ПРИМЕНЕНИЕ OSINT В АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

А.Г.Додонов, Д.В. Ландэ, В.Г. Путятин

1. Постановка проблемы

Разведка на основе открытых источников является важным направлением разведывательной деятельности, которая должна быть интегрирована в разведывательный цикл для гарантий того, что вышестоящее руководство как лицо, принимающее решения (ЛПР) и формирующее политический курс, целиком и полностью проинформировано. Одним из методов ведения технической разведки с помощью мониторинга информации из открытых источников, ее анализа, подготовки и своевременного предоставления конечного продукта ЛПР в целях решения определенных разведывательных задач, является OSINT (Open source intelligence) – разведка на основе открытых источников [1].

2. Цель работы

Необходимо выполнить анализ методологии и применяемых инструментов и сервисов для OSINT в аналитической деятельности.

3. Изложение основных результатов исследований

OSINT включает в себя [1]: 1) поиск, выбор и сбор достоверной информации, полученной из общедоступных источников, и её анализ и составление аналитических рекомендаций, информационно-аналитические отчеты, ретроспективные обзоры СМИ, мониторинги, рейтинги, индивидуальные тематические подборки и аналитические записки по определенным темам (событиям, лицам, структурам); 2) проведение конкурентной и бизнес разведки в Интернет; 3) составление графических схем визуализации информации. OSINT используется как в частном секторе, так и в военных и разведывательных службах в течении многих лет, подходы и источники информации были отобраны и упорядочены специалистами из Лэнгли (где находится штаб-квартира главной американской разведывательной организации). Ныне OSINT доступен всем при помощи нескольких Интернет утилит или приложений, которые можно установить на свои компьютеры дома. *Суть всего процесса OSINT* во-первых в том, что обязательным является наличие стороны, для которой исследование будет представлять реальную ценность. Во-вторых - это «Анализ», который является ключевым для проведения оценки информации, полученной из открытых источников. Сегодня компании используют OSINT называя его, однако, «конкурентной разведкой». Можно получить аналитическую информацию по заданной теме исследуя множество медиа и онлайн источников. Эта информация может быть экстраполирована в значимые сведения о компании, лицах, группах или странах, которые они возглавляют. *Базовая идея OSINT* – сбор информации для последующего анализа отчетов об Объекте. Анализ может также привезти к упреждающему анализу поведения и прогнозу, однако все зависит от целей аналитика. В разведывательном сообществе термин «открытый» указывает на общедоступность источника (в отличие от секретных источников и источников с ограниченным использованием), он не связан с понятием open source или public intelligence. По утверждениям аналитика ЦРУ Шермана Кента, политики получают до 80 % информации, необходимой им для принятия решений в мирное время, из открытых источников. OSINT применяется из-за низкой стоимости, повсеместной доступности, быстрого доступа, режима реального времени, надежности, отсутствия грифа секретно.

Терминология OSINT

В терминологии OSINT существуют два важных определения: 1) Открытый источник – персона или группа, которая предоставляет информацию без требования сохранения ее конфиденциальности – информация или отношения незащищенные от публичного раскрытия. Открытый источник информации может быть общедоступным, но

не вся публично доступная информация является открытым источником. Открытые источники относятся к среде общедоступной информации, и не имеют ограничения в доступе для физических лиц. 2) Общедоступная информация - данные, факты, инструкции или другие материалы, опубликованные или размещенные для широкого использования; доступные для общественности; законно увиденные или услышанные случайными наблюдателями; представленные на открытых встречах для общественности.

Открытые источники для OSINT

К открытым источникам для OSINT относят: печатные и электронные средства массовой информации (СМИ) - газеты, журналы, радио, телевидение, телефонные справочники; интернет (социальные сети, чаты, форумы и т.д.), в частности веб-сообщества и контент, созданный пользователями (en:user generated content) - социальные сайты, видеохостинги, вики-справочники, блоги, форумы; публичные правительственные отчеты; официальные данные о бюджетах, демографии, материалы пресс-конференций, различные публичные заявления, белые книги, технические документы, руководства и инструкции – всё то, что можно услышать, посмотреть, прочитать; наблюдения - радиомониторинг, использование общедоступных данных дистанционного зондирования земли и аэрофотосъемок; информация из профессиональных или академических источников: профессиональные и академические отчеты, конференции, доклады, статьи, включая ту литературу, которая относится к «серой»; коммерческие данные - например, ежегодные отчеты компаний; аналитические работы отдельных экспертов.

К открытым источникам и публично доступным сведениям относят также [2]: дипломатические миссии; торгово-промышленные палаты - неправительственные организации; религиозные организации; разведывательные организации общенационального уровня; академическая сфера - программное обеспечение, диссертации, лекции, презентации, научно-исследовательские работы, знания в печатном и электронном виде по экономике, географии, международным отношениям, региональной безопасности, науки и технологий; государственные, межправительственные и неправительственные организации - базы данных, обнародованная информация и печатные отчеты, обзоры широкого спектра в экономике, окружающей среде, географии, гуманитарных науках, безопасности, науке и технике; коммерческие и общественные информационные службы, печатные новости текущих международных, региональных и локальных событий; архивы (библиотеки) и исследовательские центры - печатные документы и цифровые базы данных по ряду вопросов таких, как знания и навыки информационного поиска; индивидуальная и групповая информация - рукописная, рисованная, опубликованная, печатная или распространенная информация (например, искусство, граффити, открытки, постеры или веб-сайты); «серая литература» - научные доклады и записи, подготовленные в частном секторе, правительственных учреждениях или академических институтах, которые лишь ограниченно доступны, экономические и исследовательские отчеты, технические инструкции, рабочая документация, неофициальные правительственные документы, диссертации (а также тезисы), препринты, маркетинговые исследования, информационные бюллетени, отчеты о путешествиях, дискуссионные документы. Преимущества открытых источников информации для разведки очевидны: они оперативны, особенно сейчас, когда любые события освещаются тележурналистами в режиме онлайн и чем быстрее поступает информация, тем меньше возможностей её исказить. Специалист сможет сделать безошибочные выводы, анализируя картинку прямого эфира из горячей точки.

Аналитические функции OSINT

Включают: контент-анализ информационных материалов; просмотр результатов тематической подборки в виде цитат (результаты сбора информации в сети Интернет); статистический анализ источников информации по освещению интересующих пользователя событий.

Этапы OSINT

Процесс поиска и обработки информации делится на несколько этапов [3]: Первый этап заключается в постановке задачи руководством - необходимо понять задачу, деконструировать аналитическую проблему. Затем выполняется планирование – этап разработки плана сбора информации, соответствующего этой проблеме. Должно быть принято решение относительно того, что должно быть проверено и проанализировано. Должна быть сделана четкая формулировка целей и задач. После этого выполняются поисковые работы, для этого необходимо выбрать методы и средства, которые помогут идентифицировать и получить необходимую информацию. Собранная информация должна быть обработана, выполнена ее очистка и анализ. Следующий этап включает анализ и оценку ключевых источников и их содержания. Помимо прочего, необходимым является оценка надёжности источника. Анализ - это ключевой фактор, без которого невозможно интерпретировать большие объемы данных. Сбор информации должен быть целенаправленным. При составлении отчета, отвечающего на конкретные вопросы ЛПР необходимо понять его информационные потребности. Законченные продукты разведки принимают много форм в зависимости от потребностей ЛПР, и требований к отчетности. Цикл разведки - замкнутый контур, обязательно должна учитываться обратная связь, полученная от ЛПР, которая может вести к пересмотру исходных требований.

Инструменты и сервисы для OSINT

Приведем некоторые инструменты и сервисы для OSINT по адресам [4]:

Программы: http://dr-watson.wix.com/home; http://www.fmsasg.com/; http://www.newprosoft.com/; http://neowatcher.com/ru/; SiteSputnik; WebSite-Watcher; http://www.scribd.com/; http:// www.atlasti.com/; Ashampoo ClipFinder HD; http://www.advego.ru/plagiatus/ - инструмент интернет-разведки; http://neiron.ru/toolbar/; http://web-data-extractor.net/; CaptureSaver; http:// www.orbiscope.net /en/software.html - система веб мониторинга; http://www.kbcrawl.co.uk/ - для работы в «Невидимом интернете»; http://www.copernic.com/en/products/agent/index.html; Maltego - позволяет устанавливать взаимосвязь субъектов, событий и объектов в интернете.

Сервисы: new http://yewno.com/about/; https://start.avalancheonline.ru/landing/?next=/; https://www.outwit.com/products/hub/; http://www.iptrackeronline.com/email-header-analysis.php; https://github.com/search?q=user:cmlh+maltego; http://www.whoishostingthis.com/; http://appfollow.ru/; http://spiraldb.com/; https://millie.northernlight.com/dashboard.php?id=93; http://byratino.info/; http://www.datafox.co/; http://visualping.io/; http://spyonweb.com/; http://bigvisor.ru/; http://www.itsec.pro/2013/09/microsoft-word.html; http://granoproject.org/; http://imgops.com/; http://sergeybelove.ru/tools/one-button-scan/; http://isce-library.net/epi.aspx; https://zmap.io/index.html; https://www.rivaliq.com/; http://watchthatpage.com/; http://falcon.io/; http://watchthatpage.com/; https://addons.mozilla.org/ru/firefox/addon/update-scanner/; http://agregator.pro/; http://price.apishops.com/; www.recordedfuture.com; http://advse.ru/; http://spyonweb.com/; http://www.connotate.com/solutions; http://saplo.com/; http://startingpage.com/; http://newspapermap.com/; http://infostream.com.ua/ - система мониторинга новостей «Инфострим»; http://www.instapaper.com/; http://www.wizardrss.com/; http://screen-scraper.com/; http://www.recipdonor.com/;

Поисковики: https://www.idmarch.org/; http://worldc.am/; https://app.echosec.net/; http://www.dtsearch.com/; http://www.strategator.com/; http://www.shodanhq.com/; http://search.usa.gov/; http://visual.ly/; http://go.mail.ru/realtime; Zanran; http://www.ciradar.com/Competitive-Analysis.aspx - система поиска информации для

конкурентной разведки в «глубоком вебе»; http://public.ru/Cluuz;
http://www.wolframalpha.com - поисковик завтрашнего дня.

4. Выводы

Применение OSINT позволяет получить ответ на многие возникающие у ЛПР вопросы, а также сосредоточить усилия разведорганов на выполнение более сложных и «узких» задач, не распыляя силы других направлений разведки на добывание того, что можно получить из открытых источников. Технология OSINT является одной из важных технологий «глубинного сбора» разноуровневой разноформатной информации, а также формирования на ее базе принципиально новых знаний. Распространение и использование проверенной информации из открытых источников позволяет осуществлять обмен такой информацией, поскольку при ее извлечении не используются скрытые методы и секретные источники.

1. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США .- [Електронний ресурс].- режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/3217
2. Open Source Intelligence (OSINT): Issues for Congress. - [Електронний ресурс]. – Режим доступу: https://www.fas.org/sgp/crs/intel/RL34270.pdf
3. Балуев Д.Г., Новоселов А.А. Анализ разведданных из открытых источников: Учебно-наглядное пособие. — Нижний Новгород: НИИ кризисных информационных систем, 2011. — 127 с.
4.Инструменты и сервисы для OSINT http://uplink.motd.org/2017/04/osint-tools-and-service/