировании, соблюдении международных договоров, различных аспектах деятельности Госкорпорации «Роскосмос». Систематический сбор подобной информации с её последующим размещением в интернете может быть, при должной находчивости, расценен как работа в интересах иностранного государства со всеми вытекающими последствиями.

Правило второе – при ссылке на зарубежных или оппозиционных российских экспертов необходимо обязательно проверять, не включены ли они в реестр иностранных агентов, нежелательных или запрещенных организаций. В соответствии с действующим законодательством, материалы запрещенных (например, террористических структур: Хайят Тахрир-аш-Шам, ИГИЛ) или нежелательных (например, Центр стратегических и международных исследований (США), Германский фонд Маршалла и др, Чэтэм Хаус[64]) запрещены к распространению на территорию Российской Федерации. Публикации иностранных агентов (как юридических, так и физических лиц) должны сопровождаться указанием на «иноагентский статус»[65].

[63] Приказ ФСБ России от 4 ноября 2022 г. № 547 “Об утверждении Перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации”

[64] Данные организация признаны нежелательными на территории Российской Федерации и приводятся в информационных целях

[65] Федеральный закон "О контроле за деятельностью лиц, находящихся под иностранным влиянием" от 14.07.2022 N 255-ФЗ

Правило третье – персональные данные россиян, полученные при проведении OSINT-исследований, в открытом доступе размещать не следует.

В 2024 году в Российской Федерации наметилась тенденция на ужесточение нормативно-правового регулирования защиты персональных данных. 30 ноября 2024 года Президент России В.В. Путин подписал федеральный закон о внесении изменений в Уголовный кодекс Российской Федерации[66]. Как отмечает Государственно-правовое управление Президента, в обновленной редакции УК РФ (статьёй 272^1), уголовная ответственность установлена соответствии со статьёй 272^1 УК РФ, устанавливающей ответственность за незаконные использование, передачу (распространение, предоставление, доступ), сбор и хранение компьютерной информации, содержащей персональные данные, полученной путём неправомерного доступа к средствам её обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путём.

Действие статьи 272^1 Кодекса будет также распространяться на лиц, передающих компьютерную информацию, содержащую персональные данные, иностранным гражданам, организациям или государственным структурам, а также за трансграничное перемещение носителей, содержащих такие данные. Кроме того, уголовная ответственность предусматривается за создание и администрирование сайтов и других интернет-ресурсах, а также программ, заведомо предназначенных для незаконного хранения и передачи персональных данных, полученных незаконным путём.

В соответствии с Федеральным законом положения новой статьи Кодекса не будут применяться в случаях, если персональные данные используются исключительно для личных или семейных нужд[67].

Правило четвёртое – know your customer. При получении заказа на подготовку исследовательской работу следует остерегаться иностранных граждан или юридических лиц, в особенности представителей государственных органов (посольств). В контактах с ними следует проявляться максимальную бдительность: в подобных случаях речь может идти о попытках привлечь российского специалиста к сотрудничеству на конфиденциальной основе – проще говоря, о попытках вербовки. Пример бывшего журналиста газеты «Коммерсант» Ивана Сафронова, осужденного по обвинению в государственной измене, печален и поучителен[68].

[66] Федеральный закон от 30.11.2024 № 421-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации"
[67] Установлена уголовная ответственность за незаконное использование, передачу, сбор и хранение персональных данных. Президент России. URL: http://kremlin.ru/acts/news/75705 (дата обращения: 6.12.2024)
[68] Дело Сафронова. Коммерсант. URL: https://www.kommersant.ru/theme/562 (дата обращения: 6.12.2024)

Список используемых аббревиатур и сокращений

API – от англ. application programming interface, программный интерфейс

OSINT – разведка по открытым источникам

КВРН – контроль над вооружениями и нераспространение

МБР – межконтинентальная баллистическая ракета

ТТХ – тактико-технические характеристики

Бужинский Евгений Петрович, Председатель Совета АНО "ПИР-Центр", Профессор Института перспективных стратегических исследований НИУ ВШЭ. Генерал-лейтенант (в отставке)

“Важность разведки данных по открытым источникам сомнений не вызывает. Современные инструменты, включая коммерческие спутниковые снимки, инструменты геолокации, социальные сети и т.д., позволяют составить более полную картину военно-политической деятельности иностранных государств. По собственному опыту знаю, что грамотный анализ открытых источников позволяет правильно оценить обстановку и сделать точный прогноз ее развития.

Отрадно, что ПИР-Центр и МГИМО МИД России взялись за разработку методики использования OSINT применительно к вопросам контроля над вооружениями и нераспространения оружия массового уничтожения. Представленное пособие будет весьма полезно для молодых специалистов-разоруженцев как отправная точка при проведении исследований в этой области.”

Данное методическое пособие (доклад) доступно для скачивания по ссылке:

Магистерская программа МГИМО МИД России и ПИР-Центра “Международная безопасность”

2025