

OSINT

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ РАБОТЫ С ОТКРЫТЫМИ
ИСТОЧНИКАМИ



автор: Нежданов Игорь
2025 год

ВВЕДЕНИЕ

С выходом генеративного искусственного интеллекта в свободное пользование сложилось впечатление отмирания профессий интернет-разведки и аналитиков. Вроде как стало возможным все задачи взвалить на ИИ. Но нет, первое впечатление оказалось не верным. И дело даже не в умении составлять промты для сервисов, что тоже требует понимания, что вы хотите получить, в каком виде и из каких источников.

Дело в том датасете, на котором обучен ИИ - в доверии к этому набору данных, а точнее в недоверии к этим данным. Ведь вы не знаете какие именно данные использованы для обучения. Да и какие ограничения на задаваемые вопросы заложили разработчики тоже не понятно. Мало того, составление обучающих датасетов требует времени, а значит «познания» нейронки отстают от текущей ситуации и такое отставание может быть от полугода и больше. А сервисы, обещающие поиск по интернету, ограничены базами глобальных поисковиков, которые «видят» менее 20% доступных данных (оценочные суждения экспертов).

Ни в коем случае не призываю игнорировать прогресс! Наоборот – обязательно исследуйте новые инструменты и используйте их. Использованию ИИ для OSINT в книге посвящен целый раздел "СБОР ИНФОРМАЦИИ" - "Сбор данных в интернете с помощью ИИ", в «Методиках» приведены промты под профильные задачи, а по тексту разбросаны другие примеры промтов. Но делайте это не бездумно, а осознанно: понимая какие есть ограничения у сервисов ИИ, как их преодолеть, как не попасть в ловушку «одного контролируемого источника» и т.п.

И вот тут мы вновь возвращаемся к тем, кто знает, как искать информацию вручную, где что можно почерпнуть, уточнить и понять, как неявно подтолкнуть собеседника к освещению интересующей темы. И к аналитикам – людям, хоро знающим интересующую нас предметную область и способным относительно быстро сформировать ваше представление о ней, знающим как правильно сопоставить данные, сделать прогноз и сформулировать рекомендации.

В книге приведено много разнообразных источников информации, но не забывайте, что они постоянно меняются, переезжают на новые площадки, прекращают поддерживаться автором, становятся платными, меняют разметку страницы и просто закрываются. Поэтому некоторые из приведенных примеров к моменту как вы решите использовать могут оказаться недоступными или со сменным функционалом.

OSINT, как много в этом слове...

Начнем с главного – с понимания что же такое этот пресловутый OSINT, а иначе будет непонятно отчего так часто мы слышим фразу «осинтеров много, а осинт реализовать никто не может».

OSINT (open source intelligence) — это дисциплина, методология и набор инструментов, ориентированных на сбор и анализ информации из открытых (общедоступных) источников. А также самостоятельный род деятельности. И слова «открытые» и «общедоступные» в характеристиках источников информации тут определяющие. Сами

источники могут быть как бесплатные, так и платные, как со свободным доступом, так и по логину и паролю. Но они должны быть общедоступные и не нарушающие закон.

Иногда в англоязычном сообществе вместо OSINT используют аббревиатуру OOSI (online open source investigations, расследования по открытым источникам в сети), и OSI (расследования по открытым источникам). Разница между OOSI и OSI заключается не только в названии: OOSI касается расследований, где используются только источники из интернета, а термином OSI описываются исследования, где используются и «оффлайновые» открытые источники. Начинающие исследователи используют термины OOSI или OSI еще и по тому, что им кажется, что OSINT указывает на связь с разведывательными органами.

Под открытыми источниками понимают любые доступные пользователям ресурсы, откуда информация может быть получена без нарушения закона. И вот тут начинается самое непонятное подрастающему поколению. Например, слитые документы или БД — это ведь общедоступные данные? Они ведь доступны всем. Но увы нет - краденные базы данных, выложенные в телеграм канале, во-первых, уже «краденные», а значит получены с нарушением закона. То-есть не могут относиться к информации, собранной без нарушения закона. Во-вторых, такие данные чаще всего содержат служебную, коммерческую, а то и государственную тайну. Использование таких сведений влечет за собой очень серьезные уголовные последствия.

Поэтому использование ворованных, слитых, «серых» баз данных или документов может быть, чем угодно, но только не OSINT. Назовем эту деятельность CheckINT (не путать с LeakINT). Правда и тут есть нюансы, связанные с разным правовым регулированием добытых данных и процесса их добывания в разных юрисдикциях.

Помимо «теоретических» отличий есть и весьма практические в разграничении что относится к OSINT, а что нет. Об этом часто забывают начинающие осинтеры, а то и вовсе не задумываются об этом, то-же самое заблуждение свойственно и специалистам, недавно ушедшим из госструктур в бизнес. Это связано с синдромом охотника.

1. Если осинтер работает внутри частной организации, то добывание информации противоправными методами становится угрозой для самой компании. Представьте, что правоохранителям становится известно о такой работе внутри фирмы. Что будет дальше?
2. Если осинтер работает автономно, поставляет результат противоправной работы заказчику из бизнеса, то такую информацию последний не может использовать в суде, как и в других действиях, связанных с доказыванием так как в этом случае будет как пункте 1.

Поэтому заявления типа «клиенту без разницы как добыта информация» свойственны либо специалистам без опыта, либо тем, кто готов подставить заказчика.

Чем же отличается обычный гуглинг от OSINT? Во-первых, в методологии и в глубине подхода. Там, для многих обывателей поиск и завершается, а для профессионалов OSINT только начинается работа. Во-вторых, OSINT не ограничивается интернетом, как бы этого не хотели молодые апологеты профессии.

Но это еще не всё. В определении «OSINT это дисциплина, методология и набор инструментов, ориентированных на сбор и анализ информации из открытых источников» есть еще одна составляющая, про которую часто забывают – анализ информации.

Перечень результатов поиска в разных источниках это не анализ. Результатом же анализа является новая информация, которая может быть выражена в выявлении неявного, осмысление проблемы на новом уровне, прогноз развития ситуации или рекомендации.

Что такое анализ

Понять, что такое анализ не просто, особенно с учетом того, что никто не знает, как работает наш мозг. Но наведение порядка с пониманием процессов хотя-бы на самом общем уровне позволяет избежать некоторых ошибок в дальнейшем.

Для начала важно принять то, что анализ начинается за долго до привычного всем одноименного этапа работы с информацией – анализ начинается с осмысления проблемы (поставленной задачи). С самых первых шагов этого процесса, вы уже осуществляете анализ информации:

1. вникая в поставленную проблему, вы разбираетесь в ситуации, стараетесь понять суть проблемы, ее предпосылки и последствия и все это анализ информации;
2. подбирая источники, для дальнейшего исследования, вы также занимаетесь анализом, принимая решение о полезности и достоверности источников;
3. создавая собственные информационные фильтры, для отсеивания ненужной информации, вы также занимаетесь анализом информации;
4. собирая информацию и осуществляя ее предварительную оценку, вы продолжаете заниматься анализом;
5. а уж затем вы приступаете к тому, что обычно называют анализом информации, но закончив его вы не прекращаете анализировать – вы формируете итоговый документ (оформляете результат анализа) и продолжаете заниматься анализом.

Главное, на каждом этапе не забывайте для чего вы все это делаете, иначе сильно отклонитесь от оптимального маршрута достижения цели, распылите и увеличите расход ресурсов, в первую очередь времени и в лучшем случае затяните процесс анализа, а в худшем – не получите ожидаемого результата.

А теперь попробуйте объяснить, как происходит анализ информации у вас в голове. Какие процессы происходят, когда вы получаете новую информацию? Что за чем следует. Это не просто – ведь вам нужно отследить изменение ваших мыслей, которые происходят ежесекундно в вашем центре принятия решений.

Например, вы узнали что-то новое, не совсем вписывающееся в вашу картину мира. Что вы делаете с поступившей информацией? С чего начинается обработка такой информации? Что происходит затем?

Если совсем упростить описание этого процесса, то вот что происходит у вас в голове:

1. вначале «декодирование» информации – её понимание, вы рассматриваете информацию с точки зрения понятно или нет, это и язык, это и терминология, это и особенности изложения материала;

2. затем происходит «осмысление» информации – проверка на противоречия, на соответствие вашим задачам, её своевременность, полезность, применимость;
3. после чего начинается выявление согласованности новой информации с уже имеющейся у вас и в конечном счете оценка доверия к новой информации;
4. и только после этого начинается использование информации – её интерпретация, формирование прогнозов, использование для самообучения, для выработки решений, формирования отчетов и т.п..

Эта последовательность действий в нашей голове, чаще всего, происходит в течении секунд. И именно из-за этой последовательности и алгоритм действий аналитика в реальном мире, обычно следующий:

1. оценка поступившей информации – то самое ее декодирование, осмысление и оценка полезности;
2. каталогизация полученной информации, ее архивирование (хранение), структурирование, сопоставление, декомпозиция;
3. формулирование выводов, построение гипотез и выработка рекомендаций.

К сожалению, у этого процесса есть несколько неприятных особенностей. Первая связана с объемами информации. По причине ограниченности ресурсов необходимо контролировать объем получаемой, исследуемой и накапливаемой информации. В противном случае нужно создавать службы сопоставимые с государственными учреждениями. Поэтому на начальном этапе необходимо поставить некоторый фильтр, уменьшающий поток информации. Бесспорно, что такое уменьшение объема должно минимально сказываться на ценности информации. А это уже зависит от настройки самого фильтра. Тем ни менее, не зависимо от качества настройки фильтра что-то должно «попасть в корзину». И чем четче описан процесс выбраковки, чем точнее выполняется такая функция, тем меньше полезной информации будет утеряно и тем меньше ресурсов потребуется для работы с поступающей информацией.

Еще одна особенность связана с необходимостью «ручного» труда в анализе. Если для работы со структурированной информацией есть достаточно известных и доступных инструментов, то обработку текстовой информации часто приходится осуществлять вручную. Да есть масса поисковых систем, но все они способны только искать заданный набор символов и не проводить смысловой анализ. Есть прекрасные решения, позволяющие выявлять дублируемую информацию, дабы не тратить время на одно и то же. Есть хорошо работающие движки, выявляющие связи в неструктурированной информации. Но конечная обработка и интерпретация всё равно остаётся за человеком. И это вполне понятно – слишком велико количество возможных вариантов и оттенков, которые дает человеческая речь, в том числе и письменная. Поэтому основным инструментом при анализе текстовой информации является голова аналитика. А важной составляющей – способность анализировать и знание технологий анализа. Тем технологиям, которые требуются в первую очередь для работы подразделений бизнесразведки на современных предприятиях.

ОРГАНИЗАЦИЯ РАБОТ

Общение с руководителем (заказчиком информации)

Начается всё для специалиста OSINT с постановки задачи. К сожалению, уже на этом шаге совершаются ошибки, приводящие к низкой эффективности, снижению точности, а значит и полезности результата работ.

Как помочь заказчику точно сформулировать задачу

Говоря об OSINT нужно всегда помнить, что есть тот, кому нужна информация, а есть тот кто эту информацию находит или готовит. Последний это собственно подразделение OSINT, а первый это всегда заказчик. Причем не важно является заказчик сотрудником той же организации, в которой работает OSINT или это внешняя организация или человек. Важно, что тот, по чьему заданию осуществляется работа это всегда заказчик информации. Такое разделение облегчит дальнейшее понимание работы OSINT.

Выполнение структурой OSINT полученного заказа не означает, что не нужно контактировать с заказчиком до момента выполнения заказа. Наоборот, с заказчиком необходимо поддерживать постоянный контакт. Фактически необходимо проводить обучение заказчика, формирование у него определенного видения ситуации и разведку его позиции. Заказчики в большинстве случаев люди слабо представляющие, что это такое и как это можно использовать. Они не понимают всех возможностей данного инструмента и его ограничений. Поэтому частенько не дают всей нужной для работы информации. Кроме того, никому не хочется «выносить сор из избы» и как следствие исполнителю передается не вся необходимая информация по вопросу, а только ее часть, причем сильно урезанная. Фактически создается ситуация использования OSINT «в темную». Это приводит к разным последствиям, например:

1. распыление средств и увеличение расхода ресурсов по сравнению с ситуацией, когда есть вся необходимая информация;
2. вероятность упустить важную информацию в силу непонимания истинной цели мероприятия;
3. а то и риск попасть под ответные меры криминальных структур, государственных органов и т.п.;

Чтобы избежать подобных ситуаций нужно получить у заказчика максимально полную информацию по проблеме и в ходе работы не только держать его в курсе происходящих у вас изменений, но и уточнять изменения ситуации у него.

Понятность и точность в формулировании задачи

Каждая постановка задачи должна быть четко и ясно сформулирована. От того на сколько точно сформулирована задача зависит как объем необходимых ресурсов, так и исключение ситуации, когда заказчик говорит «а я не то имел ввиду...». Кроме того, четкая постановка задачи облегчит заказчику контроль за исполнением, а вам даст возможность не расплывать ресурсы.

Обсудите выполнимость поставленной задачи

Выполнимость задачи это не только то возможно ее выполнение или нет. Это еще и границы выполнимости: что можно сделать, что сложно, а что опасно пытаться сделать. Отсюда и оценка рисков и затрат и стоит ли полное решение поставленной задачи затрат на нее.

Обсуждение выполнимости поставленной задачи позволяет устраняет у заказчика иллюзию «волшебной палочки» и позволяет вам более прагматично обсудить пределы ваших задач и полномочий. Ни в коем случае не пытайтесь сформировать у заказчика мнение о вас, как о человеке способном сделать все что он пожелает. Это ведет к разочарованию и разрыву отношений.

Поставьте реальные сроки

В ходе обсуждения проблемы необходимо договориться о временных рамках выполнения заказа. Предлагайте только реальные сроки, иначе сами себя загоните в ловушку. Ведь вам необходимо как минимум:

1. разработать план мероприятий;
2. выявить, привлечь к сотрудничеству или создать источники и обеспечить с ними четкое взаимодействие;
3. собрать информацию и обработать ее;
4. проверить результаты ваших исследований;
5. оформить отчет.

На все это требуется время, которого может не хватить и тогда вы, скорее всего, попытаетесь ради исполнения заказа в срок не обращать внимание на качество. Результат такого отношения нет смысла даже рассказывать.

Перспектива или тенденция

В ходе общения необходимо просвещать заказчика на предмет того, что точность всегда требует значительных ресурсов, но, в тоже время, как тенденция (перспектива) выявляется всегда значительно дешевле и быстрее. И что не менее важно – перспектива уже позволяет принимать обоснованные и правильные решения. Ведь не секрет, что часто

бывает так, что в сложившейся ситуации надо принять хоть какое-то решение, а не топтаться на месте. Поэтому понимание ситуации в общих чертах сегодня к вечеру гораздо ценнее в сегодняшнем быстро меняющемся мире, чем точное знание ситуации, но через пару дней.

Поддержка обратной связи

Вам необходимо непрерывно поддерживать обратную связь со своим заказчиком. Это особенно важно на первом этапе. Такая обратная связь позволяет точнее и быстрее достичь цель, и главное, вовремя скорректировать свои усилия при выявлении ошибки или изменении обстановки. Особенно если вы работаете в новой для себя теме. В такой ситуации ваш заказчик становится вашим основным консультантом. Формы поддержания такой связи могут быть различными. Например, еженедельные отчеты по конкретным направлениям держат конечного пользователя в курсе дела некоторых из наиболее важных моментов развития событий. Кроме того, заказчик всегда может что-то уточнить и вовремя среагировать на какие-то изменения. В современном быстро меняющемся мире это очень важно.

Стремитесь общаться по вопросам информационных потребностей с максимальным числом сотрудников компании. Сотрудники компании заказчика тоже ваши потенциальные источники. Нельзя ими пренебрегать. Первые беседы со всеми ими имеют следующие основные цели:

1. собрать максимальное количество информации о положении дел на новом для вас рынке;
2. выяснить положение дел с добычей конкурентной информации в компании;
3. сформировать у сотрудников определенное мнение о сотрудниках структуры OSINT.

Но тут есть ряд особенностей. Например, ТОП-менеджеры. Это очень занятые люди. Но это люди, которым очень важно положение компании, и они гордятся своей компанией. Это люди, основной частью работы которых является думанье и общение (выработка решений и участие в обсуждениях, совещаниях и пр.). Скорее всего у вас не получится записать все мысли, которые будут вам высказаны, поэтому воспользуйтесь диктофоном. Учитывая особенности ТОП-менеджеров постарайтесь чтобы они рассказали о бизнесе в свободной форме, что бы поведали вам:

1. о самой компании, ее положении, ее сильных и слабых сторонах, о ее ресурсах и особенностях;
2. о рынках, на которых конкурирует компания и об особенностях этих рынков;
3. об общей стратегии компании для каждого рынка, а также, ключевых факторах успеха на этих рынках;
4. о первостепенных конкурентных силах на каждом рынке;
5. как ведется конкуренция на этом рынке;
6. что он считает самым сильным конкурентным преимуществом у других компаний;

7. какие виды конкурентной информации являются для них наиболее важными;
8. какого типа должны быть новости, и какого рода должен быть анализ;
9. каково их восприятие того процесса анализа, который на сегодня имеется в их компании (если он есть), и что им в нем нравится, а что – нет;
10. какие типы информации они получают сегодня (определив то, что они считают наиболее важным и то, что они получают сегодня, вы получите список невыполненных потребностей);
11. какие конкурентные ситуации не дают вам спать спокойно.

Чем больше вы общаетесь с заказчиком и его сотрудниками, тем лучше. Постарайтесь побеседовать с максимальным количеством персонала. В результате вы получите массу вводной и корректирующей информации, составите первичное представление о проблемах и потенциале компании, выявите общие тенденции, и что не менее важно пропиарите свою деятельность, разъясните людям необходимость OSINT и снимете ряд ограничений для поступления к вам информации. Но при этом не обещайте, что OSINT обеспечит «всем все». Объясните, что это только начало движения в определении направления работ.

Постановка задачи

Что из себя представляет результат работы подразделения OSINT? Это информация, необходимая для обоснованного и взвешенного принятия решения по сложным стратегическим вопросам. Все остальное — это побочный продукт. Да этот побочный продукт может быть очень полезен и значим, но тем ни менее главное это знания необходимые для стратегического видения. А кто занимается стратегическим планированием в компании, кто определяет направление развития, кто может сказать куда движется компания в дальней перспективе? Пожалуй, только первый руководитель.

Вот и получается, что результат работы подразделения OSINT является «сырьем» для работы руководителя компании, именно на руководителя компании в первую очередь должна быть ориентирована OSINT. Значит и задачи подразделению OSINT должен ставить именно первый руководитель – он единственный кто точно знает куда идет компания и какая информация ему нужна для принятия решений. Но руководитель чаще всего не может достаточно точно сформулировать свои информационные потребности. В этом ему необходимо помочь, поскольку от точности постановки задачи перед аналитиком зависит и эффективность работы данного подразделения и, в конечном счете, удовлетворенность потребителя информации (руководителя). От того, насколько четко сформулированы информационные потребности напрямую зависит то, как вы справитесь с задачей их удовлетворения.

Берем за правило, что эффективность разведывательной деятельности напрямую зависит от точности постановки задачи. Трудно представить ситуацию, когда руководство страны ставя задачу разведке говорит что-то вроде «Узнайте что-нибудь...». При этом наверняка, многим известна формула «Дайте мне все что известно о компании X и я сам решу что мне нужно». Куда идти, кого спрашивать, о чем спрашивать... Такая постановка вопроса ведет к следующим проблемам:

1- вам придется сильно распылять свои ресурсы, как финансовые и людские, так и время, (иногда весьма ограниченные), поскольку изучать придется объект со всех сторон и все что его (объект) окружает;

2- при передаче информации вы всегда можете оказаться в ситуации не справившегося с поставленной задачей, поскольку не знаете, что же нужно потребителю информации, и этот потребитель в любой момент, в зависимости от своего настроения, может утверждать, что он ожидал совсем иного. А теперь сравните формулировку «Дайте мне все что известно о компании X и я сам решу что мне нужно» с формулировкой «Мне нужно знать кто поддерживает компанию X на уровне губернатора». Вопрос не простой, но очень конкретный, и ответ на него должен быть очень конкретный. И исходя из самого вопроса уже можно строить план действий посредством разложения на составляющие вопросы.

К сожалению, не всегда можно добиться точной постановки вопроса от заказчика или руководителя. Это не обязательно связано с попыткой что-то скрыть от вас. Чаще это проявление особенности психики заказчика: если знаю я, то подразумеваю, что это знает и собеседник, а значит незачем об этом говорить. Для выявления цели аналитического исследования можно использовать несколько приемов.

Первый прием – последовательно задаем вопрос «зачем». В этом случае на каждый абстрактный ответ заказчика задается вопрос «зачем это вам». Простой приём, но будьте аккуратны. Часто после третьего «зачем» вас могут обвинить в тупости или начнут раздражаться.

Второй прием - беседа с заказчиком посредством наводящих вопросов пытаетесь понять, что его беспокоит, почему беспокоит именно это и именно сейчас, где он видит угрозу или почему важно именно это. Это тот-же прием «зачем», но чуть в более мягком формате. Поэтому и раздражение в ответ получите чуть позже, но увы – чаще всего все равно получите.

Третий прием - самостоятельно анализируете поставленную задачу с точки зрения чем это поможет заказчику в его работе. Поставьте себя на место заказчика и исходите из его целей и задач. Это сложнее и требует определенного опыта, но и результат полезнее.

Если заказчик настаивает, что бы вы ему дали всю информацию по проблеме или объекту, а он сам решит, что ему нужно, можно подыграть ему, сказав, что безусловно будет собрана вся информация, но, чтобы ему хотелось получить в первую очередь? Чтобы определить очередность. Тогда появляется шанс, что заказчик укажет что ему нужно прямо сейчас, а значит и важнее для него.

Перед началом такого разговора, поставьте себя на место заказчика и попробуйте понять, как поможет OSINT решить его проблемы. Как работа OSINT поможет ему избежать потенциальных угроз или снизить их негативное воздействие, как не упустить новые возможности, как их выявить и использовать для своей выгоды. Любой бизнесмен в своей работе обязан учитывать ключевые факторы успеха на том рынке, на котором он работает. Иначе очень быстро такой бизнесмен окажется в аутсайдерах, а на его место придут более прозорливые и быстрые. Такими факторами успеха может быть все что угодно (уровень подготовки персонала, цена, сервисное и постгарантийное обслуживание, качество самой продукции, новизна идеи, узкая специализация товаров или услуг, и т.п.). Кроме этого факторами влияющими на эффективность бизнеса являются действия конкурентов, их планы и стратегии, их ресурсы и способности повлиять на ваш бизнес, на вашу конкурентоспособность, и т.т.. Как видите разброс очень большой, а ресурсов обычно

ограниченное количество. Поэтому становится важно максимально точно выделить ту информацию, которая действительно является критической для компании. Сделать это можно только посредством продолжительных бесед с самим потребителем информации и с его сотрудниками.

Беседа с заказчиком

В ходе общения с заказчиком по поводу его информационных потребностей, исполнитель уясняет суть проблемы и что хочет от него заказчик. От того, как он это уяснит зависит то на сколько качественно исполнитель выполнит свою работу.

Первое общение с заказчиком по его проблеме является наиболее важным. Это первое определение его потребностей, это попытка понять, что действительно нужно руководителю, что он хочет, что его волнует на самом деле. Чаще всего, руководитель не может достаточно четко и ясно сформулировать свои информационные потребности. В такой ситуации вашей задачей становится подтолкнуть его к точному запросу информации. Задать направление движения мыслей заказчика можно посредством направляющих вопросов, сформулированных таким образом, чтобы понять его потребности, но не в коем случае не сформулировать за него. Но до того как вы зададите первый такой вопрос очень важно расположить к себе собеседника, показав ему, что он не единственный кто столкнулся с такой проблемой, что его проблема не такая уж эксклюзивная, что есть способы ее эффективного решения и вы их знаете и умеете применять.

Суть направляющих вопросов сводится к уточнению задачи, которую ставит перед вами «постановщик задачи», к пониманию того какая информация ему нужна для принятия решений. Строить такие вопросы можно от общего к частному. Например, от общих особенностей ситуации на рынке, на котором действует компания, к особенностям отдельных игроков на этом рынке и ситуаций здесь возникающих. При этом нужно использовать открытые вопросы, вопросы, которые не сужают и не подталкивают к заложенному в них ответу:

1. что помогло бы компании стать лидером в отрасли?
2. какое событие на рынке заставило поволноваться вас более всего?
3. какие действия конкурентов принесли больше всего проблем?
4. какие возможности были упущены вашей компанией и почему?

Ответы на такие вопросы уже содержат информацию что нужно искать, на что обращать внимание, что само по себе крайне важно для компании. А при их анализе выясняются те составляющие, по которым можно прогнозировать появление или развитие этих факторов.

На такую беседу с руководителем нужно идти имея при себе продуманный список вопросов. А в процессе беседы, ставя отметку напротив каждого пункта вы получаете предварительный план действий и исключаете ситуацию «я подразумевал не то...». Этот опрос гарантия того, что вы сами и ваш руководитель понимаете и согласны с теми результатами, которые он ожидает получить.

Заказчик обычно говорит, что надо то и еще то и еще вот то и то и другое. Слушая, вы понимаете, что если взяться за все сразу, то результат придется ждать очень долго –

просто не хватит ресурсов. В этой ситуации важно понять, что беспокоит заказчика более всего. А на его аргумент о необходимости ему всего, что он перечислил, ответить можно примерно так «Безусловно, мы исследуем все указанные направления, но что вам нужно в первую очередь?».

Формулировка задачи

Определиться с целью исследования это еще не все. Сама формулировка проблемы (задачи) имеет значение, ведь эта формулировка задает дальнейший ход рассуждений. Поэтому при получении задачи желательно попробовать ее расширить. Именно для этого и существует этап предварительной оценки ситуации, когда вы смотрите на задачу не с точки зрения ее выполнения, а с точки зрения ее связанности с другими процессами, ее влияния на них и значимость всех этих элементов для заказчика.

Разберем на примере. Предположим сложилась не простая ситуация «На парковке у офиса компании толчея, места всем желающим не хватает. Руководство компании поручает группе сотрудников предложить способы перепланировки парковки, чтобы она вмещала больше авто».

Руководство изначально определило проблему так: «Как увеличить емкость парковки». Но попробуйте вы сформулировать проблему. Ведь это можно сделать по разному. Например, так:

1. Избавиться от толчеи на парковке.
2. Обеспечить всех желающих местами на парковке.
3. Снизить нервозность в коллективе из-за споров по поводу машиномест.

Согласитесь, уже эти варианты формулировки проблемы заставляют взглянуть на ситуацию под разными углами. При этом, не надо забывать, что у разных участников ситуации разные интересы. Вот две основные группы участников этой не простой ситуации:

1. Руководство компании
2. Сотрудники компании, приезжающие на авто

Попробуйте сформулировать решение проблемы с точки зрения этих двух групп участников и с учетом их интересов. Обращаю внимание, что при предварительной оценке ситуации у вас уже возникла потребность в дополнительной информации (участники ситуации и их интересы). И эта дополнительная информация позволяет вам разобраться в хитросплетении отношений, понять, что на что влияет и с какой силой, а в дальнейшем определиться с оптимальным вариантом постановки задачи.

Руководство компании может сформулировать решение проблемы в следующем виде: «Повысить эффективность сотрудников».

Исходя из такой постановки задачи, для ее достижения надо «Снизить нервозность в коллективе из-за парковки».

А добиться снижения нервозности в коллективе по поводу какого-то ресурса можно разными способами, порой радикальными:

1. Увеличить число машиномест, доступных сотрудникам;
2. Закрыть парковку, чтобы все оказались в равных условиях;

Сотрудники компании, приезжающие на авто, могут сформулировать решение проблемы в следующем виде «Создать более комфортные условия работы для себя». И это подразумевает иной взгляд на проблему и иные варианты ее решения от «Переноса офиса поближе к дому» до «Найма психолога, который сделает всех пофигистами». Поэтому формулируйте задачи осмотрительно, с учетом потребностей заказчика и своих ресурсов.

Планирование

Планирование вообще — это системный подход к определению задач, ресурсов и стратегии для эффективного достижения желаемых результатов. А планирование в аналитической деятельности имеет ряд особенностей, которые нужно учитывать.

Определение информационных потребностей

Предположим, что задача сформулирована достаточно четко. Вы понимаете, что от вас хотят. Пора начинать основную работу. Начинать ее нужно с составления плана мероприятий. Как и любой план, он должен содержать этапы, работы, планируемые результаты и ресурсы (люди, время, финансовые затраты, технические средства, нематериальные ресурсы). Кроме того, в плане должны быть учтены альтернативные варианты достижения результата особенно в тех случаях, когда время жестко ограничено или есть риск не успеть за оппонентом. Но прежде надо ответить себе на следующие вопросы:

1. Что вы уже знаете об объекте вашего интереса? Или что можете узнать прямо сейчас?
2. Какие ресурсы могут вам понадобиться для выполнения задачи в срок и с минимальными затратами?
3. На что следует обратить особое внимание, на чем стоит сконцентрироваться?

Что вы уже знаете об объекте интереса?

Составьте перечень вопросов, на которые вам необходимо ответить. После этого просмотрите более ранние информационные материалы по проекту (если таковые есть) и проверьте свои материалы – возможно что-то уже попадало в поле вашего зрения. Проверьте нет ли у вас дополнительной информации по проекту. Посмотрите не появились ли за последнее время источники информации, связанные с проектом.

Что можете узнать прямо сейчас?

Изучите имеющуюся в компании информацию по проекту и связанным с ним вопросам. Поговорите с сотрудниками в других подразделениях вашей организации. Пообщайтесь с экспертами в данной области.

Тщательно изучив результаты общения с ТОП-менеджерами можно сформулировать в чем нуждается каждый из них, что нужно всем, что для них наиболее важно. Беседы позволяют определить приоритеты для проведения эффективного сбора и анализа информации. В свою очередь, понимание основных потребностей руководства (природа и масштаб запросов разведки для организации) позволяет оптимально использовать ресурсы для выполнения поставленной задачи. Итак – вы осознали то, на чем сконцентрируете свои усилия по данному проекту. Теперь можно определить, что вам необходимо для достижения поставленной цели:

1. в состоянии ли вы провести необходимые работы самостоятельно или вам нужна помощь?
2. есть ли необходимость в услугах сторонних организаций?
3. какие дополнительные ресурсы могут потребоваться и где их взять?

Услуги сторонних организаций это:

1. отчеты сторонних организаций по исследованию рынка;
2. доклады экспертов по интересующей вас проблеме;
3. консалтинг как организаций, так и отдельных экспертов;
4. услуги сотрудников вашей организации;
5. онлайн-базы данных.

Определение приоритетов.

Теперь необходимо определить, что нужно выполнить в первую очередь, а что может и подождать. В начале составьте приоритетность информационных потребностей заказчика (что он оценивает как наиболее важное, а что наименее). Далее разложите на составляющие эти потребности и опишите необходимые ресурсы для ответа на поставленные вопросы (в том числе и время). В ходе этой работы у вас выстроится общая картина выполнения поставленной задачи.

После построения такого перечня приоритетов проведите полный обзор планируемых вами действий – скорее всего, вы решите некоторые из них поменять местами. После окончательной правки перечня работ, приоритетов и ресурсов вы должны решить, как убедить заказчика дать вам доступ к требуемым ресурсам. Фактически вы составите план действий и необходимые для этого ресурсы.

Сведя воедино все выше сказанное можно утверждать, что до начала активных работ по проекту необходимо провести осмысление и составление концепции проекта. Это способ

заострения внимания на конечной цели, общей оценке и ее логическом обосновании. При проведении осмысления, устанавливаются два момента:

1- название проекта как тезис, четко ориентирующий вас на достижение поставленной цели, создающий в уме потребителя информации надежду на получение чего-то нового – заголовок проекта (название) передает смысл планируемой к передаче информации;

2- главное (резюме проекта) это - "синтезированная формулировка, широкая картина, основной момент информации, основное мнение о ней и главное содержание", - все это в виде краткого, простого повествовательного предложения, синтезирующего информацию о проекте в виде аналитического утверждения. Наличие этих двух составляющих позволит в дальнейшем не отклоняться от поставленной цели и даст некий ориентир при планировании и выполнении работ по проекту.

Составление плана

Что же такое план в OSINT? Это, как и везде, описание последовательности действий с комментариями в виде предполагаемых расходов ресурсов. Фактически для составления плана нужно последовательно ответить на несколько вопросов:

1. Какова ваша цель? Или что вы хотите узнать?
2. Какая информация вам нужна для достижения вашей цели?
3. Где или у кого эта информация может находиться?
4. Как получить доступ к этой информации? Что нужно для этого предпринять?

Какова ваша цель?

Это формулирование задачи. Вам нужно максимально кратко и при этом четко сформулировать вашу потребность. Это делается в несколько приемов:

1. формулировка проблемы — это описание того, что вы хотите в формате «как есть»;
2. формирование проблематики – это описание проблемы с учетом выявленных связей с другими системами ее ближайшего окружения;
3. постановка задачи - переформулирование исходной проблемы таким образом, чтобы кроме задания она содержала и направление поиска возможных вариантов решения;
4. определение целей — это ответ на вопрос ЧТО нужно сделать для решения обозначенной проблемы.

Какая информация вам нужна для достижения вашей цели?

Нужно понять, основываясь на какой информации вы сможете достигнуть поставленной цели или получить ответ на свой вопрос.

Где или у кого эта информация может находиться?

Используя профессиональные знания, знания коллег и житейский опыт нужно понять кто располагает нужной вам информацией, где эта информация может находиться. В данном случае не плохо бы привлечь экспертов, которые подскажут как обрабатывается интересующая вас информация, как передается, и кто имеет к ней доступ.

Как получить доступ к этой информации?

В данном случае вам предстоит понять возможные пути подхода к носителю интересующей вас информации. Например? подходы к человеку, который обладает нужной вам информацией.

После того как вы ответите на все эти вопросы и опишите какие ресурсы вам понадобятся для каждого шага, можно говорить, что план составлен. Останется лишь придать ему форму, соответствующую вашим требованиям. Это что касается общего планирования. Но ведь есть достаточно специфические мероприятия, к которым подобный подход не достаточен. Возьмем в качестве учебного примера планирование беседы с не знакомым консультантом, который предположительно обладает необходимой вам информацией. Не вдаваясь в пространные рассуждения план будет выглядеть так:

1. цель (что хотим получить);
2. объект (с кем будем общаться);
3. где когда планируется мероприятие (в т.ч. Обстановка);
4. используемая легенда;
5. вопросы, которые можно задать напрямую;
6. косвенные вопросы.

Развернутый план беседы дополняется несколькими вероятными направлениями хода общения, которые могут возникнуть и вашими действиями в случае развития ситуации не по сценарию.

Исходя из приведенного плана при подготовке к такому мероприятию вам необходимо проработать следующие вопросы:

1. идентификация объекта;
2. изучение объекта;
3. определение способов подхода к объекту (легендирование);
4. определение общего хода беседы;
5. определение способов подхода к интересующей вас теме;
6. определение способов «возврата» к интересующей вас теме;

7. определение способов «выхода» из беседы.

Идентификация объекта — это выявление признаков, позволяющих однозначно идентифицировать ваш объект. Применительно к человеку это может быть следующий набор:

1. фамилия-имя-отчество;
2. дата рождения;
3. паспортные данные;
4. прописка;
5. что-то еще...

Для каждого конкретного случая такой идентификационный набор может быть разным. Например, в очень узкоспециализированных областях может оказаться достаточно имени и отчества, или звания (академик) и фамилии. Поэтому при определении набора признаков (идентификаторов) необходимо руководствоваться принципом разумной достаточности и не стараться найти все что можно.

Изучение объекта – это исследование вашего будущего собеседника с точки зрения последующего эффективного общения с ним. Какая информация может вам помочь в получении от него нужных сведений? Это могут быть его увлечения и пристрастия, его отношение к тем или иным событиям, фактам, людям, его связи с организациями, его образование и культурный уровень, его язык общения и разговорчивость в конце концов. Все это вполне может оказать воздействие на ход планируемой беседы. Помимо этого, такое знание даст возможность более эффективно спланировать следующий этап.

Определение способов подхода к объекту (легендирование) – это выбор легенды, которой вы воспользуетесь для завязывания отношений с объектом, в том числе и краткосрочных отношений – на один разговор. Такая легенда выбирается исходя из нескольких факторов:

1. особенности той информации, которую вы хотите получить;
2. особенности вашего визави;
3. планы по дальнейшему взаимодействию с объектом.

Определение общего хода беседы – это ни что иное как составление собственно плана самой беседы – последовательности «вопрос-ответ» или последовательности смены тем. В начале определяется удобная вам последовательность – это оптимистический сценарий. Но не забывайте о необходимости (хотя и не всегда) наличия вводной части.

Определение способов подхода к интересующей вас теме – это определение того, как или посредством каких тем, каких переходов, намеков, уловок можно подойти к интересующему вас вопросу создав впечатление логично развивающегося диалога.

Определение способов «возврата» к интересующей вас теме – это то, как вы будете действовать (разговаривать) если общение пойдет не по планируемому вами пути. Для

этого нужно взять составленный план беседы (последовательности «вопрос-ответ» или последовательности смены тем) и каждый пункт составленного плана рассмотреть с точки зрения «а как может отреагировать на это объект?» и добавляется как правило еще два варианта - реалистический и пессимистический. По каждому «неудобному» для вас варианту необходимо определить то, каким образом вернуть беседу в нужное для вас русло. Какими словами, какими темами, какими приемами... И так вплоть до достижения конечной цели – получения требуемой информации.

Определение способов «выхода» из беседы – это определение того, как вам завершить общение, при этом не заострив внимание собеседника на интересующих вас вопросах, не оставив ощущения, что его использовали, создав возможность для дальнейшего общения если это необходимо.

Составленный вами таким образом план сам по себе уже подготовит вас к этой беседе и позволит значительно увереннее и спокойнее общаться с объектом и с большей вероятностью получить нужный вам результат.

Дезинформация

Еще одна особенность, а точнее глобальная проблема для OSINT, это дезинформация. Или как теперь модно говорить - фейки. Дезинформация оказывает значительное влияние на «сырье» для анализа, на сам аналитический процесс и на его результаты. Поэтому необходимо разобраться в этом явлении, прежде чем изучать сам анализ.

Что такое деза и откуда она берется

Дезинформация — это способ воздействия на человека, заключающийся в намеренном предоставлении ему информации, которая вводит его в заблуждение относительно истинного положения дел. «Дезинформация — это намеренное распространение заведомо ложной или искаженной информации с определенными целями.»

Цель дезинформации всегда одна – объект должен поступить так, как это необходимо дезинформатору. Совершить нужное действие, которое может выражаться в принятии решения, совершения действий в реальном мире или бездействий. Чаще всего дезинформацию используют для формирования репутации как негативной, так и позитивной.

Под дезинформацией в общем виде понимается формирование, компоновка и продвижение ложных сведений про интересующей объект, формирование неверного представления о событиях, фактах и явлениях и подталкивание к принятию неверных решений.

Дезинформация является чуть ли не основным инструментом информационно-психологических операций, которые проводят по всему миру все против всех. Поэтому объемы дезинформации в мире просто огромны.

Основные характеристики дезинформации:

1. **Намеренность:** Дезинформация создается с осознанием ее ложности, с намерением обмануть, что отличает её от случайных ошибок или неточностей.

2. Целевое воздействие: часто дезинформация направлена на конкретные группы или индивидов с целью вызвать определенные эмоциональные реакции.
3. Методы распространения: используются различные тактики, включая имитацию авторитетных источников, манипуляцию с рейтингами поиска, создание фальшивых новостных сайтов и использование социальных сетей для быстрого распространения информации.

Для примера, основные цели дезинформации в информационно-психологических операциях США, в соответствии с их доктринальными документами, включают:

1. Легитимизация военных действий в глазах международного сообщества и собственного населения.
2. Формирование благоприятного общественного мнения для поддержки военных операций США.
3. Дискредитация противника и создание негативного образа вражеского режима.
4. Поднятие морального духа своих войск и деморализация противника.
5. Обеспечение международной поддержки внешнеполитического курса США.
6. Создание условий для размещения военных баз США в стратегически важных регионах.
7. Оправдание применения военной силы путем создания видимости справедливости своих действий.
8. Изменение отношений, восприятия и поведения иностранных государств в выгодном для США направлении.
9. Поддержка военных операций на тактическом, операционном и стратегическом уровнях.
10. Формирование благоприятных условий внутри страны-противника перед началом военной операции.

Как дезинформируют

Дезинформирование тем сложнее осуществить, чем осведомленнее является объект воздействия. Оно и понятно – если объект знает истинное состояние дел, то информация, отличающаяся от этого знания, будет попросту игнорироваться им и воздействия не будет.

Соответственно основополагающие правила дезинформирования:

1. объект дезинформирования должен быть максимально отрезан от источников информации по интересующей и смежным темам – для него (объекта) должно быть непросто, а лучше совсем невозможно получить дополнительную информацию или проверить имеющуюся;

2. объект дезинформирования необходимо снабжать информационным суррогатом – урезанной информацией – только той информацией, которая отвечает задаче манипулятора. Это необходимо по тому, что в противном случае Объект будет сам искать возможность удовлетворить своё любопытство.

Помимо прямого обмана существуют и другие приемы дезинформирования:

1. Информационная перегрузка;
2. Дозирование информации;
3. Сенсация и сенсационность;
4. Смещение или отвлечение внимания;
5. Затягивание времени или замалчивание;
6. Легализация информации;
7. Своевременная ложь.

Одна из самых распространённых тактик дезинформаторов – выявить существующую в сообществе социальную проблему и работать на обострение напряжённости и разногласий, эксплуатируя эту проблему. Публикация материалов, усиливающих разногласия и разделение на «свой-чужой» – один из лучших способов привлечь аудиторию в социальных сетях.

Поэтому, для эффективного выявления дезинформации, нужно знать сообщества (целевые аудитории), на которые направлены манипуляции. Для этого поговорите с людьми в этих целевых аудиториях и попытайтесь понять, чем они живут. Что стало причиной их проблем в первую очередь и что делает попытки манипуляции эффективными? Может быть, какие-то обсуждения только кажутся манипулятивными, а на самом деле там так принято? Погрузившись в такую «цифровую этнографию», вы сможете полнее понять дезинформацию и, во многих случаях, видеть признаки особенно мощной кампании ещё до её «взлёта».

В интернете наиболее распространены следующие типы дезинформации:

1. Ложные новости (Fake News) - намеренно распространяемая ложная информация, выдаваемая за актуальные новости;
2. Манипуляция контентом - соединение реальных фактов, изображений или видео с вымыслом для создания ложного контекста;
3. Кликбейтные заголовки - привлекающие внимание, но часто искажающие суть новости заголовки;
4. Политическая пропаганда - систематическое распространение информации с определенным посылом для влияния на общественное мнение;
5. Ресурсы-клоны - создание поддельных сайтов, имитирующих авторитетные источники;

6. Манипуляция фактами - представление информации в искаженном или выборочном виде;
7. Политический ретроспективный анализ - искаженное представление исторических фактов и событий.
8. Использование ботов и фейковых аккаунтов для массового распространения ложной информации. Это позволяет создать иллюзию широкой поддержки определенных идей или новостей.
9. Эмоционально заряженный контент, направленный на разжигание недоверия к политическим институтам или определенным группам людей.

Психологические механизмы, способствующие распространению дезинформации в социальных сетях, включают:

1. Эффект иллюзии правды: Повторение информации увеличивает вероятность её восприятия как правдивой. Уже знакомая информация легче воспринимается и анализируется, что способствует её закреплению в сознании;
2. Эхо-камеры и групповая поляризация: Пользователи склонны взаимодействовать с теми, кто разделяет их взгляды, что усиливает существующие убеждения и способствует распространению дезинформации в замкнутых сообществах;
3. Эффект первичности: Люди придают большее значение информации, полученной ранее, что затрудняет изменение мнений даже после опровержения ложных сведений;
4. Эмоциональное заражение: Дезинформация часто вызывает сильные эмоциональные реакции, такие как страх или гнев, что способствует её быстрому распространению;
5. Когнитивные искажения и подтверждение существующих убеждений: Люди склонны принимать информацию, подтверждающую их уже сложившиеся мнения, и игнорировать противоречащие данные;
6. Недоверие к традиционным СМИ: Низкий уровень доверия к официальным источникам информации побуждает пользователей искать альтернативные источники, которые могут быть менее надежными.

Формируя в наших головах нужное мнение (отношение), манипулятор пытается воздействовать на нашу систему принятия решений. Мишенью может стать любой элемент от восприятия внешней информации (то, что мы видим, слышим, ощущаем) до реализации принятого нами решения. Но чаще всего злоумышленник нацеливается на одно из пяти элементов мыслительного процесса:

1. Сам процесс мышления;
2. Наши эмоции;
3. Наше воображение;
4. Наше внимание;

5. Нашу память.

Мышление

При атаке на наш процесс мышления манипулятор обычно старается нарушить логику рассуждений или подменить анализ оценочным суждением. Например, идеологически правильным суждением или ожидаемым аудиторией суждением. Очень показательный пример такого манипулирования приводит Осипов Г. в своей книге Общество знания: «Возьмем важнейшее утверждение, которое Горбачев высказал в обоснование перестройки, перефразируя Андропова (далее цитата):

«Мы не знаем общества, в котором живем». Из этого утверждения он сделал вывод о необходимости радикальной (революционной) перестройки этого общества. Это прямое нарушение логики. Если оператор не знает системы, он просто не имеет права ее «перестраивать», ибо это неминуемо кончится катастрофой. Логичным следствием утверждения Горбачева мог бы быть только призыв к срочному изучению нашего общества.»

При атаке на логику используются все приёмы софистики, но наиболее эксплуатируемый - «предвосхищение основания» (лат. *retitio principii*). Этот приём заключается в том, что в качестве аргументов используются недоказанные, как правило, произвольно взятые положения: ссылаются на слухи, на чьи-то мнения, высказанные кем-то предположения или даже на собственный вымысел, выдавая их за аргументы, якобы обосновывающие тезис. В действительности же доброкачественность таких доводов лишь предвосхищается, но не устанавливается с несомненностью.

Обычно подобные лже-аргументы сопровождаются фразами: «Как абсолютно всем известно...», «Кто же будет спорить с тем, что...», «Аксиомой, не требующей доказательств, является то, что...», «Само собой разумеется, что...», «Каждому известно, что...», дабы рассеять возможные сомнения у простого слушателя.

О приёмах софистики и противодействия ей написано огромное число материалов, где вы и можете почерпнуть обширные, дополнительные знания. Например, Ахманов А. С. "Логическое учение Аристотеля", Брутян Г. "Паралогизм, софизм и парадокс", Лисанюк Е.Н. "Софистика – это не аргументация". Эстеты могут начать с трудов самого Аристотеля.

Эмоции

Эмоции по своей сути это самая простая и самая древняя сигнализационная система в организме человека. Еда, сон, хорошее жилище и т.п. вызывают позитивные эмоции, которые подталкивают человека к действиям, направленным на обладание ими. Эта сигнальная система прямо влияет на наши действия. Когда нам страшно мы хотим спрятаться, когда нам неприятно мы хотим отвернуться... И любое рациональное мышление отходит на вторые роли.

Именно поэтому при воздействии сильных эмоций человек поступает вовсе не так, как в нейтральном состоянии. Вспомните про состояние аффекта и состояние эйфории. Это крайнее проявление негативных и позитивных эмоций. И в таких состояниях человек

совершает то, что в обычном своем состоянии не совершил-бы. Именно поэтому манипуляторы так активно эксплуатируют эмоции.

Воображение

В случае воздействия на наше воображение манипулятор подталкивает нас к тому, чтобы мы спрогнозировали своё будущее в позитивном или негативном свете, что и подталкивает нас к действиям по достижению такого будущего или его избеганию. Почти вся реклама построена на этом: заставить мечтать о чем-то. Например, об успехе у противоположного пола, или заставить бояться потери этого успеха из-за запаха изо рта... Мечта — это виртуальная реальность, созданная нашим сознанием и доступная только нам. Когда мечту вкладывают в нашу голову извне промышленным способом (реклама), то тем самым хотят подтолкнуть ЦА к совершению нужного манипулятору действия.

Манипулятор использует этот механизм для того, чтобы подтолкнуть жертву к нужным действиям. Например, что-то получить в собственность или получить доступ к какой-то информации. Мечта — это виртуальная реальность, созданная нашим сознанием и доступная только нам. Когда мечту вкладывают в нашу голову извне промышленным способом (реклама), то тем самым хотят подтолкнуть ЦА к массовым действиям. И тут используются все доступные технологии от прямого воздействия (реклама) до кино, литературы, искусства (product placement). На этом эффекте построен целый пласт манипулятивных технологий.

Внимание

При воздействии на внимание аудитории манипулятор старается отвлечь аудиторию от нежелательного события, чтобы не видели, не задавали лишние вопросы, не совершали нежелательные действия (например, не отказывались от продукции определенного бренда).

Или, наоборот, привлечь внимание аудитории к чему-то важному для манипулятора. К бренду, к конкретному продукту, к определенному свойству продукта и т.п..

Память

В этом случае манипулятор воздействует на нашу память. Его задача сделать так, чтобы аудитория забыла какой-то факт. Не упоминают в новостях, не пишут в публикациях, не делают отсылок в выступлениях. В результате сущность выпадает вначале из общественного дискурса, а затем и из памяти. Иногда это имеет обратный эффект. Помните фразу «тот, чьё имя нельзя называть»? Или, наоборот, помнила и не забывала, для чего аудитории регулярно напоминать об этом. Для этого в каждом новостном выпуске, в каждой публикации прямо упоминают или делают отсылку, чем стимулируют нашу память и не дают забыть.

Выявление дезинформации

Выявление дезинформации — это сложный процесс, требующий усидчивости и внимательности. Организовать автоматическую проверку фактов в сообщении на данном технологическом уровне развития не получится по ряду причин:

1 Нет непрерывно и быстро пополняемого реестра всех достоверных фактов, с которым сравнивать получаемую информацию. Попыток создать такой механизм много, только вот все они носят очень локальный характер и формируются фактически вручную. Одна из самых известных попыток создать такой реестр проверенной информации — это Википедия, но после череды скандалов называемых «войной правок» стало понятно, что претендовать на истину в последней инстанции этот проект не может.

2 Другая сложность заключается в том, что каждое сообщение содержит больше одного утверждения, претендующего на звание факта, а значит и подвергать проверке нужно все. И не понятно какое из утверждений ключевое, а какое нет.

Например, сообщение «Вовина мама мыла оконную раму в своей квартире на 10-м этаже» содержит следующие утверждения:

1. У Вовы есть мама
2. Мама Вовы мыла оконную раму
3. У Вовиной мамы есть квартира
4. В квартире есть как минимум одно окно
5. Их квартира находится на 10-м этаже

И что из этого важно, а что нет, что проверять, а что не нужно, как это проверять непонятно.

3 Дезинформацией может быть ложная информация, а может быть вполне достоверная, но подаваемая особым способом, ведь цель манипулятора — это подтолкнуть аудиторию к нужным действиям. А достичь этого можно разными способами, например вызвав эмоции у аудитории, но вовсе не обманывая. Поэтому наличие обмана не является достаточным признаком для отнесения сообщения к дезинформации. Нужен другой признак, и он вроде как на поверхности — наличие манипулирования аудиторией в сообщении. Но и тут все не просто. Строго говоря, любой акт общения это в той или иной мере манипулирование, а значит в любом сообщении присутствует элемент манипулирования. И возникает вопрос — а где та граница, до которой это не дезинформация, а после которой уже точно дезинформация?

История методов проверки информации и их эволюция демонстрирует, как изменялись подходы к верификации данных с течением времени.

Ранние подходы

В XIX веке, с ростом сенсационной журналистики, возникла необходимость в более точной проверке фактов. Примером является создание Associated Press в 1850-х годах, ориентированной на краткие и фактические материалы. В начале XX века, такие

инициативы, как «Бюро точности и честной игры» Ральфа Пулицера из New York World, начали формировать стандарты для проверки фактов.

Середина XX века

Журнал Time и газета The New Yorker внедрили отделы проверки фактов, что стало важным шагом в институционализации этого процесса.

Начало XXI века

В начале 2000-х годов в США появились «независимые» организации, занимающиеся постфактумной проверкой фактов, такие как FactCheck.org и PolitiFact.

Но увы, на практике ничего фундаментально не изменилось. Общих правил выявления дезинформации всего два:

1. перепроверка самих данных;
2. контроль источника этих данных и канала поступления информации.

Перепроверка данных подразумевает наличие нескольких, независимых друг от друга или от чего-то общего, источников. И соответственно сопоставление поступающих от них сведений. Такое сопоставление может быть полным, когда все источники дают развернутую информацию по одной проблеме. Или частичное сопоставление, когда информация из каждого источника лишь частично дублирует остальных.

Контроль надежности источника и канала передачи информации подразумевает:

1. постоянный контроль достоверности поставляемых сведений из источника и по каналу;
2. учет и разбор всех допущенных огрехов;
3. контроль «близости» источника к добытой информации.

Начать проверку поступающей информации на наличие дезы можно с простых действий. По поводу проверяемой информации задайте себе несколько вопросов:

1. Возможно ли перепроверить источник? Указан ли источник информации? Можно ли проверить источник информации? Даже если источник указан – действительно ли он существует? Если источник указан, но найти вы его не можете, это тоже может быть признаком дезы.
2. Есть ли попытка вызвать эмоции? Есть ли в сообщении эмоциональная составляющая? Если есть – на сколько сильно она цепляет? Возможно, она специально включена, чтобы "зацепить"? Что-то, что касается личной безопасности, денег, здоровья, конкретно вас, вашей семьи, детей или домашних животных. В зависимости от аудитории это может быть отсылка к несправедливости или к зависти. Вместо конкретики и рациональных доводов, в фейках и пропагандистских новостях часто содержится множество эмоционально окрашенных слов — они провоцируют у читателя сильную реакцию, например, злость или страх.

3. Насколько тема новости актуальна? Актуальность может быть общей или под определенную ЦА. Например, отмена пенсий, продажа ценных рыбопродуктов японцам, поджоги с целью скрыть незаконные вырубki леса и т.д. Если тема уж очень на злобу дня, есть повод насторожиться.
4. Есть ли в новости так называемая "достоверная мелочь"? Что-то очень правдоподобное, создающее у вас иллюзию, будто вы имеете дело с реальными фактами. Например, адрес, или имя некоего эксперта, или отсылка к недавнему и реальному событию и т.п.
5. Если в сообщении есть призыв к распространению – насторожитесь. Такой призыв может быть явным «Разошли, сделай репост, отнесись серьезно, расскажи тем, кого ты действительно любишь...». Или не явным «Позаботьтесь о своих близких...», «Помоги себе и своим родным». Как правило, это характерно для фейков, распространяемых через личную переписку, соцсети и мессенджеры.

Если речь о новостях в интернете, то чаще всего мы вынуждены не «выявлять дезинформацию», а оценивать степень доверия к поступающей информации. То есть мы имеем возможности сказать, что перед нами (правда или ложь). Но у нас есть возможность оценить на сколько мы можем доверять этой информации. Вот ряд рекомендаций для такой оценки.

Обращайте внимание на заголовки: ложные новости часто имеют броские заголовки. Если шокирующее заглавие статьи кажется вам неправдоподобным, скорее всего, так оно и есть. Сплошные заглавные буквы и несколько восклицательных знаков так-же являются признаком наличия манипулирующей информации.

Смотрите на адрес сайта - он тоже может указать на обман. Сайты, специализирующиеся на дезе, часто имитируют подлинные новостные источники, повторяя их адреса с незначительными изменениями. Зайдите на сайт уважаемого источника и сравните адреса.

Исследуйте источник. Убедитесь, что история написана источником, которому вы доверяете и имеет репутацию достоверного. Если история исходит от незнакомой организации, загляните в раздел «О нас», чтобы узнать больше.

Обращайте внимание на правописание: часто сайты фейковых новостей грешат орфографическими ошибками. Это результат спешки и плохого образования авторов фейков.

Обратите внимание на необычное форматирование. Многие сайты с ложными новостями грешат странной структурой. Если видите подобное – отнеситесь к сайту с подозрением.

Деза часто сопровождается поддельными изображениями или видео. Иногда фотография подлинная, но вырвана из контекста. Желательно установить источник фото или видео. Это можно сделать через поиск по фото в Яндексe или Гугле, или в специализированных сервисах.

Изучите даты: ложные новости могут ссылаться на реальные события, но не соответствовать их времени. Произошло раньше, чем надо или не в то время, что указано в проверяемой новости.

Сопоставьте информацию с данными из других источников. Если сообщение не встречается более нигде в новостях, возможно, оно ложное. Если сюжет повторен многими источниками, которым вы доверяете, то больше шансов, что это правда.

Проверьте доказательства. Проверьте автора, чтобы убедиться в достоверности. Отсутствие доказательств или доверие к неназванным экспертам могут указывать на ложную новость. Посмотрите другие отчеты. Если ни один другой источник новостей не сообщает о той же новости, это указывает на то, она ложная. Если об этой новости сообщается из нескольких источников, которым вы доверяете, она с большей вероятностью окажется правдой.

Не шуточная ли это новость? Иногда ложные новости сложно отличить от юмора или сатиры. Проверьте, не известен ли источник как пародийный, и не подразумевают ли детали и тон новости, что она написана просто для смеха. Некоторые новости намеренно ложны. Критически относитесь к новостям, которые вы читаете, и делитесь только теми, которые, по вашему мнению, заслуживают доверия.

Как создать эффективную систему OSINT

А теперь несколько слов о том, с чего начать на практике, особенно если нет опыта создания системы OSINT и недостаточно знаний в этой области, но создать нужно.

Каждая компания по-своему приходит к пониманию необходимости OSINT. Кто-то через возникшие проблемы, кто-то через упущенные возможности, кто-то через понимание перспектив, кто-то через модную тенденцию... Но так или иначе решение о создании принимается, выбирается ответственный за направление. И далее ему нужно начинать работу. Хорошо если подобрали настоящего специалиста OSINT, но таких пока еще крайне мало. А по тому, скорее всего, на направление поставят человека без соответствующей подготовки или знаний. И ему с чего-то нужно начать.

OSINT по своей сути это эффективная работа со специфической информацией на специфических источниках. Если совсем обобщенно это переработка большого количества информации о свойствах и действиях интересующих объектов и создание на их основе описаний, прогнозов, рекомендаций и еще одного специфического продукта для активных мероприятий – информации воздействия (или влияния) и каналов ее доставки объекту. Но начнем с простого – с пассивных мероприятий, а именно со сбора информации, ее обработки и представления заказчику.

Понять потребности компании в информации

Для начала нужно понять какая информация нужна сотрудникам разного уровня компании от стратегов до исполнителей для принятия ими решений по своей работе. Определиться с этим можно несколькими способами:

1. размышляя самому;
2. спрашивая у тех самых потребителей информации.

Начать лучше именно с размышлений. Это позволит разобраться в ситуации не приставая к сотрудникам и не раздражая их заранее своими вопросами.

Такие размышления удобнее вести отталкиваясь от целей, стоящих перед потребителями информации. Но для начала определитесь со стратегией компании. Иными словами, попробуйте понять какая информация нужна руководству компании для ежедневной

работы. Ответы на какие вопросы им нужны для принятия решений на своём уровне. Если перефразировать, то вам нужно понять, информация, о чем может быть полезна руководству. В самом общем виде это информация о факторах, оказывающих или могущих оказать существенное влияние на компанию. Причем как в позитивном, так и в негативном направлении. Сюда относятся и действия клиентов и действия конкурентов, и поставщиков, и регуляторов (госструктур) и тех, кто разрабатывает новые технологии... Эта тема очень хорошо проработана в маркетинге.

После составления списка (схемы) для себя и структурирования своего представления об информационных потребностях компании можно переходить к опросу сотрудников. Повторюсь – делать это нужно осторожно. Попробуйте начать с маркетологов – они также работают с информацией о силах, действующих на рынке. Затем пообщайтесь с PRщиками, затем с «продавцами» продукта.

Но всё это лишь подготовка к основному разговору. Вам нужен кто-то из «стратегов» компании. Кто то, кто участвует в разработке стратегии компании.

Подобрать источники

Но не вся информация об участниках рынка нужна руководству. Чаще всего им нужна информация о ресурсах и планах основных сил, действующих на рынке. Именно зная ресурсы и планы можно спрогнозировать ближайшие действия и ответную реакцию на ваши действия. Поэтому сконцентрируйтесь именно на этих аспектах. При этом о ресурсах можно как-то составить представление и отслеживать изменения. А вот понять планы объекта интереса бывает весьма сложно. Здесь необходимо использовать косвенные признаки и оговорки ТОПов объекта.

Косвенные признаки — это события, действия, изменения, которые обязательно сопровождают значимые процессы в организации. Например, запуск новой технологической линии требует специалистов соответствующей квалификации, которых служба персонала будет искать. И эту активность можно вовремя обнаружить. Также возможно понадобятся новые площади, которые будут подыскивать (опять соответствующая активность) или строить (а здесь своя специфическая активность).

Оговорки ТОПов — это не осторожные высказывания ведущих специалистов объекта или руководства в интервью, на выставках и конференциях, в блогах или твиттере. Такие высказывания могут указать на косвенный признак, например поиск сотрудника с уникальной квалификацией или же может указывать прямо на планы в той или иной области.

Исходя из этих рассуждений и нужно подобрать источники информации. К таковым точно можно отнести сайты соответствующих компаний и отраслевые источники, официальные и частные блоги ТОПов и ведущих специалистов компании, официальные и не официальные форумы компании.

Как выбрать нужные источники в инете

Частично вы уже определились с рядом источников - с такими как сайты компании и сайты ее сотрудников. Куда сложнее обстоит дело с новостными ресурсами. Если таковых не много, то можно задействовать все имеющиеся, но чаще всего новостных источников

много и объемы информации превышают все мыслимые размеры. В этом случае нужно выбрать наиболее ценные. Ценность здесь зависит от того насколько релевантную вашим потребностям информацию он приносит, насколько свежую и насколько соответствующую действительности. Всё как в жизни □ Способов понять это два.

Первый – статистический – он подразумевает наблюдение за этим источником с подсчетом сколько он принес, сколько из этого оказалось «в тему», сколько пропустил и сколько раз «обманул». Да – да нельзя забывать и про дезинформацию умышленную или не умышленную. И по сочетанию этих показателей можно сделать вывод какие из источников вам более пригодны. Из известных мне программ такой инструмент определения эффективности источника есть только у СайтСпутника в разделе «Статистика».

Второй – «умозрительный» - нужно оценить насколько «близок» источник к вашей проблематике. Такая оценка может строиться на разных показателях. Например, на «территориальном» признаке. Если объект интереса — это производственное предприятие в регионе, то скорее всего местный сайт, посвященный этому производству, будет поставлять достаточно эксклюзивную информацию. Или на «конфликтном» признаке – площадка оппонента вашего объекта будет освещать каждый его промах, правда в этом случае необходимо делать «поправку на веее».

Что сделать в первую очередь

После того, как вы начали понимать какая именно информация полезна, нужно организовать ее сбор. Источники такой информации есть внутри компании и во вне. Но не спешите задействовать внутренние источники – начните с внешних и не затратных. С того же интернета. Такой подход позволит отшлифовать систему, вникнуть в проблематику и при этом не надоест коллегам и не потратить деньги в пустую.

Создать общую новостную систему

После получения и обработки информации результат работы нужно использовать. А использовать его можно только для принятия решений. Т.е. результат вашей работы нужно отдать тем, кто будет принимать решения основываясь на этих результатах. Но не «всем отдать всё», а только то, что нужно тому или иному потребителю информации. Если он (потребитель) получит только нужную ему информацию, а не «поток данных», то он не потратит лишнее время на чтение и с высокой вероятностью захочет еще получать подобную информацию.

Поэтому систему информирования также нужно тщательно продумать. А «обкатывать» ее нужно вновь с отдельных сотрудников нижнего уровня управления. Так вы отточите систему и сделаете меньше ошибок при подключении к ней «стратегов».

Первая часть такой системы – общая. Это все значимые для компании новости в виде «новостной ленты». Можно это делать рассылкой, но удобнее на специализированном ресурсе в сети, куда может зайти любой авторизованный пользователь в любой момент времени и из любой точки доступа к интернету. Такое решение сделает систему мобильной, удобной и гибкой, что несомненно скажется на оценке ее эффективности потребителями информации.

Вторая часть системы – персонализированные новости. Здесь нужно настроить «фильтры», которые позволят делать «видимыми» или активными только те новости, которые нужны каждому конкретному пользователю.

Создать профили конкурентов

Еще один элемент системы информирования потребителей информации — это библиотека структурированной информации по ключевым объектам рынка (досье). Это не обязательно конкуренты – это могут быть и ключевые клиенты, и поставщики, и разработчики, и регуляторы... Все зависит от каждой конкретной ситуации.

Для организации такого каталога поступающую информацию нужно не просто раскладывать в соответствующие папки (Профили), но и внутри структурировать так, чтобы это было удобно просматривать. Накапливать таким образом нужно по началу всю информацию, а в последствии значимую. «Значимая» информация в данном контексте это ее способность пролить свет на определенные стороны объекта. Обычно такой «стороной» объекта бывает знание о его ресурсах и планах. Да – да – история повторяется. Ресурсы это как материальные ресурсы (финансы, основные средства, товар в обороте и т.п.), так и не материальные (административный ресурс или криминальный...).

Такой «накопитель» информации постепенно станет сосредоточением ключевых данных по объектам интереса. Если таковых не много, то вероятно ее «популярность» будет не значительной. А вот если их много, то обращаться к ней будут часто, а через какое-то время начнут требовать от вас регулярного пополнения ее актуальной информацией.

СБОР ИНФОРМАЦИИ

Когда возникает необходимость запустить «OSINT конвейер», то встает ряд вопросов организационного, технического и технологического характера. И что интересно, пока мы занимаемся анализом в одиночку, мы об этом не задумываемся. А как только начинаем работать в команде, тут-же проявляются сложности, связанные с координацией действий, исключением дублирования функций и т.п..

Ошибки

Для начала разберем основные ошибки, которые обычно совершают начинающие OSINT-исследователи, и которые вы не допустите так-как предупреждены о них.

Отсутствие системного подхода

Это синтетическая ошибка, включающая в себя и неумение четко формулировать цели, периодическое забывание зачем проводится исследование и как следствие метания и распыление сил. Неправильная организация работы, отсутствие четкой стратегии и плана могут привести к пропуску важных данных и некорректному результату, и неэффективному использованию времени – слишком долго.

Пренебрежение документированием расследования

Отсутствие документирования процесса сбора данных, как минимум фиксации ссылок на первоисточники и скриншотов страниц, делает исследование менее убедительным, затрудняет проверку результатов исследования и повторный анализ в случае появления новых обстоятельств.

Использование непроверенных источников

Доверие слухам или недостоверным источникам может сделать результаты работы откровенной дезинформацией. Поэтому крайне важно использовать надежные источники, перепроверять данные, а в случае использования источников с неизвестной надежностью – прямо указывать это.

Ошибки в интерпретации данных

Неправильное толкование информации может привести к неверным выводам. Это часто происходит из-за недостатка контекста, предвзятости в анализе, отсутствия опыта и знаний предметной области.

Зависимость от одного инструмента или методики

В случае, когда выводы сделаны на основании одного источника вы становитесь заложником этого источника и рискуете дать заказчику дезинформацию. Нужно как минимум перепроверить информацию. Хотя-бы по косвенным признакам.

Сбор избыточной информации

Как это не странно, но чрезмерное дублирование информации также приводит к неприятным последствиям. Как минимум неоправданные затраты своего времени, а также злоупотребление временем постановщика задачи, который будет вынужден тратить много времени.

Организация сбора информации

Сбор сырья для аналитической деятельности настолько тесно переплетен с анализом этой информации, что рассматривать эти два процесса в отрыве друг от друга нельзя. Да и сбором занимаются и аналитики тоже для первичной оценки ситуации, для оперативного получения дополнительных данных, для последующего уточнения, для дополнительных исследований и для разных срочных задач.

Источники информации

Не забываем, что источники информации в OSINT исследованиях должны отвечать основным критериям открытых: общедоступность и не противозаконность. Сейчас наблюдается тенденция сужения направлений разведки с ориентированием на специфические источники информации (GeoINT, HumINT, SigINT и тд). Но изначально это всё одна дисциплина.

СМИ

СМИ в их традиционном виде – как мы привыкли их себе представлять. При таком подходе к средствам массовой информации следует отнести все периодические издания, телевиденье, радиовещание. По большому счету и Интернет такое же средство массовой информации, но в силу специфических особенностей его стоит рассмотреть отдельно.

В мире огромное количество самых разнообразных изданий. Все они имеют свои особенности. Но всех их объединяет то, что они имеют бумажную основу. Эта их особенность является причиной определенных свойств:

1. некоторая задержка в подаче информации вызванная необходимостью редактирования материала, печати и распространения;
2. наличие типографии или договоренность с таковой.

Безусловно, удобнее получать информацию с листа – это привычнее, с таким носителем можно поработать (что-то пометить и т.п.), но именно бумажный носитель делает данную группу СМИ менее поворотливыми. Поэтому, в настоящее время, данный тип СМИ ориентируется не столько на подачу оперативной информации, сколько на аналитику, рассуждения и т.п.. Хотя и новости в них присутствуют, но с задержкой необходимой для издания и распространения. С этой точки зрения необходимо оценивать периодические издания и определять их нишу в вашем информационном портфеле.

Радио и телевиденье можно рассматривать вместе поскольку их общая черта и основная особенность — это донесение информации до конечного пользователя посредством электромагнитных колебаний. Эта особенность соответствующим образом отражается на их свойствах:

1. задержка в передаче информации может быть сведена к минимуму;
2. необходимо наличие передающей аппаратуры или ее аренда;
3. у аудитории должна быть приемная аппаратура.

Но и работать с данным источником несколько труднее – необходимо фиксировать полученные данные и переводить их в удобоваримый для компьютера вид, в такой вид с которым в последствии будет удобно работать (искать, цитировать, объединять и т.п.). А это исключительно текст. Поэтому за оперативность получения приходится платить дополнительными затратами на перекодировку. Хотя, необходимо отметить, что многие центральные каналы и станции имеют свои сайты, на которых выкладывается необходимый материал, а иногда с минимальной задержкой, а то и в реальном времени.

Документ

Массу нужной информации можно найти в документах. Причем информации из документов мы верим больше, чем иной. А как же еще? Ведь информация в документе имеет некое юридическое подтверждение, некий официальный статус.

В нашем случае документ это материальный носитель информации, зафиксированной вне памяти человека. В соответствии с ГОСТ 16487 - 70 «документ» является средством «закрепления различным способом на специальном материале сведений о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека». В свою очередь, ГОСТ 7.60-2003 понимает под документом «зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать». С юридической точки зрения документ [juridical (legal) document] – это средство закрепления сведений, оформленное в соответствии с действующим юридическим законодательством и имеющее правовое значение.

Обращаю ваше внимание на то, что документ должен быть оформлен в соответствии с законодательством, а значит иметь соответствующие реквизиты (печать и подпись, возможно еще что-то). Только в этом случае он тянет за собой необходимые правовые последствия.

Предметно-вещественная среда

Это то, что нас окружает. Мир вокруг нас без людей, документов и интернета. Та материальная среда, в которой мы живем. Составляющие этой среды также являются носителями информации и порой весьма ценной. Например, опытный образец продукции конкурента сам по себе уже может многое рассказать.

Мероприятия

Конференции, выставки, круглые столы, слёты, семинары, симпозиумы и подобные мероприятия тоже являются источником полезной информации. Работа на них требует особых знаний и опыта. Тем ни менее, посещая такие мероприятия вы можете узнать свежую информацию, завести нужные знакомства в интересующей вас среде.

Базы данных

Данный источник нельзя отнести к внешним или внутренним. Он может быть и тем и другим – либо вы используете свою базу данных (собственного производства или приобретенную) либо получаете временный доступ к чьей-то базе. А работа с базами данных требует специфических навыков, выходящих далеко за пределы «вставить в поисковую строку фразу и получить результат». Поэтому рассмотрим этот вопрос отдельно.

Интернет

Все сайты интернета, куда вы можете попасть свободно, либо залогинившись, либо оплатив вход, являются для вас источниками информации. И это значительно больше, чем соцсети, форумы и блоги.

По сути своей Интернет и есть хранилище информации, эдакая огромная распределенная база данных. У этой огромной инфраструктуры есть свои особенности, которые необходимо учитывать при реализации своих исследований.

Особенности Интернет, как хранилища информации:

1. Интернет — это распределенное хранилище информации, то есть информация разнесена по разным хранилищам в том числе и физически;
2. Только часть, причем меньшая часть информации, выложенной в Интернет, индексируется известными вам поисковыми сервисами (Яндекс, Google и др);
3. В индексы поисковых сервисов информация попадает далеко не сразу, а с некоторой задержкой, что связано с необходимостью содержать большую парсинговую инфраструктуру;
4. Разные поисковые сервисы покрывают («видят») разные части Интернета;
5. Алгоритм работы разных поисковых сервисов разный.

Та информация, что выложена на общедоступном сайте, доступна и поисковым роботам и видна любому посетителю этого сайта. Именно эту информацию мы видим, когда вводим запрос в поисковый сервер и затем просматриваем результат. Сложнее обстоит дело с общедоступной информацией, находящейся не на сайте, а на отдельном сервере (например, в базе данных). Эту информацию поисковик не видит и соответственно не выдаст по вашему запросу, хотя она и общедоступна. И совсем недоступна информация, находящаяся в закрытых зонах, например за паролем.

Интернет это не что-то эфирное или облачное, а вполне себе материальная инфраструктура, пусть и очень сложная, и разветвленная. И у этой инфраструктуры есть свои особенности, понимание которых позволяет эффективнее работать с информацией.

Инфа в интернете всегда имеет конкретный носитель (HDD, SSD, оперативная память, ленточные, оптические и иные накопители, на котором она хранится или канал передачи информации (медь, оптика, радио во всех вариациях), по которому в данный момент передается.

Человек

Люди являются очень важным источником информации, но требующим специфических технологий получения информации. Именно по этой причине данное направление выделилось в HumINT.

Эксперты и консультанты

Весьма интересные сведения можно найти в неопубликованных источниках вне компании. Эти сведения всплывают на поверхность в ходе общения с экспертами, клиентами, заказчиками, поставщиками, журналистами или другими людьми сведущими в интересующей вас области. Но надо помнить, что данные источники вторичны. Ведь они черпают свои знания не из первоисточника, а если и из первоисточника, то мы этого не можем знать наверняка.

Процесс работы с людьми вне компании требует определенной самоотдачи и должен проводиться активно на постоянной основе. Вначале нужно согласиться с тем, что источниками информации для вас являются такие же люди, а соответственно у них есть свои потребности, свои желания, свои взгляды и т.п.. Поэтому и работать с ними нужно так, чтобы у них после общения с вами осталось благоприятное впечатление и желание еще пообщаться именно с вами. Это достаточно сложно и требует определенных усилий, но и результат получается значительный. Прежде чем начинать работу с людьми по сбору нужной вам информации необходимо для себя ответить на ряд вопросов:

1. с кем можно продуктивно поговорить на эту тему (кто может быть достаточно осведомлен в данном вопросе)?
2. что мне у него спросить (о чем спросить)?
3. как спросить (как сформулировать или в какую форму облечь свои вопросы)?
4. как можно подвести к разговору на интересующую тему?

5. как я смогу обработать полученную информацию (идентифицировать как факт, а не слух, систематизировать и сопоставить)?

Изначально включите в свой список всех знающих людей вашей по вашей теме, с которыми вы хотите регулярно контактировать. Этот перечень постепенно будет расти по мере того, как вы будете его обрабатывать. Ведь в процессе общения будут появляться новые контакты, ранее вам не известные. Не забывайте фиксировать дни рождения людей, их профессиональные праздники, вообще значимые для них даты и поздравлять их. Эти простые знаки внимания создают необходимую атмосферу стабильности и доверия, которые так необходимы для откровенного разговора.

Телефонный разговор – один из наиболее оптимальных методов для сбора неявной информации из внешних источников. Он не требует много времени, достаточно гибок и, недорог. Если проявить терпение и настойчивость вы можете пообщаться с достаточно большим числом людей в короткий промежуток времени. Проанализировав полученные таким образом данные, помогут быстро определить, сколько еще дополнительной информации вам требуется, где ее можно найти, кто поможет вам в этом. Когда в ходе телефонного разговора выявляется новый источник, то вы можете незамедлительно вступить с ним в контакт, сославшись на предыдущий телефонный разговор. Но есть одно ограничение – когда вы общаетесь по телефону не стоит задавать новому знакомому достаточно сложные вопросы – ограничьтесь несколькими простыми и уместными вопросами. В этом случае вы с большей вероятностью получите результат. Очень подробно технологию использования телефона для получения в том числе и закрытой информации рассказал в своих работах «Искусство обмана» и «Искусство вторжения» Кевин Митник. Социальная инженерия (а это именно она) стала в свое время для него фактически искусством.

Оптимальная стратегия для сбора информации посредством обзвона, по мнению Кевина Митника заключается в следующем:

1. В первую очередь переговорите с известными вам людьми, либо с людьми чьи координаты есть в открытом доступе. У них вы получите исходные данные и дополнительные контакты. А после того как сориентируетесь в проблеме вам станет проще строить беседу с незнакомыми людьми и правильно формулировать вопросы.

2. Получите данные из мест концентрации информации:

- справочные службы;
- отдел продаж;
- центры послепродажного/гарантийного обслуживания;
- лица, ответственные по связям с общественностью / инвесторами.

3. Попробуйте переговорить с высшими должностными лицами в организации, как-то: с генеральным директором или другими членами высшего управления. Эти люди часто изъявляют желание говорить. Их график включает в себя общение с аналитиками, средствами массовой информации, местными общественными деятелями и другими посторонними лицами. Высшие управленцы, обычно, очень разговорчивые люди и они очень гордятся организацией, в которой работают. Вопрос только в правдоподобном и весомом поводе для разговора с ними.

4. Управленцы среднего звена трудны для общения. Эта группа персонала включает в себя продакт-менеджеров (менеджеров по определенному виду продукции), менеджеров по маркетингу, менеджеров по планированию и тому подобное. Как правило, они не будут с вами разговаривать. Достаточно интересно, что эти личности часто не делятся информацией с другими людьми и в своих собственных компаниях. Если вам обязательно надо найти подход к среднему звену управления, имейте под рукой ответы, которые Вы уже получили предварительно. Используйте управленцев среднего звена, прежде всего, для подтверждения или опровержения ваших предположений.

Не забывайте точно фиксировать полученную информации, неплохо пользоваться диктофоном. Позднее возникнет необходимость ее классифицировать и сравнить с другими данными. Важно, что бы не потерялся ни один элемент. С самых первых шагов заведите правило фиксировать всю поступающую к вам информацию.

Сбор информации из баз данных

До начала работы с базой данных полезно ознакомиться с ее структурой. Важно понять какие поля есть, в каком формате вносятся данные в те или иные поля, как связаны между собой разные таблицы одной базы. Помните, что поиск можно вести по содержимому любого поля базы. Так в телефонно-адресном справочнике по номеру телефона можно установить кому этот номер принадлежит и где географически установлен. Но не стоит на этом останавливаться. Ведь можно посмотреть кто еще проживает по этому адресу, и кто еще использует тот же номер в качестве контактного. А также – какие телефоны есть у выявленного человека или организации. Обычно называют это «обратным поиском» — это когда найденную в базе информацию вы используете для поиска «что или кто еще с этой информацией связан».

Работа с базами данных ГАИ, адресными и телефонными справочниками, базами статистической и регистрационной информации — дело довольно сложное. Учиться этому искусству приходится долго, опыт накапливается очень медленно. Рассмотрим ситуацию, когда вам просто указали на некую фирму, и нужно провести первое ознакомление с ней. Перед началом работы нужно четко понимать, что нет ни одной организации, у которой не было бы разветвленных связей. Любая организация создается для какой-то деятельности или для имитации этой деятельности. А коммерческая организация не просто для деятельности, а для получения прибыли. Ну а получение прибыли невозможно без клиентуры, которая потребляет результат работы изучаемой организации. Вот вам и связи. И если эти связи не выявлены, значит, плохо искали.

Для начала необходимо определиться с поисковыми признаками. Название организации это уже признак, правда не всегда уникальный, но тем ни менее. Как правило, название фирмы может служить толчком для дальнейших поисков. Так, если в нем встречается некоторый нераспространенный символ, вроде буквы греческого алфавита, или слово «газ», это уже может направить OSINT по нужному руслу дальнейших изысканий. Интерес представляет и юридический адрес компании, и ее телефон. Далее можно посмотреть какая собственность, зарегистрирована на данное предприятие и кому эта собственность принадлежала ранее. Далее нужно понять, с кем эта организация связана. Предположим в распоряжении у вас три базы данных: регистрационная палата, адресный и телефонный справочники. Первоначально нужно определиться: кто учредители компании, ее руководитель и главный бухгалтер. Полученный список фамилий «запускается» сразу по всем трем базам. База регистрационной палаты позволяет установить, в каких еще фирмах учредители выступают как учредители и руководители.

То же — относительно руководителей. С главными бухгалтерами ситуация не менее интересная — их ищут именно в этой функции по другим фирмам, а также в качестве руководителей и соучредителей.

По адресному справочнику идет добавление в поиск новых фамилий. Если некто проживает вместе с руководителем, учредителем или главным бухгалтером исследуемого предприятия — он обязательно должен быть включен в поиск, поскольку это явная связь. Ведь в российском бизнесе больше доверяют родственникам, особенно на начальном этапе.

Весьма интересные моменты несогласованности информации. Скажем, в данных регистрационной палаты указан телефон. Но по телефонному справочнику он принадлежит другой фирме, иногда это вообще квартирный телефон. Это — особо ценная информация. Каждое рассогласование информации, содержащейся в разных базах данных, должно радовать, а не огорчать. Оно — источник важных открытий, которые помогут пролить свет на сущность происходящего. Подобные нестыковки часто указывают на неявные либо скрываемые, либо на ранее существовавшие связи.

Уже на первом цикле полезно использование информации о местоположении компании-объекта исследования. Здесь также возможны полезные находки. Кому принадлежит данная территория, кто владеет зданием, кто еще находится в этом здании, какие организации зарегистрированы по данному адресу...

После такого – первичного изучения число вовлеченных в изучение лиц увеличилось. Каждый из новых объектов представляет отдельный интерес. Очень интересны их связи, которые ведут в тот же «первый круг» - к тем лицам и объектам, с которых началось изучение – к объектам вашего интереса. Если такое обнаруживается, то формируется особая группа тесно связанных между собой людей. С высокой долей вероятности можно утверждать, что это «костяк» изучаемой организации, и что их отношения были и ранее не менее тесными, и возможно где-то еще они совместно что-то организовывали. Все это рабочие гипотезы, требующие отдельной проработки. Поэтому стоит повнимательнее присмотреться к их предыдущей жизни и к тому, чем они занимались, с кем контактировали, с кем конфликтовали.

Также необходимо помнить, что информацию в эти самые базы вносят люди, а людям свойственно ошибаться. Ошибки могут быть самые разные от пропусков букв и их дублирования до сложных орфографических ошибок. Особенно стоит уделять внимание написанию имен собственных не славянского происхождения. Здесь вероятность ошибок выше всего. А уж если информация заносится «со слуха», то ошибки гарантированы. Поэтому при поиске стоит попробовать ввести слово как правильно написанное, так и с возможными ошибками. Да и государственные учреждения не блещут точностью данных. Взять ГИБДД с их системой присвоения названия цветам, в которые окрашены автомашины. Не посвященному человеку трудно понять какой цвет обозначен названиями «торнадо», «болотный танк», «золотое руно», «вальс», «цвет не установлен» ... О таких нюансах нужно помнить всегда.

Работа с людьми

Самую ценную и своевременную информацию могут предоставить только люди - люди, которые близки к источнику информации. Именно они, при правильном использовании, могут получить доступ к святой святых объекта вашего интереса. Фактически человек

может дать информацию о планируемых мероприятиях еще на этапе их планирования. Наиболее полно данная проблема освещена в работах Землянова В.М. и Ронина Р.. Здесь же я предлагаю краткий обзор основанный, в том числе, и на их публикациях.

Для начала нужно указать на то, что агентурной работой может заниматься строго ограниченный Законом круг лиц. Это отдельные сотрудники силовых ведомств. Остальным гражданам такая деятельность запрещена. Однако такая деятельность вполне может вестись против вас злоумышленником и, для эффективного противодействия, полезно знать как это происходит. Кроме того, знать, что это такое нужно для того, чтобы четко понимать, где проходит граница законности, чтобы не переступить ее и не подвергать ни себя, ни свою компанию дополнительному риску. Помимо этого, агентурная деятельность запрещена, но вовсе не запрещены дружеские отношения.

Побуждение человека делиться с вами полезной информацией

Подбор источника информации

Если вы определились с тем какую информацию хотите получить и иные способы получения искомых данных себя исчерпали, можно приступать к поиску кандидата для вербовки. Наиболее часто на кандидата обращают внимание в силу его личных качеств, близости к искомой информации, или исходя из стратегических планов. Подбор кандидатуры может происходить одним из двух методов:

1. определяется человек, обладающий необходимой информацией, или близкий к источнику информации, а затем ищутся подходы к нему;
2. очерчивается круг подходящих людей и из них выбирается наиболее пригодный для вербовки (наиболее уязвимый).

Человек не может существовать в вакууме, не контактируя с другими людьми. Рядом с ним всегда находятся другие люди. Действия человека всегда оставляют следы. Важно найти эти следы, собрать их и тщательно изучить. Это даст исходный материал для изучения намеченной кандидатуры. Исходные данные для подбора нужного человека можно также получить из:

1. его ближайшего окружения (родственники, друзья, коллеги...);
2. посредством прямого общения с кандидатом (под разными предлогами);
3. посредством наблюдения за его поведением в разных ситуациях (в т.ч. созданных искусственно...);
4. по опубликованным кандидатом статьям, письмам, докладам, по его интервью, выступлениям...

Выбирая кандидата для вербовки, обращают внимание на особенности человека, на то, что выделяет его из общей массы людей. Особое внимание нужно уделить изучению и анализу его неудач (маленьким и большим), политических взглядов (симпатиям и антипатиям), увлечений (особенно аморальным), национальных особенностей, финансово-имущественного положения, религиозности, его связей и т.п. На данном этапе можно наметить основные сценарии вербовки:

1. используя убеждения кандидата;
2. используя компромат;
3. используя чувства;
4. используя финансовую заинтересованность.

Проверка кандидата на роль источника

Предварительная проверка кандидата имеет целью более подробно изучить выбранного кандидата: его окружение, его поведение, его отношение к тем или иным фактам и событиям. Что бы точно определить движущие им мотивы и, соответственно, методы наиболее эффективного воздействия. Вначале нужно собрать сведения без непосредственного контакта с исследуемым. Наиболее используемыми источниками информации на данном этапе могут стать:

1. ближайшее окружение объекта интереса (коллеги, знакомые, родственники и т.п.);
2. документы (трудовая книжка, личное дело, медицинские карты, учетные карты и т.п.);
3. личная корреспонденция;
4. телефонные переговоры;
5. наружное наблюдение за объектом;
6. упоминания в прессе.

Чаще всего наиболее интересная информация добывается у лиц, контактирующих с объектом интереса. Именно люди, окружающие кандидата, могут рассказать много интересного о нем. Но при сборе таких данных необходимо помнить о том, что человек, рассказывая о чем то, привносит свое мнение – рассказчик интерпретирует данные по своему усмотрению, а значит изменяет первоначальный смысл. Иногда это делается умышленно, иногда неумышленно, но это происходит. Поэтому при анализе таких сведений необходимо учитывать следующее:

1. в какой степени рассказчик осведомлен об объекте, на сколько у них тесные отношения, на сколько объект ему доверяет;
2. какие отношения между объектом и вашим собеседником в настоящее время, какими они были ранее;
3. в какой степени свойство характера объекта, описываемое вашим собеседником, развито у самого собеседника (если свойство развито сильно – его оценки скорее занижены, если слабо – скорее завышены).

Если бесконтактный способ сбора данных исчерпал себя, а информации явно недостаточно – надо переходить к контактными методам сбора информации:

1. прямое общение и обсуждение тех или иных вопросов;

2. провоцирование (искусственное создание ситуации и наблюдение за поведением объекта);
3. просьбы и контроль их исполнения.

Организация первого контакта и его углубление

Первый контакт должен быть организован так, чтобы у объекта была абсолютная иллюзия случайности этого контакта. В противном случае объект может насторожиться и развития не получится. Ситуации, которые подходят для такого контакта, часто возникают сами и тут главное не упустить шанс, а в последствии правильно развить общение. Наиболее удобные варианты знакомства зависят от самого объекта: от его пола, возраста, профессии, привычек, увлечений, характера и т.п.. От его настроения, состояния здоровья, от погоды, от окружающей обстановки и еще от огромного количества факторов. Важное значение имеет ваш внешний вид, ваш стиль общения, ваше настроение. Наиболее используемые способы знакомства:

1. провоцирование объекта на оказание помощи;
2. оказание помощи объекту;
3. знакомство через общих знакомых;
4. знакомство на различных мероприятиях;
5. знакомство посредством хобби;
6. вызов интереса к себе;
7. через продажу или покупку чего-то.

Первый контакт имеет целью только знакомство. Поэтому при первом знакомстве можно лишь договориться о дальнейшем общении и не более того.

Далее необходимо создать поводы для поддержания контакта. Необходимо максимальное количество встреч (контактов) поскольку в результате вы сможете получить максимум необходимой информации об объекте и выше вероятность, что вы понравитесь объекту. Способы углубления контакта основаны на подигрывании объекту, на удовлетворении его потребностей особенно тех, которые ему затруднительно удовлетворить. Здесь можно сыграть на:

1. потребности в общении объекта;
2. потребность в сочувствии;
3. потребность в доминировании;
4. потребность в самоутверждении;
5. потребность в сотрудничестве.

Собственно убеждение делиться информацией

Для привлечения человека к сотрудничеству, необходимо максимально точно выявить его наиболее сильные мотивы. Когда точно знаешь, что человеку нужно и есть возможность ему это предложить или забрать – несложно стать его господином. А мотивами объекта могут быть:

1. месть;
2. тщеславие;
3. политические убеждения;
4. романтизм;
5. религиозные чувства;
6. властолюбие;
7. национализм;
8. высокое самомнение;
9. материальные затруднения;
10. любовь;
11. жадность;
12. страх;
13. сострадание;
14. пороки...

Привлечение к доверительному сотрудничеству можно осуществлять несколькими способами в зависимости от поставленных целей и особенностей самого объекта:

1. от своего имени;
2. от чужого имени;
3. от имени одного с последующей передачей другому;
4. без указания интересующейся стороны.

Помимо использования имеющихся у объекта мотивов не добросовестные люди могут прибегнуть к следующим методам:

1. убеждение;
2. шантаж;
3. угроза физической расправы;
4. зомбирование;

5. игра на эмоциях.

Связь с человеком, обладающим нужной вам информацией

Связь является достаточно уязвимым аспектом работы с людьми. Особенно, если обнаружение факта вашего взаимодействия может быть опасна для источника. Поэтому организации связи необходимо уделять особое внимание. Всегда нужно помнить, что по разным причинам существующий канал может быть нарушен, поэтому должен быть запасной вариант связи и не один. Помимо обычных (информационных) каналов необходимо иметь несколько сигнальных каналов. Их смысл заключается не в передаче значительных объемов информации, а в передаче одного единственного сигнала. Такой сигнал может означать разное от «готов к встрече» до «работаю под контролем». О таких каналах и о значении сигналов нужно договариваться заранее. Формы сигнальной связи зависят только от вашей фантазии и ограничены лишь тем, что должны выглядеть естественно и не вызывать у окружающих никакого интереса.

Обычная информационная связь может осуществляться следующими способами:

1. непосредственное общение;
2. техническая связь (телефон, радио, электронная почта...);
3. почтой;
4. подбрасыванием сообщений;
5. курьерами;
6. посредством тайников;
7. передачей при мимолетных контактах...

Прямое общение может происходить у общих знакомых, в местах общего пользования, на общественных мероприятиях... Только при подготовке такого контакта не забудьте подготовить и пути для экстренного ухода и убедительное и благопристойное объяснение того, что ваш источник с вами общается. По телефону возможно прямое общение, общение через аппарат – посредник, с использованием шифраторов. Хорошие возможности дают мобильные телефоны, купленные на подставных лиц. Только при этом нельзя забывать о возможности локализации мобильного телефона, иногда с точностью до десятка метров. Правда стоит сделать оговорку – локализация осуществляется в горизонтальной плоскости, а вот выявить высоту источника сигнала обычными средствами нельзя. При курьерской связи можно использовать постороннего курьера, или последовательность из нескольких курьеров. Почтовые отправления лучше делать из неожиданных мест или при помощи посторонних людей. Передачу информации через электронную почту нужно проводить из Интернет кафе, причем каждый раз из нового или с помощью мобильника оформленного на дядю Васю из Рио-Дэ-Жанейро. Лучше использовать несколько почтовых ящиков с последовательной переадресацией, а также шифрование данных.

Особенности вывода из операции

Целью консервации агента является нейтрализация возможных неприятностей от него. А как этого достичь зависит от особенностей самого агента. Один из наиболее используемых способов это объявление агенту, что в связи с его ценностью с одной стороны и опасностью ситуации с другой, принято решение на некоторое время его деятельность приостановить, а связь прервать. Но через какое-то время контакт будет возобновлен. Такое расставание имеет свои преимущества:

1. агент надеется на дальнейшее сотрудничество и не предпринимает нежелательных шагов;
2. агент, в случае необходимости, может быть возвращен в работу.

Но бывают ситуации, когда надежды на благоразумие агента нет. В таком случае важно как была организована работа с агентом. Если связь была бесконтактной (агент не имеет возможности самостоятельно выйти на вас) то контакт просто прерывается.

В зависимости от особенностей агента, и от видов на него в дальнейшем, заканчивать отношения с агентом можно:

1. учтиво;
2. грубо;
3. радикально.

Все зависит от ситуации и самого агента.

Поиск данных в интернете поисковыми сервисами

Инструменты для онлайн-расследований изменчивы. Они зависят от прихотей их владельцев, которые в любой момент могут сменить тип данных, выкладываемых в открытый доступ. Поэтому полагаться в расследованиях только на уже кем-то созданные – плохая идея. Но есть один островок относительной стабильности, который может пригодиться практически в любом исследовании: поиск глобальных поисковиков (Яндекс, Гугл...).

Поисковики

Поиск – это основа работы цифрового расследователя, поэтому нужно уметь пользоваться поисковыми сервисами так, чтобы выжимать из них максимум. А значит нужно уметь составлять запросы и использовать операторы для различных платформ. И тут нужно помнить, что поисковых сервисов сильно больше, чем Яндекс и Google. Вот только наиболее известные из них:

- Aol <http://search.aol.com>
- Ask <http://www.ask.com>
- Baidu <http://www.baidu.com>

- Bing <http://www.bing.com>
- DuckDuckGo <https://duckduckgo.com>
- entireweb <https://www.entireweb.com>
- Exalead <https://www.exalead.com/search>
- Gigablast <http://gigablast.com>
- Goodsearch <http://www.goodsearch.com>
- Google <http://www.google.com>
- Infospace <http://www.infospace.com>
- Lycos <http://www.lycos.com>
- MyWebSearch <http://home.mywebsearch.com>
- Naver <https://www.naver.com>
- Sogou <https://www.sogou.com>
- Soso <http://soso.com>
- Teoma <http://www.teoma.com>
- Wolfram Alpha <http://www.wolframalpha.com>
- Yahoo! Search <http://www.yahoo.com>
- Yandex <https://www.yandex.com>

Кроме этого, есть мета-поисковые системы, которые транслируют ваш запрос к двум или более поисковикам, собирают из них результаты, удаляют дублирование, чтобы вы не читали по несколько раз одно и то же и выдают вам список релевантных ссылок:

- 100SearchEngines <https://www.100searchengines.com>
- All-in-One <http://all-io.net>
- AllTheInternet <http://www.alltheinternet.com>
- Bing vs. Google <http://bvsg.org>
- Creafy <http://www.creafy.com>
- DADgogo <http://dadgogo.com>
- Dogpile <http://www.dogpile.com>
- Etools <http://www.etools.ch>
- Excite <https://www.excite.com>

- FaganFinder <https://www.faganfinder.com>
- Findwith.me <http://www.findwith.me>
- Info.com <http://www.info.com>
- iZito <http://www.izito.com>
- The Lookup <http://the-lookup.com>
- occusearch <https://occusearch.net>
- runnaroo <https://www.runnaroo.com>
- Search <https://www.search.com>
- Search <https://search-it.netlify.app>
- SearchAll <https://www.searchall.net>
- searchlino <https://www.searchlino.com>
- Search-it <https://search-it.netlify.app>
- SEARCHtify <https://www.searchtify.com>
- SonicRun <http://www.sonicrun.com>
- toki <https://toki.com>
- WebCrawler <http://www.webcrawler.com>
- weboasis <https://weboas.is>
- Zapmeta <http://www.zapmeta.com>
- ZUREU <http://zureau.com>

Но с мета-поисковиками есть одна сложность – из-за разницы поисковых алгоритмов в разных поисковиках и разнице в поддерживаемых операторах, сложные запросы обрабатываются не самым лучшим образом. Но вот работа по простым запросам значительно облегчается.

А есть специализированные поисковые сервисы, заточенные под определенную сферу или отрасль.

Поиск событий

- Evensi <https://www.evensi.com>
- Eventbrite <https://www.eventbrite.com>
- Meetup <https://www.meetup.com>
- Townscript <https://www.townscript.com>

- weezevent <https://weezevent.com>
- What up in town <https://whatupintown.com>
- WhereEvent <http://www.whereevent.com>
- Wikido <https://www.wikido.com>

Поиск по базам данных и каталогам

- Fonetask <http://fonetask.com>
- GIIT IT <http://giitit.com>
- Grayhat Warfare <https://buckets.grayhatwarfare.com>
- Lendx <http://lendx.org>
- OD Finder <https://odfinder.github.io>
- Open Directory Crawler <https://odcrawler.xyz>
- Open Directory Search <https://opendirsearch.abifog.com>
- Open Directory Search <https://open-directories.reecemercer.dev>
- Open Directory Search <https://doyou.needmorehdd.space>
- Open Directory Search <https://sites.google.com/view/133tech/tools/ods>
- Open Directory Search Finder <https://ewasion.github.io/opendirectory-finder>
- Palined Search <http://palined.com/search>
- Shodan <https://www.shodan.io>
- Opendirectories <https://www.reddit.com/r/opendirectories>

Поиск на форумах, новостных группах и досках обсуждений

- Binsearch <http://www.binsearch.info>
- BoardReader <http://boardreader.com>
- Craigslist Forums <https://forums.craigslist.org>
- Create a Forum: Forum Directory <https://www.createaforum.com/directory.php>
- Delphi Forums <http://www.delphiforums.com>
- Facebook Groups <https://www.facebook.com>

- Find a Forum <https://www.findaforum.net>
- Google Groups <https://groups.google.com>
- Iron March Exposed <https://www.ironmarch.exposed>
- The Joomla! Forum <https://forum.joomla.org/results.php>
- LinkedIn Groups <http://www.linkedin.com>
- Ning <http://www.ning.com>
- NZBIndex <https://www.nzbindex.com/groups>
- Omgili <http://omgili.com>
- ProBoards: Forum Directory <https://www.proboards.com/forum-directory>
- Xing Groups <https://www.xing.com/communities>
- Webhose.io <https://webhose.io>
- Wikipedia: List of Internet
- Forums https://en.wikipedia.org/wiki/List_of_Internet_forums
- Yahoo Groups <https://groups.yahoo.com>

Для начала разберемся с простыми запросами. У всех поисковых систем есть поисковые операторы, позволяющие уточнить результат поиска, сузить его, чтобы не читать то, что не относится к предмету поиска. В самом простом случае это логические операторы «И», «ИЛИ», «НЕ», которые обозначаются по-разному в разных поисковых системах.

Google dorking

Google hacking, также называемый Google dorking - изначально это хакерский метод, который используется в Google Search и других приложениях Google для поиска дыр в конфигурации и компьютерном коде, которые используют веб-сайты. Это предполагает использование расширенных операторов в поисковой системе Google для поиска определённых строк текста в результатах поиска. А теперь — техника, используемая журналистами, следственными органами, инженерами по безопасности и любыми пользователями для создания запросов в различных поисковых системах для обнаружения скрытой информации и уязвимостях, которые можно обнаружить на общедоступных серверах.

Прежде чем начнете изучать тему, есть несколько моментов, которые нужно запомнить:

1. Регистр не имеет значения. Гуглу неважно, написано заглавными или маленькими буквами.
2. Пробел между словами — это оператор «И». Мало того, Гугл будет искать все слова из запроса, а не только фразу целиком.

3. Гугл умеет склонять слова. Не надо тратить время на разные формы слов, он сам разберётся.
4. Гугл сортирует по релевантности. То есть показывает то, что ему кажется самым релевантным запросу.
5. На результаты влияет язык запроса. Искать нужно на том языке, на котором нужен результат.
6. На результат влияет история запросов. Гугл помнит, что искал в этом браузере, даже если ты в инкогнито. Поэтому нужно не только регулярно чистить историю поиска и куки но и использовать специализированные браузеры.
7. На результат влияет геопозиция. Гуглу важно, где ты находишься. Нужен VPN, если надо получить адекватные результаты из другой стран

Вот, в качестве примера, несколько наиболее используемых (но не всех) операторов. За каждым оператором следует двоеточие, за которым следует соответствующий ключевая фраза или слово:

intitle	Поиск по заголовку страницы
numrange	Поиск номера
daterange	Поиск в диапазоне дат
author	Поиск авторов группы
group	Поиск по названию группы
insubject	Поиск по теме группы
inurl	Поиск по URL
filetype	конкретные файлы
intext	Искать только текст страницы
site	Искать на конкретном сайте
link	Искать ссылки на страницы
inanchor	Поиск по якорному тексту в гиперссылках
related	Отображает список «похожих» веб-сайтов на нужный. Сходство основано на функциональных ссылках, а не на логических или содержательных связях.

Оператор «@» Используется для поиска индексации пользователей в социальных сетях: Twitter, Facebook, Instagram

AROUND(n) Позволяет искать два слова, расположенные на расстоянии определенного количества слов, друг от друга

Для Google существуют целые базы уже готовых дорков. Самая популярная из них – это Exploit DB: <https://www.exploit-db.com/google-hacking-database>

Правила формирования запроса поисковику

Правила мониторинга или правила отбора публикаций — это те правила, в соответствии с которыми система принимает решение соответствует конкретная публикация данному запросу или нет, показывать ее пользователю или нет.

Простое правило по сложной теме обычно дает много результатов, не относящихся к искомому объекту или проблеме. В результате аналитик вынужден читать (обрабатывать) много не целевой информации.

Чтобы отсеять информацию, не относящуюся к изучаемой проблеме, нужно сформировать соответствующие правила для запроса. Сложные правила позволяют точнее настроить сбор и свети к минимуму попадание в результаты запроса результатов, не относящихся к объекту или теме.

Для этого нужно тщательно продумывать запрос и использовать имеющиеся в системе инструменты его настройки. И хорошо, когда объект интереса имеет уникальное обозначение. Например, «Аэрофлот». В этом случае для отбора целевых сообщений достаточно в качестве правил указать само это обозначение, вероятно его вариант на латинице и, если есть, производные части речи. В случае с Аэрофлотом это прилагательное «аэрофлотовский», которое могут использовать в общении:

аэрофлот ИЛИ аэрофлотовский ИЛИ Aeroflot

Но в случае, если тема интереса может быть обозначена не просто разными словами, а сочетаниями разных слов, то важно продумать все варианты. Иначе появляется шанс упустить важное.

Предположим, что Вы планируете в ближайшее время совершить пешее путешествие по склонам Альп. Раньше Вы не бывали в горах. Вам нужно подготовиться. Как найти в инете возможные угрозы и опасности, к которым стоит подготовиться заранее? Самый простой способ – воспользоваться поисковым сервисом, но проблема в том, как составить запрос, чтобы не читать лишнее, но не упустить важное. Если задать запрос «альпы» или «горы», то вы получите невероятное число ответов, не имеющих отношение к тому, что вы ищите. Значит нужно как-то отсеять лишнее. Вот для таких ситуаций и предназначены поисковые операторы.

Этапы формирования запроса по сложной теме (сложного запроса):

1. Сформулировать задачу (проблему) «как есть»;
2. Оптимизировать описание задачи (проблемы);
3. Выделить ключевые слова из описания задачи;
4. Осуществить «семантическое расширение» ключевых слов;
5. Составить запрос с учетом поисковых операторов.

Сформулировать задачу (проблему) «как есть»

Вначале запишите вашу проблему теми словами, которые в данный момент вам приходят. В форме утверждения или вопроса – не важно. Главное зафиксировать.

Если рассматривать вопрос с подготовкой к походу в Альпы, то это может выглядеть следующим образом:

«К каким проблемам или угрозам мне нужно подготовиться заранее, если я планирую пешее путешествие по склонам Альп»

Оптимизировать описание

Затем необходимо оптимизировать описание проблемы таким образом, чтобы решить две задачи:

1. Свести к минимуму возможный «информационный шум» – ненужную информацию;
2. Не упустить важное.

Для этого переформулируем проблему по возможности кратко и в то же время однозначно характеризующим искомые данные. Например, укорачиваем формулировку, удаляем из формулировки проблемы слова-паразиты, заменяем ненормативную лексику на общепринятые понятия. Если рассматривать вопрос с подготовкой к походу в Альпы, то это может выглядеть следующим образом:

«Проблемы или угрозы при пешем путешествии в Альпах»

Выделить ключевые слова

Затем выбираем в формулировке проблемы те слова, без которых теряется ее смысл. Если рассматривать вопрос с подготовкой к походу в Альпы, то это:

1. опасность или угроза
2. путешествие
3. Альпы

Осуществить «семантическое расширение» ключевых слов

Нахождение дополнительных понятий, которые могут быть использованы другими людьми для описания интересующей вас проблемы. Например, синонимы для слова «переход» — это путь, ходьба, движение.

«Расширяем» выбранные ключевые слова проблемы с подготовкой к походу в Альпы:

1. «Альпы» - горы, Анды, Пиренеи, другие горные системы...
2. «путешествие» - движение, перемещение, туризм, поход...
3. «опасность» - сложность, трудность, проблема, угроза...

В зависимости от исследуемой темы такими словами (понятиями) могут быть сами синонимы, синонимические выражения из двух и более слов, слова близкие по значению, слова, используемые в той же области, в том числе родо-видовые и связанные понятия.

Например, для понятия САМОЛЁТ:

1. Родо-видовые понятия – летательный аппарат (так-как это и вертолёт, и аэростат...)
2. Синоним – аэроплан
3. Подчинённые понятия – истребитель, бомбардировщик...
4. Связанные понятия – крыло, фюзеляж, лётчик...

Еще один важный момент, который приходится учитывать, связан с ошибочными написаниями. Но он имеет значение в случае, если вам нужны данные из социальных сервисов. Дело в том, что люди часто совершают ошибки и опечатки при формулировании своих мыслей в виде текста. И при формировании поискового запроса, если важно не упустить ничего, необходимо учесть вероятность неправильно написания ключевых слов, задействованных в запросе.

Вариант ошибочных написаний — это намеренные ошибки или замена кириллических букв на аналогичные латинские для усложнения поиска исследователями. Например «а» в кириллице на «a» в латинице и т.п...

Составить запрос с учетом поисковых операторов

Посредством правил и доступных операторов поисковой системы описывается взаимное положение поисковых блоков и их взаимная зависимость.

Если рассматривать вопрос с подготовкой к походу в Альпы, то запрос будет выглядеть так:

(Альпы ИЛИ горы ИЛИ Пиренеи) И (трудность ИЛИ сложность ИЛИ опасность ИЛИ проблема ИЛИ угроза) И (переход ИЛИ движение ИЛИ перемещение ИЛИ туризм ИЛИ поход)

оператор ИЛИ должен быть оформлен по правилам той поисковой системы, в которой планируете поиск. Для Google это «OR», а для Яндекса «|».

Оператор «И» на «AND» и «+» соответственно.

Сбор удаленных или измененных данных в интернете

Нередко бывает, что ссылка на интересующие материалы уже «не работает». Происходит это по разным причинам, но наиболее неприятная для нас это удаление информации для сокрытия следов или в связи с какими-то изменениями. В такой ситуации может помочь поиск по особым источникам, хранящим прошлые версии страниц разных сайтов.

Кэш поисковых систем

Если информация была удалена совсем недавно и все еще появляется в поиске Google или Яндекс, попробуйте щелкнуть соответствующий значок (иконку) рядом с ее упоминанием в поисковой выдаче. Так вы можете получить доступ к копии, сохраненной в кэше поисковой системы.

Кэш Google

Для просмотра прошлой версии страницы из кеша Google надо в адресной строке набрать: <http://webcache.googleusercontent.com/search?q=cache:http://www.iphones.ru/>

Где <http://www.iphones.ru/> надо заменить на адрес той страницы, прошлую версию которой ищите.

Кэш Baidu

Когда ищешь в кэше Google статьи удаленные с habrahabr.ru, то часто бывает, что в сохраненную копию попадает версия с надписью «Доступ к публикации закрыт». Ведь Google ходит на этот сайт очень часто! А китайский поисковик Baidu значительно реже (раз в несколько дней), и в его кэше может быть сохранена другая версия. Иногда срабатывает, иногда нет. Ссылка на кэш находится сразу справа от основной ссылки.

Архивы интернета

Есть специализированные сервисы в интернете, которые занимаются тем, что сохраняют разные версии сайтов и страниц на них. Также есть сервисы, которые делают поиск по таким архивам более удобным.

Wayback Machine archive.org

Wayback Machine — это интернет-архив, который сохраняет копии веб-страниц. Он позволяет просматривать, как выглядело содержимое веб-сайтов в прошлом. Сервис полезен для анализа изменений на сайтах, доступа к удаленной информации или просмотра сайтов, которые больше не существуют в своем исходном виде.

Archive.is аналог предыдущего сервиса. Но в его базе явно меньше ресурсов, чем у Wayback Machine. Да и отображаются сохранённые версии не всегда корректно. Зато он может выручить, если вдруг в Wayback Machine не окажется копий необходимой вам страницы.

WebCite webcitation.org

В базе WebCite преобладают научные и публицистические статьи. Если вдруг вы процитируете чей-нибудь текст, а потом обнаружите, что первоисточник исчез, можете поискать его резервные копии на этом ресурсе.

CachedPage cachedpage.co

Альтернатива CachedView. Выполняет поиск резервных копий по хранилищам Wayback Machine, Google и WebCite.

CachedView cachedview.com

Сервис CachedView ищет копии в базе данных Webcache, Wayback Machine, Library of Congress, Perma.cc, Live Version и Archive today или кеше Google — на выбор пользователя.

Иные способы

«Зеркало» сайта

Зеркало веб-сайта — это точная копия этого сайта, которая находится на другом сервере в Интернете. Если вы ищете удалённый файл, попробуйте найти зеркало страницы, на которой находилась ссылка на него. Может быть, на странице-зеркале ссылка будет изменена и файл, в отличие от оригинального, не будет удалён. Найти зеркало веб-сайта очень просто: надо ввести известную часть текста одной из его страниц в качестве запроса поисковой системе. Если текст на страницах сайта вам совершенно незнаком, укажите имя страницы или файла, путь к которым вы знаете.

Сбор данных в интернете с помощью ИИ

Современные сервисы, основанные на генеративном ИИ, очень хорошо справляются с быстрой переработкой большого объема информации из интернета. Конечно, они имеют свои ограничения, которые нужно учитывать, но для старта работ или в условиях сильного ограничения по времени, эти сервисы позволяют существенно ускорить процесс первичного сбора и структурирования информации из открытых источников.

Для того, чтобы максимально задействовать возможности ИИ нужно научиться правильно задавать ему вопросы. Такой вопрос (запрос) к ИИ называется промпт. Промпт (от англ. prompt — «подсказка») — это текстовое описание задачи, которую необходимо выполнить с помощью ИИ-модели. Это запрос, который задается модели для генерации текста, изображений, кода или других видов контента.

Например, если вы хотите получить изображение в стиле картины «Звездная ночь» Ван Гога, то ваш промпт может выглядеть так: «Ты — профессиональный иллюстратор. Тебе хорошо известны стиль и манера письма популярных художников. Твоя задача — создавать изображения в манере выбранного художника. Создай изображение ночного неба в стиле Ван Гога». Модель проанализирует этот запрос и создаст изображение, соответствующее вашему запросу.

Промпты по нашей теме (сбор открытых данных об объекте) для разных сервисов отличаются не значительно, поэтому используйте промты в том сервисе, который вам удобен. Основная задача — научиться создавать и формулировать такие промты, чтобы получать от них наиболее точные и релевантные результаты. Для этого нужно уметь формулировать запросы так, чтобы модель могла понять и выполнить задачу максимально точно.

В процессе создания промпов вами будет собрана библиотека промпов. Библиотека промпов — это набор качественных промпов, которые можно использовать для обучения или тестирования языковой модели. Промпты в библиотеке могут быть сгруппированы по темам, стилям или другим параметрам, что упрощает их поиск и использование.

Применение библиотеки промпов позволяет ускорить процесс создания контента с помощью языковых моделей, а также обеспечивает более предсказуемый результат, поскольку все запросы уже были предварительно проверены. При этом нужно учитывать, что модели регулярно обновляются и будет полезно тестировать имеющиеся промпы на новых версиях.

Как создать качественный промпт

Качественный промпт — это хорошо структурированный и детализированный запрос, который точно транслирует пожелания пользователя и дает нейросети достаточно информации для генерации корректного и релевантного ответа. Такой промпт повышает вероятность получения желаемого результата.

Первый шаг — это четкая цель. Например, если вы хотите собрать актуальную информацию о текущей политической ситуации в стране X, вы можете начать с цели:

Предоставьте список надежных онлайн-источников актуальной политической информации в X, включая любую известную предвзятость каждого источника .

Затем добавьте контекст:

Список должен включать 5 источников на английском языке и 5 источников на арабском языке, включая новостные агентства, академические журналы и аналитические центры .

Наконец, укажите ограничения:

Источники должны быть сосредоточены на политических новостях и информации о правах человека за 2024 год .

Четко определяя эти элементы, вы помогаете ИИ составить целевой список, который не только включает разнообразные источники, но и дает критически важную информацию об их надежности и предвзятости, делая ваши усилия по OSINT более комплексными и эффективными.

ИИ сервисы еще могут быть очень эффективными в помощи при создании сложных запросов Google (известных как Google dorks или Google dorking) и команд для различных инструментов OSINT с открытым исходным кодом. Google dorks

Примеры:

Напишите Google dork, чтобы найти общедоступные документы, которые могут непреднамеренно содержать конфиденциальную информацию на домене example.com

Напишите Google dork, чтобы найти адреса электронной почты, связанные с доменом example.com

Напишите Google dork, чтобы найти поддомены, связанные с основным сайтом domain.com

Мало того, можно запросить у ИИ информацию о методологии проведения исследования. Например:

Предоставь мне целенаправленную структуру для проведения технического расследования домена, направленного на раскрытие владельца подозрительных веб-сайтов. Исключи журналистские и писательские фазы; мой главный интерес заключается в выявлении и проверке связей домен-домен и домен-человек. Сгруппируй эти шаги в 4 основные категории, чтобы обеспечить более рациональный подход.

Результат:

1. Сбор информации о домене и владельце

WHOIS-данные: Используйте WHOIS-сервисы для получения информации о владельце домена (имя, адрес, электронная почта, дата регистрации). Это первый шаг для установления контактов или получения скрытой информации через сервисы WHOIS, которые могут предоставить исторические данные.

DNS-анализация: Примените инструменты для анализа записей DNS (например, A, MX, NS, TXT). Это поможет выявить связанное оборудование или серверы.

История регистрации домена: Используйте сервисы для анализа исторической информации о доменах (например, DomainTools), чтобы узнать, какие лица или организации владели доменом в прошлом.

Обратный поиск IP-адресов: Для установления связи с другими доменами, размещенными на тех же IP-адресах, используйте инструменты вроде Reverse IP Lookup.

2. Анализ веб-ресурсов и связанной информации

Анализ структуры веб-сайта: Исследуйте сайт на наличие контактных данных, метаданных, специфических настроек (например, идентификаторы в URL, скрытые формы), которые могут указывать на связанное лицо или организацию.

Анализ ссылок: Используйте инструменты для анализа внешних и внутренних ссылок (например, Ahrefs, Majestic), чтобы выявить веб-сайты, ссылающиеся на этот домен, а также сайты, на которые ссылается этот домен.

Анализ хостинга: Узнайте, какой хостинг-провайдер обслуживает сайт, и ищите возможные связи с другими клиентами этого провайдера.

Сертификаты SSL: Используйте анализаторы SSL для получения информации о владельцах сертификатов, это может дать представление о связях с другими веб-сайтами.

3. Поиск и анализ сопутствующих доменов

Использование сервисов для поиска похожих доменов: Используйте инструменты для поиска схожих доменов (например, DNSdumpster), чтобы найти домены, которые могут быть зарегистрированы на ту же организацию или людей.

Проверка на альтернативные TLD (доменные зоны): Иногда организация может зарегистрировать домены в других расширениях, схожих с основным (например, example.org, example.net). Используйте подобные инструменты для поиска этих доменов.

Проверка на субдомены: Ищите субдомены, которые могут быть зарегистрированы с похожими именами, указывая на возможные скрытые связи.

Идентификация цепочки доменов: Если домен связан с подозрительными или поддельными веб-сайтами, используйте технологии для отслеживания последовательности регистрации доменов, чтобы выявить связанное лицо или организацию.

4. Анализ социальных связей и поведенческих данных

Поиск по email-адресам, использованным для регистрации: Проведите анализ email-адресов, связанных с регистрацией домена, с помощью социальных сетей или сервисов проверки (например, Hunter.io), чтобы попытаться найти другие сайты или профили, где этот email использовался.

Анализ IP-адресов и геолокации: Используйте инструменты для анализа геолокации IP-адресов, которые использовались для доступа или хостинга сайта, чтобы получить дополнительные данные о владельцах или операторах.

Интервьюирование вовлеченных сторон: Если информация о владельцах или операторах доменов скрыта, можно обратиться к третьим сторонам (например, регистраторам доменов, хостинг-провайдерам) для получения дополнительной информации.

Поиск следов в социальных сетях: Если домен или организация связаны с определенным человеком, исследуйте его возможные аккаунты в социальных сетях, а также активность вокруг домена.

Основные рекомендации для создания промптов

Общие правила (требования) составления промптов:

1. В запросе используйте однозначные формулировки без дусмысленностей или противоречий.
2. Ответ ИИ может выдать неактуальную информацию, если промпт содержит устаревшие данные.
3. Добавьте в промпт примеры, которые продемонстрируют модели, как следует выполнять задания правильно. Модель будет стремиться обнаружить закономерности и связи в приведенных примерах и использовать их для формирования своего ответа. Экспериментируйте с оптимальным количеством примеров: от одного до нескольких.

Что поможет улучшить промпт

Как еще можно повысить качество ответов ИИ и повысить вашу эффективность?

Экспериментируйте с формулировками.

Создайте несколько вариантов запроса на одну тему и проанализируйте полученные результаты, чтобы выявить наиболее продуктивные подходы.

Уточняйте запросы.

Используйте полученные данные для дальнейшей оптимизации промптов и их уточнения. Постоянный анализ ответов поможет улучшить качество запросов и, как следствие, итоговых результатов.

Спрашивайте ИИ как она пришла к таким выводам и что не хватает.

Не стесняйтесь уточнить у сервиса ИИ на основании каких данных она пришла к таким выводам или что по ее мнению не хватает в описании объекта, на что нужно обратить внимание. Это позволит выявить пробелы в вашем промпте и еще его улучшить.

Спрашивайте у ИИ что ей не хватает для более детального ответа на ваш запрос. В этом случае сервис укажет вам на то, какую информацию желательно поместить в ваш промпт, чтобы ответ на него был полнее.

Примеры

Примеры промптов и результатов их работы.

Составление досье на компанию

Предположим вам нужно изучить некую компанию.

Промпт:

Ты конкурентный разведчик.

Тебе нужно сформировать досье на компанию "Пфайзер" она-же Pfizer для оценки ее надежности.

Сформируй результаты сбора данных по разделам:

- название компании, его варианты и установочные данные;
- руководство компании;
- акционеры компании;
- история компании;
- контакты компании;
- ключевые проекты компании;
- клиенты компании;
- проблемы, конфликты, споры, суды компании.

Результат работы ИИ:

Название компании, его варианты и установочные данные:

Название: Pfizer, Inc.

Варианты названия: Пфайзер (в России)

Тип: Публичная компания

Листинг на бирже: NYSE: PFE

Основание: 1849 год

Основатели: Чарльз Файзер и Чарльз Эрхарт

Расположение: Нью-Йорк, США

Руководство компании

СЕО и председатель совета директоров: Альберт Бурла

Председатель совета директоров (ранее): Йен Рид

Другие ключевые фигуры: Дон Корнуэлл, Констанц Хорнер, Джеймс Смит, Элен Хоббс, Джеймс Килтс, Деннис Аузилло, Шантану Нарайен, Сьюзан Нора Джонсон, Роналд Блейлок, Ден Литтман, Жозев Эшвария

Акционеры компании

Институциональные инвесторы: 66,45% акций

The Vanguard Group, Inc (8,3%)

BlackRock (7,3%)

State Street Corporation (5,1%)

Capital World Investors (4,2%)

Wellington Management Group (3,9%)

Geode Capital Management (1,8%)

Northern Trust Corporation (1,2%)

Bank Of America Corporation (1,0%)

История компании

Основана в 1849 году Чарльзом Файзером и Чарльзом Эрхартом.

2004 год: Акции включены в Промышленный индекс Доу Джонса.

2006 год: Продажа подразделения безрецептурных препаратов компании Johnson & Johnson.

2011 год: Соглашение с НПО «Петровакс Фарм» о производстве пневмококковой вакцины в России.

2018 год: Сотрудничество с BioNTech по разработке вакцин против гриппа.

2019 год: Объединение с Mylan для создания Viatris.

2020 год: Исключение из Промышленного индекса Доу Джонса.

2021 год: Приобретение компании Arena за \$6,7 млрд.

Контакты компании

Штаб-квартира: Нью-Йорк, США

Представительства: Многочисленные офисы по всему миру, включая Россию (с 1992 года).

Ключевые проекты компании

Comirnaty (вакцина от COVID-19): Разработана в сотрудничестве с BioNTech.

Виагра, Липримар, Дифлюкан, Целебрекс: Известные фармацевтические препараты.

Сотрудничество с BioNTech по вакцинам против гриппа: Инвестиции в размере \$425 млн.

Приобретение Seagen за \$43 млрд: Расширение портфеля онкологических препаратов.

Клиенты компании

Глобальные: Миллионы пациентов и медицинские учреждения по всему миру.

Россия: Более 100 зарегистрированных препаратов, доступных российским пациентам.

Проблемы, конфликты, споры, суды компании

Споры и суды: Pfizer участвовала в различных судебных разбирательствах, связанных с патентами и маркетингом препаратов.

Критика и конфликты: Критика в отношении цен на лекарства и маркетинговых практик.

Регуляторные проблемы: Встречается с регуляторными вызовами в различных странах из-за рекламы и безопасности препаратов.

Цифры в конце предложений это номера источников, из которых взяты данные.

Согласитесь, если вы начинаете «с нуля» изучать организацию, то такой результат в течении секунды - это неплохой старт в формировании досье. Безусловно, дальше нужно уточнять, расширять, детализировать...

Досье на человека

Можно подойти к задаче чуть иначе.

Промпт:

Цель материала: написать развёрнутый, информативный текст о Илон Маск. Основной акцент должен быть сделан на объяснение его возможностей в политике (бизнесе, криминале...).

Стиль изложения: текст должен быть написан простым и понятным языком. Без сложных терминов, требующих разъяснения.

Объем и содержание: материал должен быть объёмом 1500 слов, равномерно распределенных между разделами.

Фокус на связях Илона Маска и его ресурсах.

Структура материала:

1 раздел. Установочные данные Илона Маска: род занятий, дата и место рождения, происхождение, вероисповедание, хобби, документы, адреса проживания, контактные данные, псевдонимы и клички.

2 раздел. Компетенции Илона Маска: где и когда учился, где, когда и кем работал, в каких проектах участвовал, какие знания имеет, какие награды получал.

3 раздел. Семья и родственники Илона Маска: супруги настоящие и бывшие, дети, родители, братья, сестры, родственники супругов. По каждому нужны дата и место рождения, род занятий, место проживания, контактные данные.

4 раздел. Бизнес Илона Маска: настоящи и прошлый бизнес, роль в нем.

5 раздел. Связи Илона Маска: с кем взаимодействовал по бизнесу, в политике, в криминальной среде.

6 раздел. Конфликты Илона Маска: с кем конфликтовал и по какому поводу, в каких уголовных делах участвовал, в каких судебных разбирательствах участвова, какие взыскания получал.

Результат работы ИИ:

Илон Маск — известный предприниматель, инженер и миллиардер, основатель нескольких инновационных компаний, таких как SpaceX, Tesla и The Boring Company¹⁶. Его вклад в развитие технологий и бизнеса делает его одной из самых влиятельных фигур в современном мире¹.

1. Установочные данные:

Род занятий: Предприниматель, инженер, изобретатель, инвестор.

Дата и место рождения: 28 июня 1971 года, Претория, ЮАР.

Происхождение: Отец — инженер из Южной Африки, мать — диетолог и модель из Канады.

Гражданство: Канада, США.

Политическая позиция:

Изначально Маск называл себя "наполовину демократом, наполовину республиканцем", но со временем его взгляды стали более консервативными².

Он поддерживал разных кандидатов, включая Барака Обаму, Хиллари Клинтон и Дональда Трампа².

2. Компетенции Илона Маска:

Образование:

Университет Куинс в Кингстоне, Канада¹.

Пенсильванский университет, где получил степени бакалавра по экономике (1993) и физике (1994)¹³.

Поступил в Стэнфордский университет, но бросил учёбу¹³.

Карьера:

Zip2 (1995—1999): Соучредитель компании, занимавшейся разработкой программного обеспечения для интернета¹. Компания была приобретена Compaq за 307 миллионов долларов¹.

X.com и PayPal: Соучредитель X.com, онлайн-банка, который позже стал PayPal¹³. В 2002 году PayPal был куплен eBay за 1,5 миллиарда долларов¹³.

SpaceX (с 2002): Основатель, генеральный директор и главный инженер компании по производству аэрокосмической техники¹².

Tesla (с 2004): Присоединился к компании в качестве председателя совета директоров и архитектора проекта, а в 2008 году стал генеральным директором¹.

SolarCity (2006): Помог создать компанию по предоставлению услуг в области солнечной энергии, которая впоследствии была приобретена Tesla¹.

OpenAI (2015): Соучредитель некоммерческой исследовательской компании, занимающейся продвижением искусственного интеллекта¹.

Neuralink (2016): Соучредитель нейротехнологической компании, разрабатывающей интерфейсы мозг-компьютер¹.

The Boring Company (2016): Основатель компании по строительству туннелей¹.

Twitter (X) (2022): Приобрёл компанию за 44 миллиарда долларов¹.

Достижения и награды:

Первым в истории достиг отметки состояния в 400 млрд долларов¹.

Является главным конструктором ракет Falcon и Dragon⁴.

Разработал систему Starlink, обеспечивающую высокоскоростной доступ в интернет из любой точки мира⁴.

3. Семья и родственники:

Отец: Эррол Маск, инженер⁴⁵.

Мать: Мэй Маск, диетолог и модель⁴⁵.

Брат: Кимбал Маск, владелец сети ресторанов The Kitchen¹⁵.

Сестра: Тоска Маск, кинорежиссёр и продюсер⁵.

4. Бизнес Илона Маска:

Текущий бизнес:

SpaceX: Компания занимается производством ракет и космических кораблей¹⁴.

Tesla: Производство электромобилей и энергетических решений¹.

The Boring Company: Строительство туннелей для уменьшения заторов на дорогах¹.

Neuralink: Разработка нейроинтерфейсов¹.

Twitter (X): Платформа социальных сетей¹.

Прошлый бизнес:

Zip2: Программное обеспечение для новостных компаний¹³.

PayPal: Система онлайн-платежей¹³.

5. Связи Илона Маска:

Встречался с представителями «Космотраса» и НПО Лавочкина в Москве, чтобы обсудить покупку ракет для SpaceX⁴.

Дональд Трамп: Маск активно поддерживает Трампа и обещает ему ведущую роль в своей будущей администрации, если тот будет переизбран¹. Он начал выражать активную поддержку Трампу после июльского покушения на него⁶.

Владимир Путин: По данным The Wall Street Journal, Маск поддерживал контакт с президентом России Владимиром Путиным с конца 2022 года¹. Путин якобы просил Маска не активировать систему Starlink на Тайване¹.

6. Конфликты Илона Маска:

В 1999 году совет директоров Zip2 пресекал попытки Маска стать генеральным директором¹.

В 2001 и 2002 годах Маск приезжал в Москву, чтобы купить ракеты, но не смог договориться о цене с российскими компаниями⁴.

Цифры в конце предложений это номера источников, из которых взяты данные.

Составление плана действий

А можно спросить у ИИ что нужно сделать, чтобы составить развернутое досье:

Предоставь мне целенаправленную структуру последовательности действий в интернете для составления досье (профайла) на человека, направленного на выявление его связей, ресурсов, возможностей. Исключи журналистские и писательские фазы, мой главный интерес заключается в выявлении и проверке его связей. Сгруппируй эти шаги в этапы, чтобы обеспечить более рациональный подход.

Вот, что ИИ предложил:

Этап 1: Сбор базовой информации

Идентифицируйте объект, собрав основные данные: ФИО, дата рождения, место жительства.

Проверьте установочные данные: ИНН, паспортные данные.

Соберите контактную информацию: телефоны, электронная почта.

Этап 2: Анализ профессиональной деятельности

Исследуйте сведения об образовании, проверяя подлинность документов.

Изучите историю трудовой деятельности и текущее место работы.

Проанализируйте участие в предпринимательской деятельности (учредитель, директор, ИП).

Этап 3: Выявление связей

Составьте список близких родственников.

Используйте сервисы вроде СПАРК для поиска связей между юридическими и физическими лицами.

Проверьте аффилированность с компаниями и другими лицами.

Этап 4: Анализ финансового положения

Соберите информацию об имуществе.

Проверьте наличие задолженностей, включая налоговые.

Изучите кредитную историю.

Этап 5: Проверка репутации

Исследуйте наличие судимостей и другой негативной информации.

Проанализируйте упоминания в СМИ и социальных сетях.

Этап 6: Углубленный анализ связей

Используйте графовую базу данных для визуализации связей.

Раскройте связи на несколько уровней иерархии.

Проверьте аффилированность с контрагентами и объектами из негативных списков.

Этап 7: Верификация и обобщение

Проверьте достоверность собранной информации из различных источников.

Систематизируйте и структурируйте полученные данные.

Составьте итоговое досье, отражающее все выявленные связи, ресурсы и возможности объекта.

Уточнение, где можно найти информацию для досье

Если сомневаетесь или не знаете какие источники информации можно задействовать для сбора информации, то это тоже можно уточнить у сервиса ИИ.

Промпт:

Какие открытые инструменты, открытые сервисы и открытые базы данных наиболее эффективны для формирования досье на человека?

Ответ ИИ:

Для формирования досье на человека наиболее эффективны следующие открытые инструменты, сервисы и базы данных:

Поисковые системы: Google, Bing, Yandex для базового поиска информации о человеке¹.

Инструменты OSINT:

-Maryam: многофункциональный инструмент для поиска информации по реальному имени и нику².

-Snoor: быстрый инструмент для поиска по имени, использующий около 500 источников².

-Alfred: утилита для сбора информации и идентификации аккаунтов в социальных сетях².

-Intelligence X: архивный и поисковый сервис с обширной базой данных⁴.

Специализированные поисковые системы:

-UserSearch.org: сеть поисковых систем для поиска людей по именам пользователей и электронной почте⁴.

Инструменты для анализа документов:

-Metagoofil: извлекает метаданные из общедоступных документов (PDF, Doc, Docx, Xls)⁴.

Социальные сети:

-Facebook, Instagram, LinkedIn для поиска публично доступной информации о человеке⁵.

Открытые государственные базы данных:

-Базы данных судебных решений

-Реестры юридических лиц и индивидуальных предпринимателей

-Базы данных исполнительных производств

Архивы СМИ и новостные агрегаторы для поиска упоминаний человека в прессе³.

-Специализированные сайты для поиска по изображениям, такие как Google Images или TinEye².

Есть в интернете и библиотеки промптов на все случаи жизни. Несколько примеров таких библиотек:

- academy.bothub.chat/biblioteka-promtov
- superhuman.ai/c/1000_chatgpt_prompts
- giga.chat/catalog
- ai.mitup.ru/prompts
- prompt-chatgpt.ru/biblioteka-promptov/

Методика сбора информации о человеке

Обсудим методику на примере составления досье на человека, как наиболее часто применяемую технологию. Для начала уточним, что именно мы надеемся найти, когда изучаем человека (составляем на него досье). Что для нас важно, на что обращать внимание. Ответы на эти вопросы позволяют определить, где искать необходимую информацию и какие технологии сбора информации применять.

В этом блоке максимально разберем все возможные приемы и технологии, а в следующих методиках уже будем разбирать только специфические, характерные для них техники.

Что ищем

Это не простой вопрос и ответ на него зависит от целей исследования. Но есть одна цель, которая присутствует полностью или частично во многих сценариях исследования человека. Это угрозы, источником которых данный объект может быть или может спровоцировать эти угрозы своими действиями.

Например, изучая кандидата на работу в компанию желательно выявить какие угрозы компании может представлять этот человек в случае его попадания «внутрь» структуры:

- Криминальные угрозы (мошенничество, воровство, рейдерский захват...)
- Экономические угрозы (низкая проф-подготовка, неспособность к данному виду деятельности...)
- Психологические угрозы (повышенная конфликтность, дестабилизация коллектива...)

А изучая частного инвестора, готового вложить в развитие компании значительную сумму, важно определить следующие угрозы:

- Криминальные угрозы (мошенничество, рейдерский захват...)
- Экономические угрозы (финансовая способность выполнить свои обязательства)
- Психологические угрозы (повышенная конфликтность, реальность намерений выполнить свои обязательства, подверженность внешнему влиянию...)

Это хоть и несколько разный, но всё же пересекающийся набор угроз. Вот на выявлении этих угроз и разберем методологию изучения человека, а под другие задачи вы сможете ее адаптировать уже сами.

Для начала формулируем цель исследования: угрозы, которые нужно учитывать в случае взаимодействия с неким человеком.

Следующий вопрос – о каких вообще угрозах идет речь? Частично мы уже ответили на этот вопрос, но уточним. Мы ищем прямое или косвенное указание на возможность возникновения следующих угроз:

- Криминальные (от личной нечистоплотности до ОПГ);
- Экономические (от слабых компетенций до финансовой несостоятельности)
- Психологические (от конфликтности до скрытых намерений).

Теперь нужно определить, что может указывать на интересующую нас информацию (на угрозы). Это то, что предстоит искать:

1. Криминальные угрозы

- 1.1. Связь с криминалом: поддержка дружеских или деловых отношений с лицами, имеющими криминальное прошлое, взаимодействие с криминальными структурами.
- 1.2. Собственный криминальный опыт: это может быть собственный криминальный опыт (приводы в полицию, уголовные дела...), косвенное, но регулярное фигурирование в событиях с криминальной составляющей
- 1.3. Действия, указывающие на готовность переступить закон: соответствующие высказывания в интервью, в своих публикациях в соцсетях, в частных беседах.

2. Экономические угрозы

- 2.1. Компетенции, а точнее их отсутствие у человека, заявляющего, что он гуру в определенной области: отсутствие профильного образования, отсутствие

профильного опыта как официальный так и не официального, соответствующее мнение о таком специалисте в профессиональном сообществе.

2.2. Наличие имущества: наличие чрезмерно дорогого имущества у человека, чей доход не может позволить владеть такими активами, указывает либо на не декларируемые доходы (например откаты), либо на богатых родственников. В первом случае высока вероятность, что такой персонаж и в отношении вашего проекта будет искать недокументированные возможности обогащения.

2.3. Чрезмерные траты как и наличие чрезмерного имущества является косвенным указанием на вероятность будущих проблем.

3. Психологические угрозы

3.1. Конфликты: конфликтный человек чаще всего наносит вред коллективу, даже при наличии интересных компетенций. А по тому является носителем потенциальных угроз для компании.

3.2. Нежелательные черты характера: имеются ввиду иные, помимо конфликтности, черты характера, которые могут вызвать в коллективе конфликты. Например интриганство, сплетничество, патологическое вранье, еще что-то.

Примеры сервисов для поиска человека:

- Addresses (US) <http://www.addresses.com>
- Aleph <https://github.com/alephdata/aleph>
- Alumni.net <http://www.alumni.net>
- AnyWho (US) <https://www.anywho.com/whitepages>
- Australia Lookup <http://www.australialookup.com>
- Aware Online: People Search <https://www.aware-online.com/osinttools/personen-search-tool>
- Classmates <http://www.classmates.com>
- Connectifier Social Links <https://chrome.google.com/webstore/detail/connectifier-social-links/dalkcdejepndhaijgjbfnocpfickn>
- CrunchBase <http://www.crunchbase.com>
- Cyber Background Checks (US) <https://www.cyberbackgroundchecks.com>
- dataScrape <https://github.com/khayes-r7/dataScrape>
- Facesearch <http://facesaerch.com>
- Full Contact <https://www.fullcontact.com>
- GoFindWho <https://gofindwho.com>

- Gravatar <http://en.gravatar.com>
- Hauziz (US) <https://hauziz.com>
- hedd <https://hedd.ac.uk>
- Hitta.se (Sweden) <https://www.hitta.se>
- Hola Connect <https://holaconnect.com>
- How Many of Me <http://howmanyofme.com/search>
- IDCrawl <https://www.idcrawl.com>
- Intelius (US) <https://www.intelius.com/people-search>
- IntelligenceX: Person Lookup by
Full Name <https://intelx.io/tools?tab=person>
- Itools <http://itools.com/search/people-search>
- <http://itools.com/tool/wink-people-search>
- John Doe (US) <https://johndoe.com>
- Keybase <https://keybase.io>
- LeadFerret (US) <https://leadferret.com/search>
- LittleBrother <https://github.com/Lulz3xploit/LittleBrother>
- LittleSis <https://littlesis.org>
- ManyContacts Mail Check <https://www.manycontacts.com/en/mail-check>
- MarketVisual <http://www.marketvisual.com>
- NameScan <https://namescan.io>
- National Student Clearinghouse <https://nscverifications.org/welcome-to-verification-services>
- Neighbor Report (US) <https://neighbor.report>
- Nextdoor (US) <https://nextdoor.com>
- Nuwber <https://nuwber.com>
- peekyou <https://www.peekyou.com>
- Peoplefinders (US) <https://www.peoplefinders.com>
- People Looker (US) <https://www.peoplelooker.com>
- People Search <http://netbootcamp.org/peoplesearch.html>

- People Search (Australia) <http://www.peoplesearch.com.au>
- PeopleSmart (US) <https://www.peoplesmart.com>
- People Yandex (RU) <https://yandex.ru/people?lr=100>
- PimEye <https://pimeyes.com/en>
- Pipl <https://pipl.com>
- PrivateEye <https://www.privateeye.com>
- Qualification Check <https://www.qualificationcheck.com>
- Radaris (US) <https://radaris.com>
- Recruit'em <http://recruitin.net>
- Reverse Genie <http://www.reversegenie.com>
- SearchBug (US) <https://www.searchbug.com>
- Search GB <https://www.searchgb.co.uk>
- Search People Online <https://www.search-people.online>
- Search Systems (US) <https://publicrecords.searchsystems.net>
- Skipease (US) <http://www.skipease.com>
- Skopenow <https://www.skopenow.com>
- Smugmug <https://www.smugmug.com/search>
- Social Catfish <https://socialcatfish.com>
- Social List <https://sociallist.io>
- SocialPath <https://github.com/woj-ciech/SocialPathSMWYG-Show-Me-What-You-Got>
<https://github.com/Viralmaniar/SMWYG-Show-Me-What-You-Got>
- Snitch.name <http://www.snitch.name>
- Snoop Station (US) <http://snoopstation.com>
- Social catfish <https://socialcatfish.com>
- Spokeo <http://www.spokeo.com>
- Spyttox (US) <https://www.spytox.com>
- Strava <https://labs.strava.com/heatmap>
- Sydex <http://sydex.net>
- TalentBin <https://www.talentbin.com>

- That's Them (US) <https://thatsthem.com>
- Trape 2.0 <https://www.kitploit.com/2018/11/trape-v20-people-tracker-on-internet.html?amp=0>
- TruePeopleSearch (US) <https://www.truepeoplesearch.com>
- Truth Finder <https://www.truthfinder.com>
- ufind.me <http://ufind.name>
- UserSearch <https://usersearch.org>
- USSEARCH (US) <https://www.ussearch.com>
- WebMii <http://www.webmii.com>
- Xlek (US) <https://www.xlek.com>
- Yasni <http://www.yasni.com>
- Zaba Search <https://www.zabasearch.com>
- Zoominfo <http://www.zoominfo.com>

Госучеты, связанные с людьми - публичные записи, включая записи о рождении, смерти, браке, иммиграции и другое

- Australia Public Records <http://australiapublicrecord.com>
- BeenVerified <https://www.beenverified.com>
- Black Book Online (US) <https://www.blackbookonline.info>
- BRB Pub.com <http://www.brbpub.com>
- BRB Publications <https://www.brbpublications.com>
- City Protect <https://cityprotect.com>
- DOBSEARCH <https://www.dobsearch.com>
- Echovita <https://www.echovita.com>
- Family Watchdog (US) <https://www.familywatchdog.us>
- Federal Bureau of Prisons - Inmate
- Locator (US) <http://www.bop.gov/inmateloc>
- Find A Grave (US) <https://www.findagrave.com>
- Find People Search (US) <https://findpeoplesearch.com>

- Fold3 (US Military Records) <http://www.fold3.com>
- Free Public Records Directory (US) <http://publicrecords.onlinesearches.com>
- Golookup (US) <https://golookup.com>
- GOVDATAACA (Canada) <https://govdataca.com>
- GPublic <https://qpublic.schneidercorp.com>
- Grave Info (US) <http://www.graveinfo.com>
- Inmate Locator (US) <http://www.theinmatelocator.com>
- Intelius (US) <https://www.intelius.com>
- Interment (Cemetery Records) <http://www.interment.net/data/search.htm>
- Instant Checkmate <https://www.instantcheckmate.com>
- Investigative Dashboard Search <https://aleph.occrp.org>
- Legacy.com (US) <http://www.legacy.com>
- Melissa (US) <http://melissadata.com>
- NETR ONLINE (US) <https://publicrecords.netronline.com>
- National Sex Offender Public Website (US)
<https://www.nsopw.gov/en/Search/Verification>
- ObitTree <https://obitree.com>
- Orbituaries Australia <http://oa.anu.edu.au>
- Peoplefinder (US) <https://www.peoplefinders.com>
- Peoplefinders (US) Criminal Records <https://www.peoplefinders.com/criminalrecords>
- Political MoneyLine (US) <http://www.politicalmoneyline.com>
- Public Info Directory (US) <https://publicrecords.directory>
- Public Records (Australia) <https://www.publicrecords.com.au>
- Public Record Online Searches <https://publicrecords.onlinesearches.com>
- Radaris <http://radaris.com>
- RecordsPedia <http://recordspedia.com>
- Reunion (US) <http://www.reunion.com>
- SCRA Website (US) <https://scra.dmdc.osd.mil/scra/#/home>
- Sorted by Birth Date <http://sortedbybirthdate.com>

- SSN Validator <https://www.ssnvalidator.com>
- UniCourt <https://unicourt.com>
- USSEARCH (US) <https://www.ussearch.com>
- xlek <https://xlek.com>

Как ищем

На старте сбора информации об объекте исследования может быть известно не много. При этом известная информация может оказаться не уникальной, что само по себе затрудняет поиск, информация может оказаться не точной – ошибка в произношении или написании, особенно, когда воспринимается «со слов». Часто бывает, что руководитель банально забыл, что у него есть дополнительная информация по объекту и он вам ее не дал. Например, контактный телефон, электронная почта, информация о связи объекта с другим, более известным человеком или организацией, возможно особые обстоятельства знакомства с ним.

А все это дополнительные возможности по выявлению полезной информации, которые будут упущены. Поэтому для повышения вероятности выполнения такого поручения настоятельно рекомендую в момент постановки задачи сразу уточнить дополнительные идентификаторы объекта, спросить иные данные по нему, выяснить причины интереса к нему или обстоятельства знакомства. Это серьезно расширит ваши возможности по поиску данных.

Шаг 1. Поиск в глобальных поисковиках

Начинаем с самого простого, универсального и доступного - с поисковиков (Яндекс, Goole, Байду...). Но в начале несколько прописных истин, о которых всегда не вредно напомнить.

1. Поисковые сервисы видят далеко не всё в интернете, а точнее все вместе по оценкам экспертов не более 20% интернета. Поэтому не стоит ограничиваться только поисковыми сервисами.
2. Информация из не новостных сайтов попадает в базу поисковых сервисов с опозданием, иногда в пару недель. Поэтому, когда вы обнаруживаете что-то интересное в поисковике со ссылкой на такой сайт, то перейдя по ней можете обнаружить, что информации уже нет или она изменена.
3. Источники определенной местности гораздо плотнее отслеживаются местными поисковыми сервисам, которых гораздо больше, чем Google, Яндекс, Baidu и Yahoo!. Поэтому, при углубленном изучении объекта есть смысл задействовать именно местные поисковики, которых достаточно много. Кроме того, есть специализированные поисковики, заточенные под определенную сферу, а еще есть мета-поисковые системы... в общем если вы планируете плотно работать по данному направлению, то имеет смысл изучить вопрос поглубже.

Определяемся с признаками объекта и начинаем поиск

Определяемся с тем, что знаем про объект исследования. Тут помогут любые дополнительные данные:

1. Как зовут, псевдоним, кличка, ник, аккаунт
2. Где работает, работал, учился или чем зарабатывает
3. В каком событии участвовал, к чему имеет отношение
4. Контакты от телефонов до электронных почт

Что такое ник, как его выбирают и что он нам дает. Ник представляет собой наше имя (псевдоним) в интернете: мы выбираем его, создавая свой личный почтовый ящик, а потом часто используем и в различных сервисах. Мы ничем не ограничены при выборе ника, если только не «пытаемся спрятаться», при этом есть любимые алгоритмы формирования наших интернет-псевдонимов:

1. Игры со своим именем: фамилия, имя + фамилия, имя + год рождения, имя + дата, инициалы.
2. Игры с именами любимых персонажей (tovbender, napoleon).
3. Немного о себе: профессия, психология (besthacker, murmur).
4. Демонстрация увлечений (footballer, boxer).
5. “Чтобы никто не догадался”: слово, написанное наоборот, русское слово в английской раскладке, слово на латыни и т.п.

Именно с этих данных и начнем поиск в поисковых сервисах. Итак, то, что вы знаете, то и используете в качестве поискового признака, то есть вставляем в поисковую строку и проверяем выдачу поисковика на наличие упоминания изучаемого объекта. Вначале простыми запросами. Например, вводим «Иванов Иван Иванович» и получаем очень много результатов, причем релевантных, но это всё не тот, кого мы ищем. Надо уточнять. Знаем, что он в руководстве некой строительной компании «СтройГипроМост». Добавляем этот признак в поисковую строку и объем найденной информации значительно уменьшается. Изучаем найденной, собираем новые данные.

Уже на этом шаге начинается то, о чем нередко забывают молодые исследователи:

1. Каждую новую или уточняющую информацию сразу помещайте в соответствующий раздел шаблона отчета по объекту. Вначале можно даже в виде цитат и не «причесывая». Красоту наводить будем позже.
2. Находя потенциально-полезную информацию, необходимо обязательно сохранять ссылку на нее. Самый простой способ делать это в виде сносок в формируемом файле отчета в Microsoft Word.
3. Каждая новая найденная информация является или новым поисковым признаком или уточняющим для уже известного поискового признака. И это нужно использовать для уточнения, расширения, углубления.

Не забывайте, что во многих странах есть свои, локальные социальные сервисы. И на местном уровне они не менее популярны, чем топовые сеточки, а порой гораздо лучше «ориентируются» в местном контенте. Например:

- Франция skyrock.com
- Япония line.me/en/family-apps
- Южная Корея kakaocorp.com/service
- Китай wechat.com
- Китай douyin.com
- Китай bilibili.com

Поиск по изображениям

Если удалось получить изображение объекта (фотографию), то есть смысл поискать по изображениям. Причем двумя способами:

1. Используя соответствующий раздел поисковых сервисов, но ища по уже известным идентификаторам (ФИО, место работы, контакты...) и сравнивая имеющееся изображение объекта с теми, что предлагает поисковик;
2. Используя соответствующий раздел поисковых сервисов, но ища уже именно по изображению (поиск похожих изображений)
3. Используя специализированные сервис поиска человека по фотографии:
 - search4faces.com/ - ищет в ВК, ОК, ТикТок, Клубхаус. Отдельный поиск по публичным персонам. Не очень аккуратный, но бесплатный.
 - primeyes.com/ - ищет лица ВЕЗДЕ
 - findclone.ru/searchclone - старый добрый FindClone для поиска похожих людей в ВК
 - <https://lenso.ai/ru> - это платформа обратного поиска изображений на основе искусственного интеллекта.

Использование обнаруживаемых данных или обратный поиск

Используйте «обратный поиск». Его смысл в том, что если, например, вы нашли адрес проживания объекта, то используйте в качестве критерия поиска этот самый адрес и посмотрите кто еще проживает по этому адресу. Так вы сможете найти членов семьи и родственников. Если нашли e-mail, то посмотрите, где еще фигурировала эта почта.

Если нашли ник, то это удача, только при условии, что ник не общеупотребительный. Именно этот набор символов люди применяют для самоидентификации и стараются использовать один ник в разных сервисах: в почтовых сервисах, в мессенджерах, в

соцсетях, на форумах, в играх... И это дает нам прекрасную возможность выявить места прибытия объекта в интернете, его увлечения, хобби, примеры его общения.

Например, такая ivaivaiva83@yandex.ru Обратите внимание на составную часть до «собаки» ivaivaiva83 – это тот самый ник. И весьма редкий, а значит вполне себе уникальный признак изучаемого человека. Используем этот набор символов для поиска почтовых ящиков и аккаунтов в других сервисах и для поиска информации в поисковиках.

Если есть номер мобильного, то его также нужно использовать для поиска информации об объекте. Люди оставляют свои контакты в документах, на мероприятиях, в докладах, отчетах, при регистрации юрлиц, для получения обратной связи, да мало ли еще для чего. И все это вполне может содержать полезную для вас информацию. Поэтому используем эту возможность, но не забываем, что телефоны пишут по-разному, что алгоритмы поисковиков отличаются и периодически без уведомления меняются.

Формирование сложных поисковых запросов описано в разделе «Поиск данных в интернете поисковыми сервисами», не будем повторяться.

Примеры возможностей Google в поиске данных человека. Здесь базовые варианты, а детальнее расписано в разделе "Поиск данных в интернете поисковыми сервисами" - "поисковики" - "Google dorking"

```
inurl: twitter @minregion
```

Данный запрос находит пользователя «minregion» в Twitter, убирая из поисковой выдачи результаты за пределами этой соцсети. Если вам нужно ограничить таким образом поиск другой социальной сетью, то именно ее название и вставьте вместо «twitter».

```
site:sudact.ru суходрищенко | михаил суходрищенко | бабель михаил суходрищенко
```

Ищем судебные дела, в которых участвовало изучаемое лицо. Для этого ограничим поиск сайтом, на котором агрегируются все судебные решения (СудАкт). Если у вас есть другие источники информации о судебных решениях, и вы хотите поискать именно по ним, то вставьте этот домен вместо «sudact.ru».

```
«john doe» site:instagram.com
```

Это еще один вариант использования ограничения поиска одним сайтом. В данном случае находится пользователь Инстаграма по точному имени.

```
«CV» OR «Curriculum Vitae» filetype:PDF «john» «doe»
```

Находит резюме с именами и фамилиями «john» и «doe» в формате PDF.

```
«@example.com» site:example.com
```

Находит почтовые ящики на интересующем вас домене. Соответственно нужный вам домен вставьте вместо example.com

HR «email» site:example.com filetype:csv | filetype:xls | filetype:xlsx

Находит контакты HR в формате xls, xlsx и csv на интересующем вас домене (здесь на сайте example.com).

Шаг 2. Поиск в специализированных поисковиках

Если известна сфера интересов, деятельности объекта, его хобби, увлечения и т.п., то есть смысл поискать именно в этой сфере. Для этого нужно задействовать специализированные поисковые системы. Такие специализированные системы есть под разные отрасли, не под все конечно, но под многие.

Вот примеры таких узкоспециализированных поисковиков:

- 192.com - поиск адреса человека в Великобритании, номера телефона и того, с кем он проживает, согласно спискам избирателей.
- 411.info - популярный в США сервис для поиска информации о людях, компаниях и предприятиях по имени, номеру телефона или адресу.
- base-search.net — один из мощнейших поисковиков по текстам академических исследований. Более 100 миллионов научных документов, 70% из них бесплатны.
- checkusernames.com - поиск сотен тысяч сообщений, утекших с более чем 180 серверов Discord, пропагандирующих превосходство белой расы и нацистов, от UnicornRiot
- eniro.se - желтые страницы Швеции (шведское издание).
- epieos.com - проверяет, где использовался адрес электронной почты.
- fastpeoplesearch.com - поиск человека по имени, по адресу, по телефону. В основном хорошо для США.
- hitta.se - поиск частных лиц, предоставляющих услуги. Картографический сервис для Швеции.
- namechk.com - Инструмент поиска имени пользователя и домена, который проверяет, на каких платформах или в каких доменах зарегистрировано данное имя пользователя.
- peoplefinder.com - сервис, который позволяет вам искать людей в США, используя различные критерии, включая полицейские записи, социальные сети и фотографии.
- personlookup.co.za - поиск людей и телефонов в Южной Африке.
- publicrecords.searchsystems.net - поиск информации о государственных записях в Интернете в более чем 70 000 базах данных, организованных по типу и местоположению, поможет вам найти записи о собственности, уголовных делах,

судебных разбирательствах, рождении, смерти, браке, разводе, лицензиях, актах, ипотечных кредитах, корпоративных записях, регистрации предприятий и многих других ресурсах государственных записей. Но в основном в США.

- Science.gov — американский государственный поисковик по более чем 2 200 научным сайтам. Индексируется свыше 200 миллионов статей.
- thelawpages.com/court-cases/court-case-search.php?mode=1 - Поиск подробностей уголовного дела в Великобритании, таких как приговор, слушание, ответчик и т. д.
- thisnumber.com - Международный справочник телефонных справочников «белые страницы» и «желтые страницы», а также онлайн-справочник.
- whatsmyname.app - Поиск имен пользователей на нескольких сотнях платформ
- whitepages.com - агрегатор информации о людях в США. Он предоставляет широкий спектр информации о частных лицах.
- Wiki.com создан для поиска информации исключительно на вики-сайтах. Полезен для образовательных целей, используется для написания научных трудов и исследований.

Бывает полезно осуществить поиск информации об объекте в новостях, особенно если фигура медийная и наблюдается слишком много информации. В новостниках вы получите если не ситуацию «на сейчас» то очень свежие материалы об исследуемом. Начать можно с Google-новости, Дзен-Новости. Они имеют хороший охват, но вполне пригодятся и другие подобные сервисы. Главное не забывайте обращать внимание на то, что разные сервисы отдают предпочтение разным источникам информации.

Некоторые сервисы не дают возможность скопировать контент или для прочтения полной версии требуют платной подписки. В ряде случаев это решается просмотром html кода, в котором присутствует весь необходимый текст. Самый простой способ - это воспользоваться функцией разработчика в вашем браузере. Но если нет навыков работы с html, то можно воспользоваться специализированными сервисами анализа. Вот некоторые из них:

- html.onlineviewer.net/
- codebeautify.org/htmlviewer
- jsonformatter.org/html-viewer
- smallseotools.com/html-viewer/
- static.app/html-viewer

Шаг 3. Поиск в специализированных базах данных

Существуют специализированные сайты и базы данных, которые собирают информацию о людях из различных источников. Эти ресурсы могут предоставить более детальную информацию, а иногда адреса, телефоны и судебные записи. Использование таких

ресурсов может быть особенно полезным, если вам нужна более специфическая информация. Собираем по этим источникам интересующую вас информацию, которой обогащаем отчет или расширяем его.

Интернет БД

Whitepages — один из самых известных сайтов для поиска контактной информации. Здесь можно найти адреса, номера телефонов и даже родственников человека. Используйте расширенный поиск, что может помочь найти более детальную информацию. Используйте обратный поиск: Это может помочь найти информацию по номеру телефона или адресу.

Spokeo — еще один мощный инструмент для поиска информации. Он собирает данные из социальных сетей, публичных записей и других источников. Здесь можно найти контактную информацию, фотографии и даже финансовые данные. Spokeo также предоставляет возможность поиска по имени, адресу, номеру телефона и электронной почте. Используйте все доступные параметры поиска: Это может помочь найти более детальную информацию. Проверьте социальные сети: Spokeo может предоставить ссылки на профили в социальных сетях. Используйте обратный поиск: Это может помочь найти информацию по номеру телефона или адресу.

Pipl - Поисковая система, специализирующаяся на поиске людей. Pipl собирает данные из социальных сетей, публичных записей и других источников.

BeenVerified - Сервис, предоставляющий детальную информацию о человеке. BeenVerified собирает данные из различных источников, включая социальные сети и публичные записи.

Intelius - Еще один ресурс для поиска контактной информации и публичных записей. Intelius предоставляет возможность поиска по имени, адресу, номеру телефона и электронной почте.

Государственные учеты

Сервисы раскрытия информации о юридических лицах содержит информацию и об руководителях, и об учредителях этих юридических лиц. Поэтому всегда есть смысл проверить ваш объект интереса на участие в юрлицах. Причем таких сервисов достаточно много и они раскрывают бесплатно разный объем информации, поэтому полезно сформировать для себя набор таких сервисов, которые дают разный набор данных о компаниях, что позволит обогатить свои знания как об изучаемом человеке, так и о юридических лицах с ним связанных.

Примеры сервисов, которые предоставляют такую информацию, их гораздо больше, чем три, приведенные ниже:

- pb.nalog.ru/index.html на официальном сайте ФНС есть кое-что;
- rusprofile.ru
- checko.ru
- audit-it.ru

Также будут полезны для решения этой задачи и сервисы, позволяющие искать юрлица и информацию о них в иностранных юрисдикциях:

- cylaw.org - данные о юрлицах на Кипре.
- dichvuthongtin.dkkd.gov.vn/inf/default.aspx - регистрация юрлиц во Вьетнаме.
- find-and-update.company-information.service.gov.uk - Поиск компаний и частных лиц в Великобритании и Гибралтаре.
- importyeti.com - Поиск среди записей таможи США о морских перевозках, поиск поставщиков компаний.
- kbopub.economie.fgov.be/kbopub/zoeknaamfonetischform.html - справочник юрлиц Нидерландов.
- northdata.com - Поиск компаний и людей в корпоративных и торговых реестрах ЕС.
- opencorporates.com просто БД юрлиц по миру;
- offshoreleaks.icij.org а это БД, сформированная на утечках данных о юрлицах в офшорах.
- sec.gov/edgar/search/ - База данных юрлиц и корпоративных документов для США.
- verif.com - проверка существования и платежеспособности компании во Франции
- www1.touki.or.jp/gateway.html - реестр предприятий Японии.

Информацию из подобных ресурсов целесообразно кроме как в тексте, сразу укладывать в схему. Это позволит одним взглядом «объять необъятное», а заодно выявить пробелы в информации, кого еще надо до-проверить, что уточнить, в какую сторону копнуть поглубже. Такие схемы можно создавать в специализированном ПО, например Visio. Простые схемы (до 20 узлов) можно прорисовывать в PowerPoint, в этом софте можно и достаточно красиво оформить такую схему при необходимости.

Через сервисы МВД можно узнать, действителен ли паспорт гражданина – этим могут воспользоваться владельцы квартир при сдаче их в найм. А по номеру водительского удостоверения через официальный сайт ГИБДД открывается информация о штрафах – и если человек претендует на вакансию водителя, сведения о слишком часто получаемых взысканиях вряд ли сыграют ему на руку, зато потенциальный работодатель будет предупрежден.

Информация о машине также может обнаружиться в реестре о залоге движимого имущества, который доступен на сайте Федеральной нотариальной палаты. Благодаря ему можно узнать, не находится ли авто, которое планируется купить, в залоге. На этом же ресурсе имеется реестр наследственных дел. Он позволяет узнать, жив ли человек и не является ли умерший гражданин стороной предстоящей сделки.

Если знать фамилию, имя и отчество человека, а также дату его рождения, можно поискать данные в базе судебных приставов – там отражена информация о долгах и делопроизводствах, открытых в его отношении.

На сайте Минюста есть реестр адвокатов с данными об их удостоверениях и статусе. К нему могут обращаться граждане, которые нуждаются в юридической помощи и планируют воспользоваться услугами специалиста. Реестр поможет предотвратить ситуацию, в которой представлением интересов клиента будет заниматься адвокат, чей статус прекращен.

Образовательные организации публикуют списки своих учащихся, а на сайтах компаний можно обнаружить перечни их сотрудников. Зачастую достаточно знать фамилию, имя и отчество человека, чтобы проследить его трудовой путь, узнать, в каких предметных олимпиадах он участвовал во время учебы, и где работает сейчас.

opensanctions.org - международная база данных о санкциях, лицах, представляющих интерес, и политически значимых лицах.

sanctionsexplorer.org - База данных санкций OFAC/ООН/ЕС.

Судебные решения

Интерес представляют и реестры судебных решений разных стран. Вот примеры некоторых из них:

- decision.coj.go.th - судебные решения Таиланда.
- judyrecords.com - судебные решения США.
- riigiteataja.ee/kohtulahendid/koik_menetlused.html - судебные решения Эстонии.
- saos.org.pl/search - судебные решения Польши
- supreme.court.gov.il/Pages/fullsearch.aspx - решения Израильского высшего судебного органа.
- splcgk.court.gov.cn/lcgkw/user# - судебные решения Китайских провинций.
- uitspraken.rechtspraak.nl - судебные решения Нидерландов.
- wenshu.court.gov.cn - судебные решения в Китае.

Пропавшие без вести

- Child Rescue <https://www.childrescue.eu>
- DOE Network <http://www.doenetwork.org>
- FBI: Kidnappings and Missing Persons <https://www.fbi.gov/wanted/kidnap>
- Global Missing Kids <https://globalmissingkids.org>
- International Centre for Missing and Exploited Children <https://www.icmec.org>

- International Commission on Missing Persons <https://www.icmp.int>
- Interpol: Yellow Notices <https://www.interpol.int/How-we-work/Notices/View->
- Yellow-Notices LOST <https://lost.team>
- Missing Children Europe <https://missingchildreneurope.eu>
- Missing Kids <https://www.missingkids.org>
- Missing People <https://www.missingpeople.org.uk>
- Missing Persons <https://www.missingpersons.ie>
- Missing Persons Australia <https://missingpersons.gov.au>
- Missing You <https://missing-you.net>
- NamUs <https://www.namus.gov>
- National Center for Missing and Exploited Children <https://www.missingkids.org>
- Polly Klaas Foundation <http://www.pollyklaas.org>
- Restoring Family Links <https://familylinks.icrc.org>
- South African Centre for Missing and Exploited Children <http://www.missingkids.co.za>
- UK Police Missing Persons <https://www.missingpersons.police.uk>

Шаг 4. Поиск в соц-сервисах

Учитывая, что люди всё больше «погружаются» в соцсети, всегда есть смысл поискать в соцсетях дополнительные данные об исследуемом объекте. Если известно в каких соцсетях обитает исследуемый, то хорошо, если не известно, то начинаем с наиболее популярных сервисов.

Есть и сервисы, ищущие сразу по нескольким социальным сетям одновременно. Вначале, если вы не знаете где обитает ваш объект интереса, задействуйте именно такие сервисы:

- pipl.com
- spokeo.com
- thatsthem.com
- beenverified.com
- fastpeoplesearch.com
- truepeoplesearch.com
- familytreenow.com

Далее нужно собирать полезную информацию уже непосредственно в соцсетях и задействуя внутренние поисковые ресурсы каждой соцсети.

Google Dorks для поиска в соцсетях

```
Суходрищенко Абам site:SOCIAL NETWORK URL 1 | site:SOCIAL NETWORK URL 2 | site:SOCIAL NETWORK URL 3
```

В поле site: введите URL платформы социальных сетей вместо «SOCIAL NETWORK URL 1», которые вы хотите исследовать, а вместо «Суходрищенко Абам» фамилию и имя изучаемого объекта. Первые несколько списков вернут все учетные записи, связанные с темой на этих платформах. Углубившись в результаты поиска, вы можете найти упоминания определенных постов, видео и комментариев.

```
site:twitter.com
```

Если нужно найти кто еще распространял данный контент. «ЦИТАТА» – какую цитату ищем. Знак минус указывает Google игнорировать все, что опубликовано из исходной социальной сети. Это также может помочь следователям OSINT определить, публиковали ли другие сайты, такие как СМИ или личные блоги, определенный пост в другом месте.

```
«john doe» -«site:instagram.com/johndoe» site:instagram.com
```

А в данном случае вы не только ограничиваете поиск одним сайтом, но и удаляете из результатов поиска посты самого пользователя, но при этом остаются его комментарии под постами других аккаунтов.

```
«john» «doe» -site:instagram.com
```

Такой вариант находит пользователя вне Инстаграма по точному имени и фамилии в разных комбинациях – из поисковой выдачи удаляются все ссылки на страницы инстаграмма.

Шаг 5. Поиск контактов

Поиск контактов и по выявленным контактам осуществляется как через глобальные поисковые сервисы, так и в специализированных сервисах.

Поиск телефона

- telefonny.zoznam.sk - телефонный справочник Словакии.
- ukphonebook.com - телефонный справочник Великобритании.

- whocalledme.com - Если объект исследования находится в Америке или Европе, используйте данный сервис с базами абонентов.
- whitepages.com - поиск телефонов, людей, биографических отчетов в США.

Google Dorks для поиска телефонов

```
filetype:csv OR filetype:xls OR filetype:xlsx "phone" "First Name" "Last Name" "Company" -sample 2020 "website" -template "contacts"
```

Найдет рабочие номера телефонов

Поиск почты

- Hunter.io — сканирует домен на наличие почтовых ящиков и показывает схемы между ними;
- Email permutator — генерирует комбинации названий почтовых ящиков из имен, фамилий, прозвищ и доменов;
- Proofy — проверяет существование электронной почты. Удобно использовать при наличии сгенерированного списка email-адресов. Можно проверять сразу несколько ящиков.
- Verifalia — тоже проверяет существование той или иной электронной почты. В бесплатном варианте без регистрации сверяет адреса по одному. Если зарегистрируетесь, сможете прогонять сразу несколько.
- Osint.industries - Введите адрес электронной почты или номер телефона интересующего вас лица и получите целый список веб-сайтов, связанных с объектом исследования, а также имена реальных людей, стоящих за именами пользователей и скрытыми цифровыми следами. «Если у вас есть номер телефона или адрес электронной почты, то с его помощью можно найти любые учётные записи, зарегистрированные на них».

Google Dorks для поиска почты

Так-же не забывайте о возможностях глобальных поисковых сервисов, в частности Google Dorks.

```
«@example.com» site:example.com
```

находит почтовые ящики на определенном домене.

```
HR «email» site:example.com filetype:csv | filetype:xls | filetype:xlsx
```

находит контакты HR в формате xls, xlsx и csv на определенном домене.

```
site:example.com intext:@gmail.com filetype:xls
```

вытаскивает ID электронных почтовых ящиков (в данном случае Gmail) из определенного домена.

```
filetype:csv OR filetype:xls OR filetype:xlsx "email" "@" "First Name" "Last Name" "Company" -sample 2020 "website" -template "contacts"
```

находит рабочие адреса электронной почты

Шаг 6. Установка местоположения

Вначале обзор методов установления локации по фотографии. Каждый из этих методов может быть использован отдельно или в комбинации для более точного определения местоположения фотографии. Успех зависит от доступности данных, качества изображения и наличия визуальных подсказок.

1-Использование реверсивного поиска изображений

- Google Images и Яндекс Картинки. Загрузка фотографии в эти поисковые системы позволяет найти похожие изображения и, возможно, идентифицировать место. Если результаты не удовлетворительные, можно вырезать часть изображения (например, здание) и повторить поиск.
- Lenso.ai Этот инструмент также предлагает реверсивный поиск изображений с возможностью фильтрации по категориям, что может помочь в нахождении местоположения.
- TinEye. Специализированный сервис для обратного поиска изображений, который может предоставить информацию о других местах, где это изображение использовалось.

2-Анализ EXIF-данных (метаданных)

Если фотография содержит метаданные EXIF, можно извлечь информацию о GPS-координатах, времени съемки и настройках камеры. Это самый прямой способ узнать местоположение, если данные не были удалены. Но глобальные соцсети удаляют эти данные из медиа-файлов из соображений экономии места.

Для анализа мета-данных можно использовать следующие программы:

- ExifTool - Мощная программа командной строки для чтения, редактирования и удаления EXIF-данных.
- Exif Pilot Pro - Удобный интерфейс для просмотра и редактирования EXIF и IPTC данных.

- jExifToolGUI Графический интерфейс для работы с ExifTool, кроссплатформенное приложение.

3-Сравнение с картами и панорамами

- Google Maps и Street View: С помощью этих инструментов можно сопоставить фотографию с картами и панорамами местности. Например, можно определить, из какого здания сделан снимок, сравнивая его внешний вид с изображениями на картах.
- Спутниковые снимки: Использование спутниковых карт позволяет детально рассмотреть поверхность местности и сопоставить её с фотографией.

4-Визуальные подсказки

- Архитектурные элементы: Узнаваемые здания, памятники, парковые комплексы, специфические конструкции могут указать на конкретное место. Например, Эйфелева башня, Останкинская башня или Колизей легко идентифицируются. Также есть смысл обратить внимание на общий стиль зданий и их оформление, на преобладающие цвета и элементы декора зданий.
- Надписи и вывески: Язык на вывесках или дорожные знаки могут помочь определить страну или регион. Вывески на остановках, магазинах, заправках, вокзалах также дают много информации. Например, надписи на кириллице укажут на русскоязычные страны.
- Природные особенности: Ландшафт, тип растительности также могут дать подсказки о местоположении. Особое внимание тут стоит уделить горным массивам, особым формам природных образований. Например, тропические растения могут указывать на экваториальные регионы.
- Климатические условия. Погода на фотографии (например, снежный пейзаж или солнечный пляж) может дать подсказки о сезоне и географическом положении.
- Дорожная разметка и транспортные средства. Номерные знаки автомобилей, типичные для определенных стран, а также особенности дорожной разметки могут помочь в определении местоположения.

5-Анализ теней и положения солнца

Этот метод включает использование времени съемки для анализа длины теней на фотографии. Сопоставив это с географическими данными о положении солнца в определенном момент времени, можно уточнить координаты места съемки.

SunCalc – инструмент для анализа положения солнца в определенное время и месте.

6-Социальные сети и сообщества

Поиск в социальных сетях может дать результаты, если кто-то уже делал публикации из того же места. Иногда пользователи оставляют геотеги или упоминают название места в своих постах. Бесплатный инструмент Creepy <http://www.geocreepy.com/> определяет месторасположение на основе данных из социальных сетей и сайтов с изображениями. Сервис Echosec <https://www.echosec.net/> умеет схожее, но он платный: месячная подписка на него обойдется в \$500. Исключения есть для журналистов и работников НПО.

Недвижимость

- 411.com (US) <https://www.411.com/reverse-address>
- Airbnb <https://www.airbnb.co.uk>
- Arivify (US) <https://www.arivify.com>
- Ananz <http://www.ananzi.co.za>
- Bigger Pockets <https://www.biggerpockets.com/rei>
- Black Book Online: USA Property <https://www.blackbookonline.info/USA-Property.aspx>
- BlueBook International <http://www.bluebook.net>
- Bret Whissel Amortization Calculator <http://bretwhissel.net/amortization>
- Carmel Realty Company (CN) <http://www.carmelrealtycompany.cn/real-estate-listings-Carmel.htm>
- CBRE (Global) <https://www.cbre.us>
- Central 21 (Global) <https://www.century21.com>
- Colliers International <https://www2.colliers.com>
- CouchSurfing <https://www.couchsurfing.com>
- Courthouse Direct (US) <https://www.courthousedirect.com>
- Digma Real Estate Tools & Analysis <https://www.digma.com/solutions/real-estate-analysis>
- Domain AU Home Price Guide <https://www.domain.com.au/property-profile>
- Emporis <https://www.emporis.com>
- EuroResales <http://www.euroresales.com>
- FixMyStreet (UK) <https://www.fixmystreet.com>
- Freddie Mac <http://www.freddiemac.com/research>
- Funda (NL) <https://www.funda.nl>

- HomeFacts (US) <https://www.homefacts.com>
- HomeMetry (US) <https://homemetry.com>
- HouseShop (UK) <https://www.thehouseshop.com>
- iLocate (NL) <https://www.ilocate.nl>
- Institute for Real Estate Management <http://www.irem.org>
- Jaap (NL) <https://www.jaap.nl>
- Land.net (US) <http://www.land.net>
- LondonRentMyHouse <http://www.londonrentmyhouse.com>
- Loopnet (US) <http://www.loopnet.com>
- Melissa Address Lookups
<https://www.melissa.com/v2/lookups/addresssearch/?number=4805&zip=50510&c=1&l=U>
- National Association of Realtors Directory of Real Estate Research Centers
<https://www.nar.realtor/directories/directory-of-real-estateresearch-centers>
- National Association of Realtors Research Reports <https://www.nar.realtor/research-and-statistics/researchreports>
- Placester Multiple Listing Service (MLS) Directory (US) <https://placester.com/mls-directory>
- PadMapper (US) <https://www.padmapper.com>
- People Looker (US) <https://www.peoplelooker.com>
- Radaris: Property Check <https://radaris.com/#findAddrH>
- Realestate.com.au (AU) <https://www.realestate.com.au>
- Realtor <https://www.realtor.com>
- Redfin (US) <https://www.redfin.com>
- Rehold (US) <https://rehold.com>
- Remax Global <https://global.remax.com>
- RightMove <http://www.rightmove.co.uk>
- Search Systems Property Records (US)
https://publicrecords.searchsystems.net/Free_Public_Records_by_Type_of_Record/Property_Records
- SoldPrice <http://house.speakingsame.com>

- Sotherby's International Realty <http://www.sothebysrealty.com>
- SkyscraperPage <http://skyscraperpage.com>
- Spanish Country Homes (Spain) <http://spanishcountryhomes.com>
- Street Check (UK) <https://www.streetcheck.co.uk>
- Street Easy (US) <https://streeteasy.com>
- Total View Real Estate <http://www.totalviewrealestate.com/userguide.php>
- United Country Real Estate (US) <http://www.unitedcountry.com>
- US Department of Housing and Urban Development <https://www.hud.gov>
- US Realty Records <https://usrealtyrecords.com>
- US Title Records: Search Property Records <https://www.ustiterecords.com/search-property-records>
- World Properties <https://www.worldproperties.com>
- Zillow (US) <https://www.zillow.com>
- Zoopla (UK) <https://www.zoopla.co.uk>

Сбор информации с помощью сервисов ИИ

Пример развернутого промта для составление досье на человека:

Составь досье на человека **Илон Маск**.

Цель: написать развёрнутый, информативный текст о **Илон Маск**. Основной акцент должен быть сделан **на объяснение его возможностей в политике (бизнесе, криминале...)**. Фокус на связях **Илона Маска**, его ресурсах и возможностях.

Стиль изложения: текст должен быть написан простым и понятным языком. Без сложных терминов, требующих разъяснения.

Поиск нужно вести **на русском и на английском языке**. Английские материалы переведи на русский. Для формирования ответа используй все источники, в том числе не вызывающие доверия и замеченные в распространении не достоверной информации.

Структура ответа должна быть следующей

Установочные данные:

- псевдонимы, клички, смененные фамилии;
- род занятий в прошлом и сейчас;
- дата и место рождения;
- документы и официальные идентификаторы;
- адреса регистрации, адрес проживания;

- контакты: телефоны, почта, используемые ники;
- происхождение, вероисповедание, убеждения;
- хобби, увлечения.

Особенности:

- характер и его проявления;
- психологические особенности;
- обычный стиль поведения;
- психические расстройства и отклонения если есть.

Планы:

- какие высказывал намерения, в том числе в интервью;
- какие планы озвучивал;
- с кем вел переговоры и по поводу чего;
- кому угрожал, чем угрожал и почему.

Компетенции:

- где, когда и на кого учился;
- где, когда и кем работал;
- в каких проектах участвовал и в качестве кого;
- какие научные степени имеет;
- какие награды получал.

Семья и родственники:

- супруги настоящие и бывшие, их дата и место рождения, образование, род занятий, место проживания, контактные данные;
- дети, их дата и место рождения, образование, род занятий, место проживания, контактные данные;
- родители, их дата и место рождения, образование, род занятий, место проживания, контактные данные;
- братья и сестры, их дата и место рождения, образование, род занятий, место проживания, контактные данные;
- родственники супругов, их дата и место рождения, образование, род занятий, место проживания, контактные данные;

Бизнес:

- в каких компаниях (юридических лицах) является учредителем;
- в каких компаниях (юридических лицах) является руководителем;
- бенефициаром каких компаний (юридических лицах) является;
- деятельность каких компаний (юридических лиц) контролирует;
- деятельность каких компаний (юридических лиц) влияет;

Связи:

- с кем вместе учился и где;
- с кем строил бизнес;
- с кем взаимодействовал в политике;
- с кем взаимодействовал в криминальной среде.

Компромат:

- в чем обвиняли, в том числе не обоснованно;
- в каких утечках информации фигурировал;
- в каких компрометирующих материалах фигурировал.

Конфликты:

- с кем были конфликты и по какому поводу,
- в каких уголовных делах фигурировал,
- в каких судебных разбирательствах участвовал,
- какие угрозы получал;
- в каких санкционных списках фигурирует, в связи с чем.

Методика сбора информации об организации

Термин «организация» в данном случае рассматривается как «устойчивая группа лиц, взаимодействующих друг с другом с помощью материальных, экономических, правовых и других условий ради решения имеющихся проблем или достижения поставленных целей». Под это определение подпадают как юридические лица, так и неформальные объединения, так и ОПГ, и государства, и межгосударственные образования. Методика их изучения очень схожая.

Что ищем

Нам, по какойто причине стало важно исследовать некую организацию. Для простоты начнем именно с юридического лица, причем коммерческой направленности. И начинаем именно с причины нашего интереса к организации так как этот интерес становится определяющим в выборе тактики исследования.

Предположим, что это юридическое лицо рассматривается вашим заказчиком в качестве клиента, причем со значительной кредитной линией. Что в этом случае важно знать бизнесу о таком клиенте до оформления с ним отношений? В первую очередь – не будет ли с этим клиентом проблем:

1. В формате финансовых потерь;
2. В формате правовых осложнений;
3. В формате криминальных разборок.

И именно на определение вероятности таких последствий направлено изучение потенциального клиента. Теперь нужно понять каким образом (по каким признакам) мы можем оценить вероятности таких последствий. Чаще всего информация, указывающая на такое, может находиться в:

1. Прошлом исследуемой организации, участии ее в событиях и процессах;
2. В особенностях лиц ее создавших, контролирующих, влияющих на ее деятельность;

3. В ее связях коммерческих и не коммерческих;
4. В ее ресурсах, особенно административных;

Как ищем

Шаг 1. Поиск в глобальных поисковиках

Начинаем с самого простого, универсального и доступного, как и в случае с изучением человека - с глобальных поисковиков (Яндекс, Goole, Байду...). Методика та-же самая, в качестве ключевых слов используются идентификаторы организации.

Начинаем также с названия организации (всех вариантов написания) и не забываем, что для сбора информации о компании в России искать нужно на русском языке, если объект интереса в США, то начать можно с русского языка, но в дальнейшем искать на английском, если объект в Китае, то вам придется таки окунуться в прекрасный и дивный мир иероглифов.

Анализируйте активность компании в Facebook, Instagram, LinkedIn и других платформах, чтобы понять ее маркетинговые стратегии. Для этого нужно изучить официальные страницы компании в соцсетях.

Официальные новости, пресс-релизы, заявления и интервью топ-менеджеров компании также являются источником полезной информации как о структуре изучаемой организации, ее ресурсах, так и о ее планах.

Шаг 2. Изучение сайта организации

Сайт организации — это ее визитная карточка, резюме и рекламная площадка одновременно. Именно из понимания этого предназначения и имеет смысл исследовать сайт организации. В разделе «О нас» («О кампании») можно найти краткое описание организации и ее историю. Конечно-же, выхолощенную, но это то, с чего можно начать анализ «биографии» организации.

В разделе «Команда» вы найдете часть, а иногда всех, сотрудников данной организации. С высокой вероятностью с фотографией и краткой биографией или как минимум с компетенциями. Тоже хорошая стартовая информация.

Раздел «Контакты» даст вам официальные контактные данные изучаемой организации, а возможно и список филиалов и отделений. По сути, географическую структуру организации.

В разделе «Продукция» («Услуги») изучаемая организация уже сформировала для вас перечень того, что она предлагает клиентам. С кратким описанием, ценами и особенностями.

Помимо традиционных разделов, часто на сайте размещают и другие, нередко несущие дополнительную потенциально интересную информацию. Поэтому всегда есть смысл изучить эти разделы.

Крайне полезно бывает посмотреть, как соответствующие разделы сайта организации выглядели раньше. Это помогает для выявления скрываемых связей организации и ее бывших сотрудников, конфликтов, в которых участвовала организация, какой продукцией занималась раньше, в каких проектах участвовала.

Структура и дизайн сайта может дать понимание ее целевой аудитории и ее маркетинговой стратегии.

Инструменты анализа

Инструменты для технического анализа сайта организации.

Ahrefs

- Анализ входящих ссылок и их качества.
- Выявление наиболее популярного контента по ключевым словам.
- Проверка позиций сайта в поисковых системах

Semrush

- Анализ поисковой выдачи, платной рекламы и контекстно-медийной рекламы.
- Проверка ключевых слов и обратных ссылок.
- Поддержка русского языка.

SimilarWeb

- Анализ трафика сайта, источников и структуры.
- Оценка перформанса конкурентов в интернете.

What Runs Where

- Мониторинг интернет-рекламы конкурентов в разных рекламных сетях.
- Определение эффективных рекламных площадок и креативов

SpyFu

- Анализ ключевых слов и рекламных кампаний конкурентов.
- Оценка органического и платного трафика.

Google Alerts

- Мониторинг упоминаний конкурентов в интернете.
- Получение уведомлений о новых публикациях.

Woorank

- Анализ и оптимизация сайта, включая SEO и технические аспекты.
- Бенчмаркинг с конкурентами.

Исследование доменов

- Access Check <https://accesscheck.thenetmonitor.org>
- AFRINIC <https://www.afrinic.net>
- APNIC <https://www.apnic.net>
- ARIN <https://www.arin.net>
- Aware Online: Website Search Tool <https://www.aware-online.com/osint-tools/websitesearch-tool>
- Better Whois <http://www.betterwhois.com>
- Central Ops <http://centralops.net>
- Complete DNS <https://completedns.com>
- Daily Changes <http://dailychanges.domaintools.com>
- Danger Zone <https://github.com/woj-ciech/Danger-zone>
- Da.whois <https://dawhois.com>
- Dedicated or Not <http://dedicatedornot.com>
- Denic web whois <https://www.denic.de/webwhois>
- DNSDumpster <https://dnsdumpster.com>
- DNS History <http://dnshistory.org>

- DNS Lookup <https://dnslookup.online>
- DNSlytics <https://dnslytics.com>
- dnspop <https://github.com/bitquark/dnspop>
- DNS Queries <https://www.dnsqueries.com>
- dnsrecon <https://github.com/darkoperator/dnsrecon>
- DNS Root Instances <https://atlas.ripe.net/results/maps/root-instances>
- DNSSec Analyzer <https://dnssec-analyzer.verisignlabs.com>
- DNS Spy <https://dnsspy.io>
- DNSStuff <http://www.dnsstuff.com>
- DNSTools <http://www.dnstools.ch>
- DNS Trails <http://dnstrails.com>
- DNS Trails <https://securitytrails.com/dns-trails>
- dnstwist <https://github.com/elceef/dnstwist>
- dnstwist <https://dnstwist.it>
- dnstwister <https://dnstwister.report>
- DNSViz <http://dnsviz.net>
- Domain Big Data <http://domainbigdata.com>
- Domain Crawler <http://www.domaincrawler.com>
- Domain Dossier <http://centralops.net/co/DomainDossier.aspx>
- Domain Eye <https://domaineye.com>
- DomainIQ <https://www.domainiq.com>
- Domain SDB <https://domainsdb.info>
- Domain To IP Converter <http://domaintoipconverter.com>
- Domain Tools <https://www.domaintools.com>
- Domain Tools <http://whois.domaintools.com>
- DomEye <https://xaviesteve.com/domeye>
- downdetector <http://downdetector.com>
- downforeveryoneorjustme <http://downforeveryoneorjustme.com>

- DNS Checker <https://dnschecker.org>
- DShield API <https://isc.sans.edu/api>
- EasyCounter WHOis <https://whois.easycounter.com>
- Easy whois <https://www.easywhois.com>
- Educause Whois Lookup <https://net.educause.edu/whois.htm>
- EURid <https://eurid.eu>
- Fierce-domain-scanner <https://github.com/davidpepper/fierce-domainscanner>
- Gaijin.at <https://www.gaijin.at/en/tools>
- gdns <https://github.com/hrbrmstr/gdns>
- Geektools <http://www.geektools.com/whois.php>
- GeoPeeker <https://geopeeker.com>
- GoDaddy WHOis <https://ca.godaddy.com/whois>
- GooHak <https://github.com/1N3/Goohak>
- GraphyStories <http://app.graphystories.com>
- GSuite Toolbox Check MX <https://toolbox.googleapps.com/apps/checkmx>
- GSuite Toolbox Dig (DNSS Lookup) <https://toolbox.googleapps.com/apps/dig>
- HackerTarget <https://hackertarget.com/ip-tools>
- Hexillion <http://hexillion.com>
- Hold Integrity IDN Checker <https://holdintegrity.com/checker>
- IANA <https://www.iana.org>
- Icann Lookup <https://lookup.icann.org>
- InfoByIp (Bulk Domain & IP Lookup) <https://www.infobyip.com/ipbulklookup.php>
- IntelligenceX: Domain <https://intelx.io/tools?tab=domain>
- intoDNS <http://www.intodns.com>
- InterNIC Whois <http://www.internic.net/whois.html>
- iwantmyname <https://iwantmyname.com>
- knockknock <https://github.com/harleo/knockknock>
- Kloth <http://www.kloth.net/services>

- LACNIC <http://www.lacnic.net>
- Lookup ICANN <https://lookup.icann.org>
- Maltego <https://www.paterva.com/web7>
- mnemonic <https://passivedns.mnemonic.no>
- MXToolbox <https://mxtoolbox.com>
- Netbootcamp Website Investigator <http://netbootcamp.org/websitetool.html>
- Network Solutions Whois <https://www.networksolutions.com/whois>
- Network Tools <http://network-tools.com>
- NS.Tools <https://ns.tools>
- Onyphe <https://www.onyphe.io>
- OpenData Rapid7 <https://opendata.rapid7.com>
- The Prefix Whois Project <https://pwhois.org>
- PTRArchive <http://ptrarchive.com>
- Purplepee.com <https://purplepee.co>
- RedirectDetective <http://redirectdetective.com>
- Reverse IP to Domain Lookup <http://www.ipfingerprints.com/reverseip.php>
- RIPE NCC <https://www.ripe.net>
- Robtex <https://www.robtex.com>
- SecurityTrails <https://securitytrails.com>
- Shodan <https://www.shodan.io>
- SIDN <https://www.sidn.nl>
- SpyOnWeb <http://spyonweb.com>
- Spyse_ <https://spyse.com>
- Sucuri Free Website and Malware Scanner <https://sitecheck.sucuri.net>
- Symantec WebPulse Site Review Request <https://sitereview.bluecoat.com>
- SynapsInt <https://synapsint.com>
- Tucows Domains <https://www.tucowsdomains.com>
- urlscan <https://urlscan.io>

- Utrace <http://en.utrace.de>
- Verisign <http://dnssec-debugger.verisignlabs.com>
- ViewDNS <http://viewdns.info>
- W3bin.com <https://w3bin.com>
- W3dt <https://w3dt.net>
- w3snoop <http://webboar.com.w3snoop.com>
- Whatsmydns.net <https://www.whatsmydns.net>
- Who.is <https://who.is>
- Whois <https://www.whois.com>
- Whois Amped <https://whoisamped.com>
- Whois Arin Online <https://whois.arin.net>
- WhoIsHostingThis <http://www.whoishostingthis.com>
- WHOis.net <https://whois.net>
- Whoisology <https://whoisology.com>
- WhoIsRequest <http://whoisrequest.com>
- Whois.Search <https://whois-search.com>
- WhoisXMLAPI <https://www.whoisxmlapi.com>
- Whoxy <https://www.whoxy.com>
- You Get Signal <http://www.yougetsignal.com>

Шаг 3. Поиск в специализированных поисковых сервисах

Официальные данные юрлица можно найти только в соответствующих сервисах госорганов. Кроме факта существования организации, в таких сервисах вы найдете установочные данные, данные о руководителе, месте регистрации, учредителях. А это всё связи, которые желательно сразу отображать в виде схемы (диаграммы) связей.

Официальные данные о компаниях в России

Сведения из ЕГРЮЛ

- <https://egrul.nalog.ru/index.html>

Сведения о юридических лицах и индивидуальных предпринимателях, в отношении которых представлены документы для государственной регистрации

- <https://service.nalog.ru/uwsfind.do>

Реестр дисквалифицированных лиц

- <https://service.nalog.ru/disqualified.do>

Решения регистрирующих органов о предстоящем исключении недействующих юрлиц из ЕГРЮЛ

- <https://www.vestnik-gosreg.ru/>

Реестр субсидиарных ответчиков

- <https://www.nalog.gov.ru/rn77/rso/>

Сервис позволяет проверять контрагента на наличие связей с лицами, которые намеренно уклонялись от исполнения обязательств или довели компанию до банкротства.

Реестр обеспечительных мер

- <https://service.nalog.ru/rom/>

Содержит информацию о наложении ареста на имущество; о запрете на отчуждение (передачу в залог) без согласия налогового органа; об отмене/прекращении действия таких решений; об имуществе, находящемся в залоге у налогового органа.

Реестр недобросовестных поставщиков

- <https://zakupki.gov.ru/epz/dishonestsupplier/search/results.html>

Отображает сведения из разных реестров: недобросовестных поставщиков (подрядчиков, исполнителей) по 44-ФЗ; недобросовестных поставщиков по 223-ФЗ; недобросовестных подрядных организаций по ПП РФ 615.

Реестр юридически значимых сведений о фактах деятельности юрлиц

- <https://fedresurs.ru/>

Ресурс позволяет ознакомиться со сведениями о деятельности субъектов экономической деятельности.

Бывает полезно узнать зарегистрированные товарные знаки, бренды, логотипы изучаемой организации. Это позволяет, помимо прочего, выяснить «родственные» организации, неочевидные связи между ними и т.п. Для США источниками такой информации являются следующие сервисы:

- Логотипы компаний companieslogo.com
- Товарные знаки tmsearch.uspto.gov/search/search-information

Неофициальные данные о компаниях

Для компаний в РФ такими источниками являются разнообразные «сервисы проверки контрагентов». Например:

- rusprofile.ru
- audit-it.ru

Для изучения компаний по всему миру:

- opencorporates.com
- offshoreleaks.icij.org
- openownership.org

subsidytracker.goodjobsfirst.org

Эту базу данных можно использовать для понимания дочерних компаний корпораций, но поисковая система была создана для отслеживания субсидий на экономическое развитие, а также других форм государственной финансовой помощи бизнесу.

Данные о компаниях в мире

Некоторые примеры таких сервисов:

- Business Reference Services <http://www.loc.gov/rr/business/company/directories.html>
- Company Research Resources by Country <http://www.rba.co.uk/sources/registers.htm>
- Overseas Company Registers <https://www.gov.uk/government/publications/overseas-registries/overseas-registries>
- AllStocksLinks <http://www.allstocks.com/links>

- Annual Reports <http://www.annualreports.com>
- Automata <https://miner.byautomata.io>
- bikudo <https://www.bikudo.com>
- Comparably <https://www.comparably.com>
- Corporate Information <http://www.corporateinformation.com>
- Corporation Wiki <https://www.corporationwiki.com>
- CorpWatch <http://www.corpwatch.org>
- Dato Capital <https://en.datocapital.com>
- Europages <http://www.europages.co.uk>
- Ezilon <http://www.ezilon.com>
- infobel <https://www.infobel.com>
- iSpionage <https://www.ispionage.com>
- Mapped in Israel <https://mappedinisrael.com>
- National Company Registers https://en.wikipedia.org/wiki/List_of_company_registers
- National Corporation Directory <https://corporation.directory/secstates>
- North Data <https://www.northdata.de>
- Opencorporates <https://opencorporates.com>
- Report Linker <https://www.reportlinker.com>
- ThomasNet <https://www.thomasnet.com>
- Vault <http://www.vault.com>
- Xing <http://www.xing.com>
- Yelp <https://www.yelp.com>
- Zaub Corp <https://www.zaubacorp.com>

Поиск компаний по некоторым странам:

Аргентина

- datos.jus.gob.ar
- bolsar.com/VistasDL/PaginaPrincipal.aspx

- informemultiburo.com/busquedaonline
- www2.jus.gov.ar/igj-homonimia/Principal.aspx
- nosis.com/es
- comprar.gob.ar
- boletinoficial.gob.ar
- reddeboletines.gob.ar
- afip.gob.ar/home/index.html
- audiencias.mininterior.gob.ar
- interactivos.lanacion.com.ar/declaraciones-juradas/#pd=0
- inpi.gov.ar
- cij.gov.ar/sentencias.html
- csjn.gov.ar

Китай

- gsxt.gov.cn/index.html - Кредитно-информационная система Китая
- wenshu.court.gov.cn - Судебные решения региональных судов Китая
- cninfo.com.cn/new/index - Финансовые отчеты публичных компаний
- qcc.com - Частный информационный агрегатор
- aei.org/china-global-investment-tracker - Интерактивный трекер зарубежных инвестиций и строительства Китая
- thereoplesmap.net - Карта внешних интересов Китая по инициативе «Один пояс, один путь»

ОАЭ

- per.economy.ae/Search_By_VN.aspx Наличие в реестре по названию на английском или арабском
- eservices.ajmanned.ae/en/tradename Наличие в реестре по названию на английском или арабском
- per.economy.ae/BASearch.aspx Хозяйственность компании

- tamm.abudhabi/wb/ded/tahaqaq/reference-number Наличие лицензии
- ner.economy.ae/Search_By_BN.aspx Национальный экономический реестр
- sca.gov.ae/en/open-data/licensed-companies.aspx#page=1 Управление ценными бумагами и товарными средствами
- adbc.abudhabi.ae/CitizenAccess/Welcome.aspx Департамент экономического развития Абу-Даби
- adx.ae/English/Securities/Pages/ListedCompanies.aspx Биржа ценных бумаг Абу-Даби
- dfsa.ae Управление финансовых услуг Дубая
- dafz.ae/en/ Каталог компаний свободной экономической зоны Дубая
- dmcc.ae/business-search Дубайский мультитоварный центр
- fujairahfreetradezone.com/appdir/company-listing.php Компании свободной торговой зоны Фуджейры
- sharjah.gov.ae/BusinessDirectory/Index Торгово-промышленная палата Шарджи.
- difc.ae/business/public-register DIFC Public Register
- flagma.ae/en/companies/dubai/ FLAGMA Companies Search in Dubai
- ae.bizdirlib.com/ United Arab Emirates Business Database
- eservices.dubaitrade.ae/clientdirectory/clientsSearch.do Dubai Trade Client Directory
- digital.abudhabichamber.ae/portal/#/commercial-directory ADCCI Commercial Directory
- adgm.com/public-registers ADGM Public Registers
- uaqchamber.ae/ UAQ Chamber
- eservices.sedd.ae/eservicesweb/license-transactions/search_license/main-inq-lic.xhtml SEDD Search for license
- dcciinfo.ae/ Dubai Chamber Commercial Directory
- dubaicareers.ae/en/Pages/default.aspx Dubai Careers
- dubaipulse.gov.ae/organisation/dld Dubai Land Department
- moec.gov.ae/en/moe-opendata Access a repository of open data from the Ministry of Economy
- adjd.gov.ae/sites/eservices/en/pages/judgments.aspx ADJD courts Judgments' Publication
- icp.gov.ae/en/services/priority-services/id-card-status/ ID Card Status

- adjd.gov.ae/sites/eServices/EN/Pages/CaseStudyEnquiry.aspx Criminal Cases Status Inquiry

США

- coordinatedlegal.com/SecretaryOfState.html#Related Информацию об американских компаниях можно найти на сайтах государственных секретарей США
- sec.gov Информацию о публичных компаниях можно найти на сайте Комиссии по ценным бумагам и биржам США
- sec.gov/edgar/searchedgar/companysearch.html поиск компании
- bbb.org/search поиск информации о предприятиях
- coordinatedlegal.com/SecretaryOfState.html#Related Регистрация по штатам

Турция

- bilgibankasi.ito.org.tr/tr/bilgi-bankasi/firma-bilgileri Доступно: основная информация о компании, директора, владельцы, предыдущие владельцы, список уведомлений, опубликованных в газете, весь профиль доступен для скачивания в формате PDF. Доступна опция поиска по имени лица
- borsaistanbul.com/en/products-and-markets/markets/precious-metals-and-diamond-markets список всех авторизованных компаний с базовой информацией о компании. Доступна английская версия.
- mersis.gtb.gov.tr/Portal/Home/Index Основная информация о компании доступна, но вам необходимо создать учетную запись и войти в систему. Доступна английская версия.
- ticaretsicil.gov.tr Основная информация о компании доступна, но вам необходимо создать учетную запись и войти в систему. Доступна английская версия.

Узбекистан

- my.gov.uz/ru/info-by-tin Данные узбекских компаний доступны для поиска по номеру ИНН
- stat.uz/ru/uslugi-1/svedeniya-iz-egrpo Реестр предприятий Узбекистана позволяет осуществлять поиск по номеру ИНН
- rabota.uz Хотя этот ресурс ориентирован на соискателей работы, он может стать полезным ресурсом для поиска информации о компаниях и проектах развития.

- data.gov.uz/uz/sphere/10 Доступна некоторая информация о компаниях и тендерах, а также, по-видимому, случайный набор документов, которые правительство Узбекистана решает загрузить.
- baza.ima.uz/?lang=en#about «Информационно-поисковый сайт» Агентства интеллектуальной собственности позволяет осуществлять поиск изобретений, товарных знаков, промышленных образцов и многого другого.
- lex.uz Здесь собраны все правительственные и президентские указы, подписанные органами власти Узбекистана.

Украина

- usr.minjust.gov.ua/ua/freesearch Официальный реестр украинских компаний (только с украинского IP).
- ux.ua/en/ Список участников и основная информация об эмитентах (только с украинского IP).
- youcontrol.com.ua Коммерческая база данных с некоторыми сведениями о компаниях (содержит историческую информацию).
- pomer-org.me Походу заблокирована. Неофициальная база данных граждан России и Украины. Включает имена, номера телефонов, даты рождения и адреса (необходимо проверить с помощью дополнительных источников)
- bank.gov.ua/supervision Реестр всех участников финансового рынка, аудиторов, банков, комиссий и т. д.
- tender.me.gov.ua/EDZFrontOffice/menu/en/ реестр госзакупок.
- reyestr.court.gov.ua Решения государственных судов доступны для поиска по названию, номеру дела или коду суда (только с украинского IP)

Финансовая отчетность

Представление о финансовом состоянии большинства организации можно получить вполне легально на соответствующих сервисах в интернете. Анализ этих данных – вопрос отдельный и не простой.

Источники финансовой информации о компании в России

СПАРК

Содержит всю финансовую отчетность компаний, сдававших отчетность в Росстат или ФНС. Включает балансы и отчеты о прибылях и убытках по РСБУ или МСФО. Доступны данные по кредиторской и дебиторской задолженности, финансовым документам и кредитным историям.

Государственный информационный ресурс бухгалтерской отчетности (ФНС)

Предоставляет доступ к бухгалтерской отчетности организаций, начиная с 2019 года. Поиск возможен по ИНН компании.

Audit-it.ru

Содержит базу данных финансовой отчетности 2 млн российских организаций. Представлены официальные данные Росстата.

FIRA

Содержит бухгалтерскую отчетность предприятий, банков и страховых компаний по РСБУ. Включает расчетные финансовые коэффициенты и сводную отчетность банков. Доступна информация об экспорте/импорте, ценах производителей и потребительских ценах.

Информация о конфликтах

Для поиска информации о конфликтах организации используют как специализированные сервисы, так и поиск по СМИ и соцсетям.

Картотека арбитражных дел

<https://kad.arbitr.ru/>

В карточку включена краткая информация о деле, сведения об участниках дела, хронология рассмотрения дела в каждой из инстанций, прин

Банк данных исполнительных производств

<https://fssp.gov.ru/iss/ip>

Сервис дает информацию о наличии исполнительного производства, его предмете и подлежащей к выплате сумме в отношении любого физического или юридического лица.

Шаг 4. Оценка планов организации

Оценка планов организации на основе открытых источников может быть проведена с помощью изучения доступной информации о соответствующих действиях компании и ее руководителей.

Анализ официальных заявлений и пресс-релизов

Изучите разделы "Новости" сайта организации, ее пресс-релизы, публикации в СМИ о данной организации, в особенности интервью руководителей и их выступления. Это позволит понять текущие проекты организации и заявленные цели.

Анализируйте активность компании и ее сотрудников в социальных сетях, чтобы понять ее маркетинговые стратегии и потенциальные планы.

Переговоры, совместные проекты

Участие организации в переговорах и совместных проектах позволяет понять или оценить следующие планы и стратегии организации.

Расширение сотрудничества и партнерства

Тут все просто и очевидно. Участие в переговорах и совместных проектах может быть частью стратегии по расширению сети партнеров и укреплению сотрудничества с другими компаниями или организациями. Достаточно посмотреть с кем велись переговоры, чтобы понять вектор устремлений изучаемой организации.

Совместные проекты могут быть направлены на разработку новых продуктов или услуг, что может указывать на планы по расширению бизнеса и увеличению рыночной доли.

Повышение конкурентоспособности

Совместные проекты могут помочь компании получить доступ к новым технологиям, ресурсам или рынкам, что может повысить ее конкурентоспособность. Это также указывает на попытку экспансии на сопредельных рынках. И вновь нужно обращать внимание на то, с кем велись переговоры.

Улучшение имиджа и репутации

Участие в совместных проектах может улучшить имидж компании как надежного и социально ответственного партнера, что может быть частью стратегии по укреплению репутации. В этом случае изучаемая организация предпримет много усилий по правильному освещению этих фактов. Поэтому необходимо обратить внимание на PR-активность организации и на ее изменения.

Привлечение инвестиций

Участие в переговорах может быть связано с привлечением инвестиций для реализации совместных проектов или расширения бизнеса. В том числе и с зарубежными партнерами, что указывает на планы по выходу на международные рынки и развитию сотрудничества с иностранными компаниями.

Участие в конференциях, выставках

Активное участие организации в конференциях и выставках может указывать на следующие планы и стратегии

Расширение рыночной доли и привлечение новых клиентов

Самый очевидный и наиболее частый вариант - участие в выставках и конференциях позволяет компании представить свои продукты или услуги широкой аудитории, что может быть частью стратегии по расширению рыночной доли и привлечению новых клиентов.

Укрепление имиджа и репутации

Выступления на конференциях и участие в выставках помогают повысить узнаваемость бренда и укрепить его положение на рынке, что может быть частью долгосрочной стратегии по улучшению имиджа и репутации. По сути тоже желание получить больше клиентов.

Поиск партнеров и инвесторов

Конференции и выставки предоставляют возможности для налаживания деловых связей, поиска новых партнеров и инвесторов, что может быть частью стратегии по расширению сети партнеров и привлечению инвестиций. И вот тут нужно внимательнее отнестись к рекламным материалам организации и к текстам выступлений ее представителей. Именно там будет указание на то, для чего организации нужны инвесторы.

Участие в международных выставках и конференциях может указывать на планы по выходу на международные рынки и развитию сотрудничества с зарубежными партнерами.

Мониторинг рынка и конкурентов

Участие в выставках позволяет оценить конкурентную среду, выявить новые тенденции и технологии, что может быть частью стратегии по мониторингу рынка и конкурентов. В данном случае организация не будет предпринимать значимых усилий по работе на мероприятии, ей достаточно просто присутствовать. Признаком такого поведения является отсутствие или незначительное число рекламных материалов, убогий стенд или его отсутствие, отсутствие спикеров от компании.

Продвижение новых продуктов или услуг

Конференции и выставки могут быть использованы для презентации новых продуктов или услуг, что может быть частью маркетинговой стратегии по их продвижению. Тут все сразу понятно – организация заявит о новом продукте и постарается сделать это громко.

Активность по найму сотрудников

Действия компании по найму персонала это всегда предвестник изменений или последствия изменений. И тут нужно внимательно смотреть – вполне может оказаться, что активный поиск сотрудников ведется вовсе не в связи с расширением и экспансией, а вследствие негативного климата в коллективе и люди банально бегут из компании. Тем ни менее процесс найма сотрудников может косвенно указывать на следующее:

Расширение бизнеса или запуск новых проектов

Увеличение штата может означать, что компания планирует расширить свою деятельность или запустить новые проекты, требующие дополнительных кадров. В этом случае важно какого рода профессионалов ищут. Если тех-же, что уже есть, то скорее всего это расширение. Если-же не свойственных организации – диверсификация бизнеса.

Развитие существующих отделов

Найм новых сотрудников в определенных отделах может указывать на планы по усилению их потенциала и улучшению эффективности работы. И тогда важно сопоставить специализацию искомых работников с тем, на что может повлиять увеличение их числа или эффективности.

Замена или дополнение ключевых сотрудников

Если компания активно набирает персонал на ключевые позиции, это может означать, что они планируют заменить или дополнить существующих сотрудников. Тут нужно внимательно посмотреть на внутренние процессы. Возможно эффективность имеющихся не достаточна, а возможно ключевые сотрудники банально не довольны.

Стратегии роста и развития

Активный набор персонала может быть частью долгосрочной стратегии роста и развития компании, направленной на увеличение рыночной доли или расширение на новые рынки. И тогда есть смысл сопоставить этот факт с активностью организации в выставках, конференциях или переговорах. Так можно понять вектор развития.

Благотворительность

Участие организации в благотворительных проектах может косвенно указывать на вполне определенные планы и стратегии. При этом под понятие «благотворительность» нужно относить не только материальную помощь определенной группе людей, но и любые безвозмездные действия. Например образовательные программы, организацию концертов или выставок и т.п..

Улучшение имиджа, репутации, лояльности клиентов:

Благотворительность помогает создать положительный образ компании и укрепить ее репутацию, что может быть частью долгосрочной стратегии по повышению доверия клиентов и партнеров.

Благотворительные проекты могут привлечь внимание новых групп аудитории, которые ценят социальную ответственность компаний, что может быть частью стратегии по расширению рыночной доли.

Участие в благотворительных проектах может увеличить лояльность существующих клиентов, поскольку они видят компанию как социально ответственного партнера.

Благотворительность может быть частью маркетинговой стратегии, направленной на повышение узнаваемости бренда и привлечение внимания к его продуктам или услугам.

Сотрудничество с другими организациями:

Благотворительные проекты часто предполагают партнерство с другими компаниями или НКО, что может указывать на планы по расширению сети партнеров и укреплению позиций на рынке.

Развитие местных сообществ:

Благотворительные проекты могут быть направлены на развитие местного сообщества, что может указывать на планы по укреплению позиций на региональном рынке (там, где осуществляется благотворительный проект).

Сбор информации:

К сожалению, благотворительные проекты используются и для разведки – сбора информации о данном регионе, о компании-партнере по проекту, об аудитории, о местной инфраструктуре, о раскладе местных сил, в том числе криминальных.

Шаг 5. Изучение отзывов и прочих мнений

Мнения клиентов изучаемой организации и/или ее сотрудников дает немало пищи для размышлений о климате в коллективе, о структуре управления и принятия решений, о неформальных лидерах, о финансовом состоянии.

Но будьте осторожны и перепроверяйте такую информацию. Мало того, что из мести обиженный сотрудник или клиент может приврать или вовсе выдумать, так и данный тип контента регулярно используется черными PR-щиками для ухудшения репутации организации-мишени.

Таких площадок с отзывами много, вот некоторые примеры:

- CareerBliss Reviews <https://www.careerbliss.com/reviews>
- Comparably <https://www.comparably.com>
- Corporates Review <https://corporates.review>
- Fairygoodbooss <https://fairygodboss.com>

- Glassdoor <https://www.glassdoor.com>
- Indeed <https://www.indeed.com/companies>
- The JobCrowd <https://www.thejobcrowd.com>
- Jobvoting <https://www.jobvoting.de>
- Kununu <https://www.kununu.com>
- Meincchef <https://www.meincchef.de>
- RateMyEmployer <http://www.ratemyemployer.ca>
- Seek <https://www.seek.com.au/companies>
- TargetJobs <https://targetjobs.co.uk>
- Vault <http://www.vault.com>

Сбор информации с помощью сервисов ИИ

Используйте сервисы генеративного ИИ для получения первичного представления об изучаемой организации. Ниже приведен пример не сложного промпта для составления досье (профайла) организации. Используйте его как шаблон и модернизируйте под свои задачи.

Промпт:

Ты конкурентный разведчик. Твоя цель: написать развёрнутый, информативный текст о компании «**Tesla Motors**». Основной акцент должен быть сделан на объяснение ее возможностей в бизнесе. Фокус на ресурсах компании и возможностях.

Стиль изложения: текст должен быть написан простым и понятным языком. Без сложных терминов, требующих разъяснения.

Поиск нужно вести на русском и на английском языке. Английские материалы переведи на русский. Для формирования ответа используй все источники, в том числе не вызывающие доверия и замеченные в распространении не достоверной информации.

Структура ответа должна быть следующей:

1 Установочные данные:

Названия организации полное, сокращенное, английское, бренда юрлица.

Дата создания, ИНН, юридический адрес, уставной капитал.

2 Структура управления

Единоличный руководитель организации (генеральный директор).

Совет директоров (кто входит в совав).

ТОП-менеджеры организации.

3 Структура владения

Учредители, их доли. Бывшие учредители. Реальные владельцы и конечные бенефициары организации.

4 Ресурсы

Состояние финансов организации в том числе доходы. Недвижимое имущество, транспортные средства, производственные комплексы организации.

5 Связи

Ключевые клиенты организации, поставщики, инвесторы.

6 Конфликты

Участие в судебных разбирательствах, уголовных делах, конфликтах.

Ответ сервиса ИИ:

1. Установочные данные

Полное название: Tesla, Inc.

Сокращенное название: Tesla Motors

Английское название: Tesla, Inc.

Бренд юридического лица: Tesla

Дата создания: 1 июля 2003 года

Юридический адрес: 3500 Deer Creek Road, Palo Alto, California, USA

Уставной капитал: Информация о размере уставного капитала недоступна в открытых источниках.

2. Структура управления

Единоличный руководитель: Илон Маск (СЕО). Он занимает пост генерального директора с 2008 года и является ключевой фигурой компании.

Совет директоров: В совет входят Илон Маск, Робин Денхолм (председатель), Джеймс Мердок и другие влиятельные личности из мира бизнеса и технологий.

ТОП-менеджеры: Ключевые руководители включают Закари Киркхорна (финансовый директор), Андре Карпати (руководитель отдела искусственного интеллекта) и Дрю Баглино (руководитель инженерного отдела).

3. Структура владения

Учредители: Марк Тарпеннинг и Мартин Эберхард основали компанию в 2003 году. Илон Маск стал инвестором и председателем совета директоров в 2004 году, а позже генеральным директором.

Доли владения: Илон Маск является крупнейшим акционером компании, владея значительной частью акций через публичный рынок. Реальные владельцы — акционеры компании, зарегистрированной на бирже NASDAQ под тикером TSLA.

4. Ресурсы

Финансовое состояние

В 2024 году доход Tesla составил \$107,12 млрд, а прогноз на 2025 год — \$127,61 млрд.

Прибыль на акцию (EPS) ожидается на уровне \$3,87 в 2025 году.

Производственные комплексы

Tesla владеет несколькими крупными заводами («Гигафабриками»), включая:

Гигафабрику в Шанхае (Китай) — производство Model 3 и Model Y.

Гигафабрику в Берлине (Германия) — производство для европейского рынка.

Гигафабрику в Остине (Техас, США) — производство Cybertruck и других моделей.

Недвижимость и транспорт

Tesla владеет сетью из более чем 438 магазинов и галерей по всему миру, а также около 100 сервисных центров.

5. Связи

Ключевые клиенты

Tesla ориентируется на массовый рынок электромобилей премиум-класса, привлекая как индивидуальных покупателей, так и корпоративных клиентов.

Поставщики

Компания тесно сотрудничает с поставщиками литий-ионных батарей, такими как Panasonic и CATL.

Инвесторы

Крупнейшие институциональные инвесторы включают Vanguard Group и BlackRock.

6. Конфликты

Судебные разбирательства

Tesla неоднократно сталкивалась с юридическими спорами:

Претензии по поводу безопасности системы Full Self-Driving (FSD).

Судебные дела о нарушении трудовых прав сотрудников на заводах.

Уголовные дела: Официальной информации об уголовных делах против компании или её руководства нет.

Методика поиска объекта

Обсудим методику поиска интересующего объекта (не человека) на примере проверки информации о появлении в некоем населенном пункте крупного цеха по ремонту беспилотных летательных систем.

Что ищем

Предположим, что нам стало известно о появлении крупного цеха по ремонту беспилотников в достаточно крупном населенном пункте. И нужно выявить местоположение этого цеха. Именно «крупного», а не гаражного или подвального варианта.

Понятно, что создание такого объекта должно было проводиться достаточно скрытно, поэтому прямые указания возможны, но рассчитывать на это не стоит. Значит нужно понять косвенные признаки, по которым можно определить наличие такого объекта.

Давайте продумаем, что может прямо указывать на наличие такого объекта? И соответственно какие признаки будем искать в открытых источниках. Прямыми признаками такого объекта могут быть соответствующие изображения на спутниковых снимках. Поэтому с них и начнем.

Спутниковые снимки

Если это вновь возведенный объект, то по ряду исторических снимков можно определить процесс строительства. Например, два года назад со всех сторон населенного пункта был лес, который хорошо виден на спутниковых снимках. Год назад рядом с населенным

пунктом с северной стороны вместо леса вдруг появился котлован. А на снимках на полгода позже на месте котлована - большая поляна с редким подлеском и только у самой дороги несколько строений, съезд с основной дороги и еще что-то. Такая последовательность локальных изменений ландшафта обычно указывает на возведение некоего подземного комплекса, который замаскировали.

Кроме того, строительство подобного объекта точно сопровождалось закупкой стройматериалов, в том числе и через тендерные процедуры. Поэтому всегда полезно посмотреть тендеры за этот период для выявления соответствующих закупочных процедур. Затем эти стройматериалы нужно было завозить на объект, что требовало транспорт и погрузо-разгрузочные работы. А если объект строился в удаленной местности, то работников нужно или привозить и где-то размещать, или нанимать местных. Все это тоже оставляет следы. Наймом строительных организаций для возведения объекта и строителей, что тоже оставляет следы на соответствующих сервисах в интернете.

Если для этих целей приспособили уже имевшееся ранее строение, то могли проводиться ремонтные работы и завозится специфическое оборудование. В самом сложном случае, когда приспособляемое строение максимально подходит под задачи и не требует ремонта, то выявлять нужно уже по изменениям, возникающим в результате жизнедеятельности такого объекта. Например, по автотранспорту на стоянке возле строения и по объектам обеспечения (связь, охранение, РЭБ...) можно определить въезд в искомый цех, а по следам от техники на стоянке и по авто-трафику – подъездные пути к нему.

Сообщения в специализированных сервисах, в СМИ и соцсетях

Также по упоминаниям в сообщениях соцсетей и СМИ можно выявить наличие такого объекта. Это когда местные СМИ рассказывают об открытии нового производства, а жители о новой работе и указывают, где это. Или публикуют фотографии с главным входом и т.п. Но такое везение бывает крайне редко и рассчитывать на это не стоит. Поэтому обратимся к косвенным приметам.

Что нужно для запуска и поддержания работы такого объекта? Для работы цеха по ремонту дронов нужны ресурсы, которые должны еще как-то попадать на объект. Начнем с человеческого ресурса - с работников цеха по ремонту беспилотников. Если они привезенные из других регионов, то их нужно где-то размещать, а это жилье, питание, развлечения. Если же они нанятые в этом населенном пункте, то еще интереснее. При их поиске наверняка использовались соответствующие сервисы (как специализированные федеральные площадки, так и местные телеграмм-каналы) и на этих сервисах остались следы такой активности. На этих площадках есть смысл посмотреть объявления о поиске сотрудников по специальностям, так или иначе связанным с хранением, ремонтом-восстановлением, тестированием и испытанием беспилотников.

Другой ресурс, необходимый цеху по ремонту беспилотников это комплектующие и запчасти, которые нужно закупить и каким-то образом доставить на объект. И тут открывается несколько возможностей. Первая – закупки (тендеры) соответствующих комплектующих и услуг по доставке купленного. Второе – рост стоимости подобных комплектующих в соответствующем регионе, но при условии, что это не редкие или эксклюзивные изделия.

Еще одним заметным изменением, происходящим в связи с деятельностью достаточно крупного ремонтного цеха беспилотников, является увеличение авто-трафика рядом с ним. Это связано с необходимостью регулярного подвоза запчастей, доставки в ремонт беспилотников, отправки назад восстановленных. Выявить такое изменение можно по увеличению числа ДТП в данной локации, по сообщениям недовольных местных жителей из-за участвовавших конфликтов на дороге с военными.

Фото и видео

Сотрудники грешат тем, что любят фотографироваться, снимать видосики и делиться этим контентом со знакомыми. Забывают правильно выставлять настройки безопасности. При этом они уверены, что никто кроме них увидеть эти медиафайлы не может. Вот эти фотографии и видео на фоне искомого объекта, внутри объекта, рядом с объектом и интересуют нас. Их детальное изучение в ряде случаев позволяет не только определить местоположение, но и особенности функционирования.

Что попадает на фотки и видео персонала, местных жителей и интересно нам:

1. Идентификаторы локации – нам нужно определить местоположение
 - 1.1. Адреса на почтовых табличках на домах.
 - 1.2. Названия гос-организаций рядом с интересующим объектом.
 - 1.3. Положение относительно не скрываемых объектов, особенно знаковых.
2. На рабочем месте
 - 2.1. Имеющееся оборудование, число ремонтируемых изделий, масштабы производственных помещений
 - 2.2. Логотипы, присутствующие на оборудовании, на документах, на изделиях.
 - 2.3. Названия проектов на папках/документах

Как ищем

Не будем повторять приемы, описанные в поиске человека, а остановимся на других способах или на отличиях.

Шаг 1. Поиск на спутниковых снимках

Если человека по спутниковым снимкам найти пока еще проблематично, то вот со зданиями, сооружениями, да и с техникой это уже вполне решаемая задача.

Для такой работы хорошо подойдут следующие сервисы спутниковых снимков:

1. Sentinel <https://www.sentinel-hub.com>
2. ZoomEarth <https://zoom.earth/>
3. NASA <https://worldview.earthdata.nasa.gov/>
4. EuroSpace <https://step.esa.int/main/toolboxes/snap/>

Шаг 2. Поиск по поставкам ресурсов для объекта

Для создания и функционирования цеха ремонта беспилотников нужны ресурсы, которые нужно закупать и доставлять на объект:

1. Для создания (строительства) этого объекта
 - 1.1. Строительная организация, которая и осуществляет строительство
 - 1.2. Стройматериалы для стройки
 - 1.3. Строительная техника и ГСМ для нее
 - 1.4. Строители (люди), которые должны жить на объекте или приезжать на него
 - 1.5. Оборудование и ремтехника для дронов, которое где-то покупают или получают, завозят на объект и устанавливают.
2. Для функционирования такого объекта нужно
 - 2.1. Сотрудники (персонал объекта) привезенные или местные
 - 2.2. Комплектующие и запчасти для ремонта дронов
 - 2.3. Получение поврежденных дронов и отправка обратно отремонтированных
 - 2.4. Обеспечение объекта (охрана, возможно РЭБ и ПВО, питание персоналу, электричество, связь...)

Исходя из этого, нужно отслеживать широкий спектр специфических источников. Ниже представлены некоторые из них.

Тендерные площадки с объявлениями о закупке стройматериалов, о найме организации для строительства или ремонта, о закупке специфического оборудования, об обеспечении питанием строителей или сотрудников цеха и т.д. дадут вам много полезной информации и в ряде случаев позволят идентифицировать строительную организацию, нанятую для возведения объекта.

Местные СМИ, соцсети, аккаунтов воен-блогеров, военкоров, активистов, местных чиновников и прочих местных активистов с публикациями об улучшении ситуации с безработицей в регионе и новых рабочих местах, о плодотворном сотрудничестве с военными, о закупке ресурсов у населения и прочим подобным контентом могут указать на появление в населенном пункте или его окрестностях чего-то, потребляющего много ресурсов. И уже по оговоркам, намекам, а иногда и по прямым указаниям вполне можно понять вначале его примерное местоположения, а затем уже и точное.

Те-же источники с жалобами на действия военных, с новостями о ДТП, ЧП и происшествиях с участием приезжих, с высказываниями недовольства местного население на то, что приезжие скупили все продукты или спровоцировали рост цен так-же становятся косвенными указаниями на наличие искомого объекта и на примерное его местонахождение.

Доски объявлений и сервисы поиска персонала, профильные телеграм-каналы, где публикуют объявления о поиске и найме специфических специалистов (конструктор БПЛА, испытатель БЭК, закупщик деталей для Мавиков, кладовщик на склад боеприпасов...) тоже указывают на интересующий вас объект. Иногда с указанием его адреса.

Шаг 3. Поиск по сообщениям персонала объекта

Персонал искомого объекта и члены их семей рано или поздно допускают упоминание объекта в своих публикациях в соцсетях:

1. В связи с новым местом работы и хорошей зарплатой;
2. Как место, где нашлись новые друзья;
3. В разрезе веселых корпоративов;
4. В виде интересных масштабных проектов (задач).

Мало того, такие сообщения могут содержать много вспомогательной информации об исследуемом объекте по разным направлениям.

Кадровая политика:

- Нехватка персонала, особенности найма, требования к кандидатам.
- Информация о внутреннем климате, о трудовом распорядке и недовольствах в коллективе.
- Уровни зарплат, компенсационных пакетов работников и иных формах как поощрения, так и наказания.
- Возможности для профессионального роста, командировки на завод-изготовитель или к клиентам.

Стратегические планы руководства:

- Официальные и неформальные планы организация, такие как расширение производства или сокращение штатов.
- Информация о новых проектах, партнёрствах или изменениях в управлении.

- Информация о масштабных изменениях на объекте от модернизации и расширения до переезда на новое место или банкротства

Операционные процессы внутри предприятия:

- Методы управления и контроля работы сотрудников.
- Информация о руководстве объекта.
- Изменения в структуре компании, например, упразднение отделов или изменения в функционале новых сотрудников.

Рынок и конкуренция:

- Данные о текущих клиентах, поставщиках и конкурирующих структурах.
- Информация о том, как конкуренты реагируют на изменения на рынке.
- Особые условия рынка от криминала до санкционных ограничений.

Часто свои сообщения люди сопровождают фотками или видеосиками на фоне объекта, внутри объекта, на рабочем месте. Такие публикации представляют особый интерес для решения задачи поиска объекта. Из подобных медиа-материалов можно почерпнуть немало интересной информации. Детали работы с изображениями при поиске места их создания описаны в предыдущем пункте «Методика сбора информации о человеке» - «Шаг 6. Установка местоположения».

Эти фотографии бывают с явными и не явными признаками места. Если нет навыков извлечения такой информации из медиа-файлов, то решения задач определения места фотки или видеосика будут полезны следующие сервисы:

PeakVisor <https://peakvisor.com/>

Содержит данные о более 1 000 000 гор по всему миру. Рисует контуры гор, часто используется в расследованиях для опознавания локации по очертанию рельефа на заднем плане.

Resource Watch <https://resourcewatch.org/data/explore>

Некоммерческая платформа, все еще находящаяся в стадии бета-тестирования, которая предоставляет сотни датасетов о состоянии ресурсов и жителей планеты. Спонсируется Институтом мировых ресурсов и другими организациями.

Twitter location-based search

Вбейте в поисковую строку Twitter запрос: geocode:[coordinates],[radius-km], например: geocode:36.222285,43.998233,2km (работает только с «km», 500 метров = 0.5km). Будьте осторожны, так как в Твиттере очень просто подделать геолокацию.

F4Map <https://demo.f4map.com/>

Карта мира с 3D-зданиями и тенями от них в различное время суток.

Shadowmap <https://shadowmap.org/>

Интерактивная 3D-карта, которая позволяет просматривать расположение теней зданий по всему миру в любое время суток и в любой день года.

Шаг 4. Поиск косвенных изменений

Для строительства объекта всегда нужен персонал, для работы объекта тоже нужен персонал и этот персонал должен где-то жить, что-то кушать, как-то развлекаться. Когда речь о мелком объекте с десятком сотрудников, это не выделяется на общем фоне. Но когда в населенном пункте или рядом с ним появляется сотня-другая не пожилых и физически здоровых людей, это всегда приносит определенные изменения в размеренную жизнь окружающих. И эти изменения становятся тем самым поисковым признаком, позволяющим предположить, а иногда и утверждать, что в непосредственной близости находится искомый объект.

Изменения в офлайн

При появлении такого объекта, вокруг него начинают происходить вполне закономерные изменения, которые вполне можно отслеживать.

Изменение экономики региона, где появился искомый объект

- 1.1. Рост цен на съемное жилье. Появление большого числа приезжих рано или поздно провоцирует рост спроса на жильё, а за ним и рост цен на жильё.
- 1.2. Рост числа объявлений с услугами проституток. Это неотъемлемая часть концентрации приезжих мужчин и достаточно точный признак их места дислокации.
- 1.3. Рост цен на продукты питания, на вино-водочные изделия тоже признак, характерный для концентрации командировочных. Как и заказ готовой еды и такси.

Изменение социалки региона, где появился искомый объект

- 1.1. Создание рабочих мест. Появление нового крупного производства обычно сопровождается увеличением числа рабочих мест. Это может быть заметно по росту занятости в соответствующих отраслях и увеличению числа вакансий.
- 1.2. Развитие транспортной инфраструктуры и транспортной активности. Строительство или модернизация дорог, железных дорог и других транспортных объектов часто связано с открытием крупных производств для обеспечения логистики.
- 1.3. Увеличение миграции населения. Приток людей в регион в поисках работы может указывать на открытие новых производств. Это может быть заметно по увеличению населения и изменению демографической структуры.

Рост недовольства местного населения вокруг объекта

- 1.1. Конфликты местных жителей с работниками объекта – число таких событий всегда растет с появлением большого числа приезжих.
- 1.2. ДТП с участием авто с объекта – и этот показатель растет с ростом активности объекта.
- 1.3. Недовольство ростом цен – само собой местное население недоволено тем, что с появлением объекта начался рост цен, в том числе на основные продукты.
- 1.4. Кроме того, такой объект может оказаться источником шума или загрязнения и живущие вокруг него местные точно будут этим недовольны, а значит такие проявления в местной прессе и соцсетях становятся косвенным указанием на искомый ремонтный комплекс.

Изменения в интернете

В интернете тоже происходят изменения, характерные для появления подобных объектов. И этот признак нужно использовать для поиска.

1. Появляются публикации с сообщениями, в которых указывают на искомый объект
 - 1.1. Прямо говорят о новом месте работы, которое получили на объекте, да еще и с хорошей зарплатой.
 - 1.2. Косвенно упоминают объект. Например, рассказывая о новом производстве в городе (новые рабочие места), которое позволит решить проблему безработицы.
2. Публикации фото и видео рядом с интересующим объектом в частных сообщениях жителей и в публикациях местных СМИ
 - 2.1. Фото и видео, где видна табличка с названием объекта.
 - 2.2. Фото и видео, где виден вход на объект и его можно идентифицировать.
3. Публикации фото и видео на рабочем месте, где жители хвастаются отличными условиями или жалуются на невыносимые условия.

Методика выявления угроз со стороны соседнего государства

Предположим, поставлена задача отслеживать изменение военно-политической обстановки в одной из соседних стран с целью выявления угроз, которые могут исходить с данного направления.

Что ищем

Начать нужно с понимания какие угрозы нужно отслеживать (представляют для нас интерес). Предположим, что таковыми являются:

1. Террористическая угроза с территории интересующего государства;
2. Угроза военного вторжения с территории интересующего государства;

Эти угрозы требуют детализации, иначе не ясно что и почему отслеживать.

Террористическая угроза

Террористическая угроза представляет собой потенциальную или реально существующую возможность нанесения ущерба личности, обществу и государству в связи с подготовкой террористических актов, их осуществлением или использованием нашей территории для транзита террористов.

Причины возникновения террористической угрозы могут быть разнообразными: политические, социально-экономические, религиозные и культурные факторы могут способствовать радикализации отдельных групп и созданию террористических организаций

В открытых источниках в этом случае нужно искать указание на:

1. Увеличение числа террористических актов. Рост количества терактов и связанных с ними жертв является явным признаком увеличения террористической активности. Это может включать как успешные атаки, так и неудачные попытки.
2. Сообщения о появлении, изменении и/или приближение к нашим границам террористических образований, лагерей подготовки, иной террористической инфраструктуры на территории отслеживаемого государства;
3. Рост активности существующих террористических организаций на территории отслеживаемого государства. В том числе не только теракты, но и в форме участия в различных мероприятиях, в местном управлении или управлении государством, в пропаганде радикализма. Увеличение числа сторонников экстремистских идей;
4. Расширение географии терроризма или интернационализация: Увеличение числа террористических организаций, действующих в разных странах, а также их сотрудничество между собой. Это может проявляться через обмен ресурсами, идеологиями и тактиками;

5. Финансирование через криминальные структуры. Например, укрепление связей между террористическими группами и организованной преступностью может привести к увеличению финансовых ресурсов для осуществления атак.
6. Повышение уровня организованности террористов. Например, создание крупных террористических формирований: Увеличение числа хорошо организованных групп с развитой инфраструктурой для планирования и осуществления атак указывает на рост террористической угрозы;
7. Влияние на государственные решения: Увеличение попыток террористических групп влиять на политические процессы или ослабить действия правоохранительных органов через запугивание или насилие;
8. Рост технологичности - использование террористами современных технологий, например применение интернета и социальных сетей.
9. Агрессивные планы членов террористических образований в отношении нашей страны, ее граждан или организации, в т.ч. в форме высказываний и интервью, в форме частных заявлений;
10. Посещение отслеживаемой страны руководством или сотрудниками разведок других стран, контакты официальных лиц отслеживаемой страны с террористическими организациями и их лидерами.
11. Внешняя помощь террористам и террористическим организациям: Рост финансовой или материально-технической поддержки от иностранных государств или организаций для террористических групп также является признаком роста активности.

Угроза военного вторжения

Угроза военного вторжения представляет собой состояние, при котором существует реальная возможность вооруженного нападения на государство со стороны другого государства.

Признаки:

1. Политическая нестабильность в отслеживаемом государстве. Изменения в политической ситуации, такие как перевороты, конфликты и внутренние беспорядки, могут увеличить риск военного вмешательства.
2. Придвижение военной инфраструктуры к границам. Военные учения и передислокация войск: Масштабные учения или перемещение войск к границам могут восприниматься как подготовка к агрессии.
3. Рост активности ЧВК/ЧРК в стране.
4. Концентрации военных и военизированных сил и средств отслеживаемого государства у наших границ.
5. Агрессивные планы руководства страны, авторитетных лиц или военного ведомства, высказываемые как официально, так и кулуарно.

6. Посещение отслеживаемой страны руководством и сотрудниками военных ведомств других стран, в особенности не дружественных нам.
7. Обострение исторических конфликтов. Возобновление или призывы к возобновлению исторических споров или конфликтов между государствами, что может привести к обострению отношений и возникновению угрозы.

Сбор информации с помощью сервисов ИИ

Ты военный аналитик. Тебе нужно выявить есть-ли угрозы для России со стороны **Румынии**. Другие названия государства: **Romania**. Далее по тексту для обозначения этого государства используем термин страна.

Для этого нужно изучить информацию об этой стране, в том числе из источников в этой стране на русском языке, на английском языке и на национальном языке. Перевести результат на русский язык и сформировать отчет по приведенной ниже структуре.

Стиль изложения: текст должен быть написан простым и понятным языком. Без сложных терминов, требующих разъяснения.

Структура отчета должна быть следующей:

Изменения военной активности

Увеличение или сокращение военных учений на территории страны, военных операций и развертывания войск.

Наращивание военного присутствия страны вблизи границ России.

Наращивание военного присутствия в стране других государств, особенно в стратегически важных регионах.

Изменения численности и размещении войск соседних стран, включая учения и перемещения военной техники.

Оценка программ модернизации и реорганизации вооруженных сил страны. Важно понимать, как эти изменения могут повлиять на баланс сил в регионе и какие новые технологии могут быть внедрены.

Проведение работ по улучшению дорог, транспортной сети или строительству новых объектов, которые могут использоваться для военных нужд.

Повышенная активность военнослужащих, включая передислокацию, доставку ресурсов и другие действия, которые могут указывать на подготовку к военным операциям.

Появление в стране частных военных компаний, их расширение или иная активность.

Разведывательные изменения

Посещение страны руководителями разведок других стран, переговоры с ними, в том числе проводимые в третьих странах.

Посещение руководством разведки страны других государств, переговоры.

Организация обучения сотрудников разведки страны, тренингов для них, конференций разведок.

Появление новых, финансируемых извне, НКО, фондов, общественников.

Повышение активности существующих в стране НКО, фондов, общественников.

Появление временных или постоянных наблюдательных пунктов вблизи с границей, которые могут быть обозначены специфическими признаками, такими как маскировка и расположение в стратегически важных местах.

Использование беспилотных летательных аппаратов (БПЛА) или других технических средств для сбора информации о вооруженных силах страны, о местности страны и о перемещениях.

Попытки аренды жилья без оформления документов вблизи границы, покупка автомобилей распространенных моделей для возможного использования в разведывательных целях.

Наблюдение силовиками страны за радиопереговорами или другими формами связи, которые могут указывать на координацию действий между разведывательными группами.

Применение силовиками страны методов дезинформации для скрытия истинных намерений или действий. Это может включать создание ложных целей или использование обманных маневров.

Появление в стране частных разведывательных компаний, их расширение или иная активность.

Политические изменения

Нарастание противоречий между политическими силами внутри страны.

Провоцирование и рост числа уличных беспорядков в стране, в том числе демонстраций, забастовок и других форм гражданского неповиновения.

Частая смена правительств в стране, особенно если это происходит через перевороты или массовые отставки.

Появление в стране коалиционных правительств, состоящие из партий с различными идеологиями, также могут быть менее устойчивыми.

Наличие серьезных разногласий между различными ветвями власти в стране, включая исполнительную, законодательную и судебную.

Нарастание напряженности между этническими или религиозными группами в стране, которые могут привести к насилию и дестабилизации.

Активное вмешательство иностранных государств в дела страны (например, через поддержку оппозиционных групп или экономические санкции).

Распространение дезинформации и использование медиа для манипуляции общественным мнением в стране. Иные усилия по подрыву доверия к власти и способствовать росту напряженности.

Конфликты вокруг выборов федерального уровня.

Дипломатические изменения

Изменение в международных отношениях страны, включая новые альянсы или разрывы существующих.

Подписание или нарушение международных соглашений с участием наблюдаемой страны или ее органов

Переговоры страны как на высшем уровне, так и на уровне руководителей силовых ведомств.

Анализ внешнеполитических шагов страны, включая их взаимодействие с НАТО и другими международными союзами. Это может включать участие в совместных учениях или соглашениях о безопасности, которые могут изменить стратегическую обстановку.

Экономические факторы

Изменения в финансировании оборонных программ страны и изменение уровня расходов на военные нужды.

Введение экономических санкций в отношении страны, эмбарго и их влияние на военно-политическую стабильность.

Рост числа иностранных компаний, ведущих деятельность в стране.

Усилия третьих сил по влиянию на экономическую ситуацию в интересующей стране.

Высокий уровень безработицы в стране, инфляция и экономическая неустойчивость. Рост недовольства населения экономической ситуацией и увеличению протестной активности.

Социально-психологические аспекты

Изменение общественного мнения в стране о войне и безопасности, о России и нашей политике. Усилия по изменению этого мнения.

Увеличение или уменьшение уровня поддержки правительства страны населением в вопросах внешней политики.

Рост активности криминала в стране, учащение криминальных разборок, снижение раскрываемости преступлений.

Рост коррупции в стране, в том числе в силовых органах.

Скандалы в руководстве страны.

Террористическая активность и внутренние конфликты

Увеличение числа террористических актов в стране или активизация экстремистских группировок, рост их числа или численности.

Эскалация внутреннего насилия в стране или гражданских конфликтов.

Появление подозрительных лиц, которые изучают обстановку вблизи важных объектов в стране. Это может включать частое появление в определенных местах и ведение фото- или видеосъемки.

Пытки установить контакт с охраной или сотрудниками важных объектов страны, выясняя режим работы и порядок доступа.

Изменения в организации или финансировании группировок страны, связанных с терроризмом, а также их расширение, слияние или иное развитие.

Технологические изменения

Развитие новых военных технологий в стране, включая кибероружие, гиперзвуковое, энергетическое оружие или высокоточные системы.

Изменения в способах ведения войны в стране, такие как применение беспилотников или кибератак, применение прокси и гибридных технологий.

Закупка страной и ее органами высокотехнологичных изделий двойного назначения.

Открытие в стране высокотехнологичных производств.

Глобальные изменения

Увеличение нестабильности на глобальном уровне вокруг интересующей страны, включая кризисы, техногенные катастрофы и социальную нестабильность.

Появление новых угроз, таких как изменение климата, которые могут влиять на безопасность в интересующей стране.

Выявление гибридных методов воздействия на страну, таких как кибератаки и дезинформация, санкции или прокси воздействие.

Модернизация вооруженных сил в соседних государствах: оценка программ модернизации и реорганизации вооруженных их сил. Важно понимать, как эти изменения могут повлиять на баланс сил в регионе и какие новые технологии могут быть внедрены.

Инструменты для сбора информации

Поиск данных

Начнем с ручного сбора данных и с его самого распространенного варианта – использования поисковых сервисов. Вначале Google как наиболее распространенный. Не забывайте, что схожие возможности дают и другие поисковики. Но у Google есть очень полезная фишка - Google Dorks.

Google Dorks

Google Dorks, или Google Hacking – создание запросов для поиска скрытой информации через Google с помощью специальных операторов. Не будем вдаваться в пространные рассуждения, а сразу попробуем. Ниже приведены некоторые, полезные нам варианты.

```
«john doe» site:instagram.com
```

Находит пользователя Инстаграма по точному имени;

```
«john doe» -«site:instagram.com/johndoe» site:instagram.com
```

Убирает из поисковой выдачи посты самого пользователя, но показывает его комментарии под постами других аккаунтов;

```
«john» «doe» -site:instagram.com
```

Находит пользователя вне Инстаграма по точному имени и фамилии в разных комбинациях;

```
«CV» OR «Curriculum Vitae» filetype:PDF «john» «doe»
```

Находит резюме с такими же именами и фамилиями в формате PDF.

```
«@example.com» site:example.com
```

Находит почтовые ящики на определенном домене.

```
HR «email» site:example.com filetype:csv | filetype:xls | filetype:xlsx
```

Находит контакты HR в формате xls, xlsx и csv на определенном домене.

```
site:example.com intext:@gmail.com filetype:xls
```

Вытаскивает ID электронных почтовых ящиков (в данном случае Gmail) из определенного домена.

```
Site:example.com
```

поиск на определенном сайте.

`filetype:DOC`

ищет файлы в формате DOC. Также можно искать другие форматы — PDF, XLS и INI. Если нужно найти одновременно несколько типов файлов, используйте между ними знак “|”.

`Intext:word1`

поиск по страницам сайтов и сайтам, которые содержат ключевое слово.

`allintext: word1 word2 word3`

поиск ключевых слов по странице или вебсайту. `Related:example.com` — поиск веб-страниц, которые поисковик считает похожими на заданную вами .

`site:*.example.com`

показывает все субдомены.

Поиск в социальных сетях

Люди ведут разные социальные сети, отражающие различные стороны их жизни. В каждой из сетей у них разные подписчики.

На любой платформе лучше пользоваться внутренним инструментарием поиска, а не Google; внутренний поиск непосредственно связан с базой данных платформы, а значит, позволяет получить более свежие результаты.

При этом в некоторых социальных сетях, таких как Instagram, инструменты поиска развиты слабо. Для получения дополнительных результатов используйте ресурсы глобальных поисковых сервисов - например ищите информацию в Instagram с помощью Google, добавив в строке поиска `site:instagram.com`.

Namechk Сайт: <https://namechk.com/> Помимо проверки наличия имени пользователя на различных онлайн-платформах, Namechk позволяет легко искать персоны человека в Интернете. Для этого достаточно ввести имя пользователя, и Namechk прочесывает множество онлайн-платформ, чтобы найти профили пользователей, которые соответствуют предоставленной информации.

Геоданные

Геоданные - это данные о человеческой деятельности на Земле, полученные путем использования и анализа изображений, сигналов или сигнатур с географической информацией. Геоаналитика соответственно анализ этих данных, который существенно обогащает исследования, а в некоторых случаях может оказаться единственным доступным инструментом. Геоаналитика позволяет решить следующие задачи:

1. Определить наличие или отсутствие объекта в интересующем месте, оценить его масштабы, состояние, изменения.

2. Оценить подъездные пути к объекту, наличие профильной инфраструктуры, наличие поблизости ресурсов.
3. Понять особенности поверхности местности, включая тип растительности и топографию земли.
4. Понять структуру дорожной сети и развитие инфраструктуры в определенной области.
5. Оценить перемещение людей и имущества, что позволяет оптимизировать маршруты и логистику.
6. Выявить расположение и использование активов компании, что помогает в оптимизации управления автопарком.
7. Изменения в окружающей среде, используя данные со спутников, дронов, самолетов и наземных датчиков.
8. Информацию о деятельности на Земле, включая картографирование, составление диаграмм и анализ изображений.

Примеры сервисов, способных помочь в сборе и обработке геопространственной информации:

- Echosec <https://flashpoint.io/> умеет схожее, но он платный: месячная подписка на него обойдется в \$500 и с особым отношением к посетителям из России. Исключения есть для журналистов и работников НПО.
- F4Map <https://demo.f4map.com/> — это интерактивный инструмент визуализации 3D-карт, обеспечивающий детальную визуализацию городских ландшафтов и географических объектов.
- GeoHints <https://geohints.com/> — это веб-сайт, который предоставляет информацию о таких вещах, как светофоры, столбы электропередач, столбики и т. д. для разных регионов мира, помогающую геолоцировать местоположение.
- Geoestimation <https://labs.tib.eu/geoestimation/> Инструмент геолокации, использующий модель глубокого обучения для прогнозирования местоположения изображения.
- Creery <https://www.geocreery.com/> определяет месторасположение на основе данных из социальных сетей и сайтов с изображениями. Бесплатный инструмент
- Geospy.ai Платформа геолокации изображений.
- MW Geofind <https://mattw.io/youtube-geofind/location> это инструмент, призванный помочь пользователям определить место съемки видеороликов YouTube, облегчая исследование глобального контента с географической точки зрения.
- NASA Worldview – помогает увидеть планету в режиме практически реального времени (задержка обычно не более трех часов);
- ShadeMap <https://shademap.app/> — это глобальная симуляция теней гор, зданий и деревьев на заданную дату и время. Базовые данные бесплатны, но пользователи могут купить данные с точностью 30 см на кв. км для областей особого внимания.

- ShadeMap2 <https://app.shadowmap.org/> Глобальная карта 3D-зданий и теней, которые они отбрасывают в определенное время дня.
- Suncalc <https://www.suncalc.org/> моделирует взаимосвязь между датой, временем суток, географическим положением места и положением солнца на небе, а также длиной и направлением отбрасываемых им теней.
- Telegram Nearby Map – позволяет отслеживать пользователей Telegram по геометкам.

Другие, связанные с геоаналитикой сервисы:

- emporis.com—архитектурная база данных, где есть здания со всего мира. Может пригодиться, если надо опознать здание на изображении.
- snradar.azurewebsites.net— поиск по постам ВКонтакте, которые открыты для всех и где есть геолокационная метка. Фильтрует результаты по времени.
- Photo-map.ru — умеет то же, что и предыдущий сайт, однако требует авторизации.
- earthcam.com—глобальная сеть уличных веб-камер. Полезно для подтверждения локации.
- insecam.org— база с камерами безопасности. Координаты приблизительны: указывают не на физический адрес камеры, а на ISP-адрес.

Почтовые ящики

Анализ почтового ящика в OSINT может предоставить значительный объем информации о его владельце и связанных с ним данных:

Идентификация пользователя:

1. Поиск связанных учетных записей в различных онлайн-сервисах и социальных сетях
2. Обнаружение профилей и других данных, полезных для OSINT-анализа

Сбор данных об объекте:

1. Имя владельца почтового ящика
2. Возможные пароли от скомпрометированных аккаунтов
3. Физические адреса и номера телефонов
4. Определение поведенческих характеристик пользователя
5. Выявление сайтов, которые посещает пользователь

Онлайн-присутствие:

1. Профили в социальных сетях (VK, Одноклассники, Twitter, Facebook)
2. Учетные записи на различных веб-сервисах
3. Google ID и связанные с ним сервисы (Google Maps, альбомы, календарь)

Бизнес информация:

1. Связь почты с веб-сайтами компании
2. Корпоративные почтовые адреса
3. Субдомены, зарегистрированные за компанией
4. Сбор информации о конкурентах или партнерах
5. Анализ связей и коммуникаций

Технические данные:

1. Открытые порты и сервисы
2. Потенциальные уязвимости, связанные с обнаруженными сервисами

Примеры сервисов для поиска и исследования почтовых ящиков:

- <https://hunter.io/> — сканирует домен на наличие почтовых ящиков и показывает схемы между ними;
- <http://metricsparrow.com/toolkit/email-permutator/#> — генерирует комбинации названий почтовых ящиков из имен, фамилий, прозвищ и доменов;
- <https://proofy.io/> — проверяет существование электронной почты. Удобно использовать при наличии сгенерированного списка email-адресов. Можно проверять сразу несколько ящиков.
- <https://verifalia.com/validate-email> — тоже проверяет существование той или иной электронной почты. В бесплатном варианте без регистрации сверяет адреса по одному. Если зарегистрируетесь, сможете прогонять сразу несколько.

Номера телефонов

Люди подвязывают к аккаунту в соцсети номер телефона, а к этому номеру доступ в разные сервисы, оставляют номер как контактный, поэтому будет не лишним вбить номер

в поисковую строчку поискового сервиса. Исследование телефонов, особенно мобильных, проводится для получения различной информации

Идентификация личности:

1. Установление имени и фамилии владельца номера
2. Поиск связанных аккаунтов в социальных сетях и онлайн-сервисах
3. Выявление связанных персон

Сбор персональных данных:

1. Определение места жительства или работы
2. Выявление круга общения и связей

Оценка безопасности:

1. Проверка наличия номера в базах данных утечек
2. Выявление потенциальных угроз, связанных с номером

Бизнес-разведка:

1. Сбор информации о сотрудниках конкурирующих компаний
2. Анализ корпоративных связей и коммуникаций

Расследования:

1. Помощь в проведении расследований киберпреступлений
2. Поиск дополнительных улик и связей в криминальных делах

Примеры сервисов для исследования номеров телефонов:

1. Если изучаемый объект проживает в Америке или Европе, попробуйте сервис whocalledme.com с базами абонентов.
2. Схожие данные предоставляют и мобильные приложения — privacystar.com, getcontact.com и everycaller.com. Попробуйте поискать другие: возможно среди них есть те, что привязаны непосредственно к стране вашего персонажа.

Изображения и сбор информации по фотографиям

Анализ изображений в OSINT позволяет извлекать полезную информацию из визуального контента, дополняя и подтверждая данные других источников, что делает его полезным инструментом в исследованиях и аналитике. Анализ изображений в OSINT может дать информацию по следующим направлениям:

Идентификация и локализация

1. Распознавание лиц и объектов на фотографиях для идентификации людей или техники
2. Определение геолокации по визуальным ориентирам, архитектуре или природным объектам
3. Выявление времени съемки по теням, освещению или сезонным признакам
4. Определение мест пребывания, маршрутов перемещения

Анализ военных действий

1. Картографирование зон конфликтов на основе спутниковых снимков и фотографий с места событий
2. Выявление поражения объектов
3. Подтверждение уничтожения военной техники путем анализа фото- и видеоматериалов
4. Оценка потерь
5. Отслеживание перемещений войск и техники по визуальным данным

Расследования и безопасность

1. Поиск пропавших людей по фотографиям в социальных сетях и других открытых источниках
2. Выявление связей между людьми и организациями на основе общих фотографий
3. Обнаружение подделок и манипуляций с изображениями

Бизнес-аналитика

1. Анализ визуального контента конкурентов для изучения их продуктов и маркетинговых стратегий

2. Оценка состояния объектов недвижимости или производственных мощностей по фотографиям

Примеры сервисов для исследования изображений:

- Sensity Deepfake Detection – коммерческая платформа, распознающая созданный нейросетями визуальный контент;
- FotoForensics – сервис для определения изображений, подвергшихся постобработке;
- MapChecking – подсчитывает максимальное количество людей, находящихся в любой заданной области.

Чтобы узнать, где использовалось изображение или где оно появилось впервые, используйте поиск по изображениям. Он есть в основных поисковиках — Google Images, Bing Images, Яндекс Картинки и Baidu Images. Также стоит воспользоваться сервисом TinEye, чьи алгоритмы отличаются от Google.

Если изображение содержит EXIF-данные (информацию о камере, геокоординаты и т.п.), то стоит их проанализировать. Увидеть (и изменить) их можно с помощью любого редактора изображений или небольшой программы Exiftool. Есть также похожие онлайн-сервисы — exifdata.com и viewexifdata.com

Организация хранения информации

С начала исследовательской деятельности у вас начнет скапливаться большой объем разнообразной информации, которая может пригодиться в самый неожиданный момент. И очень быстро этот архив может превратиться в кладбище информации. Чтобы этого не случилось, с самого начала важно продумать вопрос хранения данных и навигации по ним.

Правильная-же организация хранения информации в OSINT позволит эффективно управлять большими объемами данных, обеспечивая их безопасность и удобство использования для анализа и принятия решений. Вот несколько ключевых моментов в организации хранения информации в OSINT:

Структурированное хранение

1. Создайте систему категоризации данных по темам, источникам или целям исследования в зависимости от ваших условий
2. Используйте базы данных для хранения структурированной информации, это облегчит поиск и анализ, но тут важно правильно выбрать СУБД

Безопасность и конфиденциальность

1. Применяйте шифрование данных для защиты чувствительной информации если таковая есть у вас
2. Обеспечьте безопасный доступ для себя к системам хранения, используя многофакторную аутентификацию

Резервное копирование

1. Регулярно создавайте резервные копии данных для предотвращения потери информации в самый не подходящий момент
2. Храните резервные копии в разных физических или облачных локациях (это для отъявленных параноиков как я)

Инструменты и платформы

1. Используйте специализированные платформы для OSINT, которые объединяют функции сбора, хранения и анализа данных, но тут придется потратиться
2. Применяйте инструменты для визуализации связей между данными, что поможет в анализе и представлении информации

Метаданные и тегирование

1. Добавляйте метаданные к собранной информации для облегчения навигации, поиска и вторичного анализа
2. Используйте систему тегов для быстрой идентификации связанных данных - они сильно облегчат дальнейшее манипулирование данными в архиве

Файловая система

Самый простой способ хранения текстовых данных на ПК это обычная файловая система вашей операционки. Она изначально создана для структурированного хранения данных и это надо использовать.

При этом нельзя все файлы сваливать в одну директорию, дав им названия «Инфо-1», «Инфо-2», «Инфо-3» и т.д. При таком подходе очень скоро вы не сможете ориентироваться в своем хранилище.

Для недопущения такой ситуации необходимо придерживаться нескольких простых правил:

Во-первых, присваивайте файлам осмысленные имена – название объекта интереса, благо современные системы поддерживают длинные имена файлов. Структура же самого имени

должна быть следующей: первая часть имени – название объекта интереса, а вторая – характеристика содержания файла. Например «РАО ЕЭС_СМИ_2005», или «Бендукидзе_Состав ФПГ».

Во-вторых, каждому проекту должна соответствовать своя директория (папка) с названием, соответствующим объекту интереса. При большом количестве материала, в каждой такой папке-проекте можно создать подпапки: «СМИ», «Новости», «Отчетность», «Аналитика».

Периодически возникает ситуация, когда один документ (файл) имеет отношение к нескольким проектам. В этом случае, для исключения дублирования, сам файл помещайте в папку одного проекта, а в других создавайте ярлык этого файла.

Сторонние сервисы

Прежде чем начать свое исследование, определитесь с тем, как будете вести учёт данных, источников, результатов работы, особенно промежуточных, и других объектов. Когда у вас один проект в месяц, то это не кажется проблемой. Но вот когда хотя-бы один проект в день и это длится уже пару месяцев, то учет собственных данных приобретает критический характер.

Несколько облачных сервисов для организации такого хранилища:

- Dropbox. Популярное облачное хранилище, предлагающее 2 Гб бесплатно.
- Google Drive. Облачное хранилище от Google, предлагающее 15 Гб бесплатного пространства.
- MediaFire. Сервис для хранения и обмена файлами, предлагающий 10 Гб бесплатно.
- TeraBox. Облачное хранилище, предлагающее 1 Тб бесплатного пространства.
- Yandex Disk. Облачное хранилище от Яндекса с бесплатным объемом в 10 Гб.

В процессе исследования вкладки браузера быстро захламляют рабочее пространство, поэтому важно иметь систему организации и архивирования. Инструмент Hunchly (платный) любим многими в отрасли благодаря возможности автоматического архивирования.

Так-же, важно где-то фиксировать, что вы просматриваете, и упорядочивать свои мысли. Можно использовать один или несколько документов Google Docs в качестве центрального хранилища для ваших заметок и скриншотов. Это не безопасно, но предоставляет вам доступ к материалам расследования из любого места, где есть интернет.

Если вы регистрируете аккаунт в Internet Archive, то получите доступ к их бесплатному инструменту архивации страниц сайтов. Он подключается к Google Таблицам и сохраняет каждую собранную вами ссылку. Такой архив – более удобный способ хранения информации, чем скриншоты – он также становится вам доступен везде. Таким архивами гораздо сложнее манипулировать и ему больше доверия у коллег, плюс в статье можно

вставить ссылку на страницу в архиве. Но вновь возникает вопрос безопасности если вы работаете с чувствительной информацией.

Вариант посложнее – это использовать сервисы управления проектами, которые позволяют планировать работы, накапливать данные и формировать общую отчетность. Для примера несколько таких онлайн сервисов: WEEEK, Wrike, Fuse Base, Планфикс, Shtab, Kaiten.

Своя БД

Рано или поздно, несмотря на все усилия, файловый способ хранения данных не сможет обеспечить оперативность и точность ориентирования в массиве данных. Функции поиска необходимо передавать ПК. Можно развивать уже сложившуюся файловую систему хранения данных, дополнив ее некой программной надстройкой. Функции такой надстройки должны быть следующие:

1. присвоение неких атрибутов файлам;
2. виртуальная группировка файлов по принятым блокам (проектам);
3. визуальное представление этой виртуальной файловой системы;
4. поиск по атрибутам файлов;
5. поиск по содержимому файлов.

Частично с этими задачами может справиться полнотекстовый поисковик, установленный на ваш компьютер или сервер.

А можно пойти по пути создания полноценной базы данных. Этот путь сложнее, но и эффективность такого хранилища будет выше. Например цифровую информацию можно будет легко обрабатывать средствами СУБД. Можно использовать статистические функции СУБД. Для такой БД нужно значительно меньше дискового пространства в силу специфического формата хранения данных и исключения дублирования данных, а значит и поиск будет вестись быстрее, особенно при оперировании миллионами объектов.

Наиболее простая и функциональная структура БД (таблицы):

1. Информация
2. Организация
3. Лицо
4. Адрес
5. Телефон
6. Проект
7. ...

Если не учитывать Microsoft Excel, Microsoft Access или Google Sheets, то вот инструменты, подходящие для организации персонального хранилища данных у себя на компьютере.

HeidiSQL

Описание: Бесплатный инструмент для работы с базами данных, поддерживающий MySQL, Microsoft SQL и PostgreSQL.

Преимущества:

- Интуитивно понятный интерфейс.
- Возможность создания и редактирования баз данных.
- Поддерживает русский язык.

Database.NET

Описание: Легкий инструмент для работы с различными форматами баз данных, включая MySQL, SQLite и PostgreSQL.

Преимущества:

- Не требует установки — можно запускать с флешки.
- Поддержка экспорта в форматы CSV, XML и TXT.
- Поддерживает русский язык.

Готовые решения для хранения

Таких решений не мало если начать искать через Гугл или Яндекс. Но каждый раз вы будете сталкиваться с тем, что в очередном найденном решении что-то да не так как вам надо. Увы, но идеальное решение найдется с трудом. Ниже приведены некоторые из подобных сервисов.

1. <https://obsidian.md/> неплохо подходит для построения графиков и представления каких-либо знаний, соответственно и для этого он тоже подойдёт.
2. <https://www.thebrain.com/> ещё одна программа, которая в отличие от предыдущей есть только на Windows и Mac

Формирование отчета

Нет, это не ошибка. Вначале, еще до начала анализа, поговорим о результате аналитической деятельности – об отчете в самом широком смысле этого слова.

Называться это может по-разному справка, досье, рекомендации, уведомление и т.п. но смысл один – это документ, являющийся результатом работы аналитика по определенному проекту или задаче.

Отчет может быть в виде справки, в виде досье, в виде информационного сообщения или дайджеста, это не важно, в конечном счете это все равно отчет о проделанной работе. Но не просто подтверждение того, что вы провели большую работу и не перечень того, что вы нашли, выяснили или спрогнозировали. Отчет это в первую очередь средство экономии времени заказчика, если только вы не делаете отчет для себя.

Попробуйте ответить себе на вопрос – зачем заказчик (руководитель, клиент...) ставит задачу что-то исследовать и оформить в виде финального документа? Правильно – чтобы сэкономить свое время. Чтобы не тратить свое время на эту работу, отдав ее вам, а сосредоточиться на том, что он лучше знает и умеет, или что важнее и без него не решится.

Поэтому главная ценность аналитического отчета для заказчика в экономии его времени. И именно из этого и нужно исходить, составляя итоговый документ (отчет) в какой-бы форме он не требовался.

А раз так, то вот основные принципы формирования итогового документа анализа:

1. Краткость;
2. Понятность;
3. Достоверность;
4. Своевременность.

Несмотря на кажущуюся простоту и понятность, необходимо детализировать эти принципы.

Краткость прямо связана с главной функцией отчета (экономия времени заказчика) – данные нужно изложить максимально кратко, чтобы не тратить зря времени на прочтение лирических отступлений. При этом краткость не должна идти в разрез с понятностью. Это два противоречивых требования и найти золотую середину не всегда бывает просто. Когда это особенно сложно, то отчет сопровождают объемным «приложением», куда выносят все обоснования, рассуждения, аргументацию. А основная часть отчета остается короткой.

Понятность – данные нужно изложить так, чтобы заказчик не тратил дополнительное время на их понимание, на поиск значения незнакомых терминов или сленга. Именно поэтому отчет должен быть не только на понятном заказчику языке, но и с использованием не просто понятных терминов, но и однозначно трактуемых.

Также данные должны быть достоверными и не только по тому, что на их основе будут приниматься управленческие решения. А еще и по тому, что в противном случае заказчику придется тратить дополнительное время на их перепроверку и вероятнее всего на исправление последствий ошибочного решения.

Со своевременностью еще проще – данные нужны вовремя, а не когда уже поздно что-то предпринимать

И вот теперь, исходя из понимания зачем нужен отчет, посмотрим на то, как он должен быть «организован». Структура отчета так-же как и содержание должна помогать в решении задачи экономии времени. Когда заказчик получает ваш отчет то что он первым видит, на основании чего начинает формироваться его мнение о полезности отчета? Да-да, именно название первым видит заказчик. Именно название в начале формирует восприятие документа. Значит название должно быть не случайное – название отчета это очень краткий ответ на вопрос «о чем отчет».

Основная часть отчета (саммари), содержит помимо его названия, еще и краткое содержание документа, и краткое обоснование выводов. И слово «краткое» тут очень важно. Краткое содержание это чуть более детальное описание, чем название, примерно в один абзац «о чем документ». Это самые важные выводы, прогнозы, рекомендации. А краткое обоснование это ответ на вопрос «почему такие выводы сделаны» и тоже в один абзац. По сути, это объяснение «почему вы так считаете».

Стиль изложения в отчетах также должен отвечать задаче экономии времени заказчика. А это значит, что заказчик не должен тратить время на выяснение что значит тот или иной термин или сленговое выражение. Мало того, что наличие незнакомой терминологии приводит к потерям времени и раздражению, так еще и трактовка сложных терминов может у заказчика отличаться от вашей. В этом случае, созданный вами документ вполне может быть понят иначе, чем вы предполагаете и на его основе будут приняты не верные управленческие решения.

Отчет должен содержать только простые и короткие предложения, желательно без причастных и деепричастных оборотов чтобы к концу прочтения предложения заказчик еще помнил с чего оно началось. И тут основные цели это экономия времени заказчика через понятность содержания и простоту восприятия.

В зависимости от цели исследования отчет может содержать разные составные части помимо названия, краткого содержания и краткого обоснования, но название и саммари должны быть всегда.

АНАЛИЗ ИНФОРМАЦИИ

Анализ информации - это процесс исследования, фильтрации, преобразования и моделирования данных с целью извлечения полезной информации и принятия решений. Целью анализа информации является понимание исследуемой ситуации в целом, выявление тенденций, прогнозирование и получение рекомендаций для принятия решений.

С чего начать

Начать надо с организации рабочего пространства – от этого сильно зависит эффективность аналитика. Удобное рабочее место, полезный инструментарий это конечно важно. Но главный инструмент аналитика это его голова, а точнее способность трезво смотреть на факты, уметь структурировать и стыковать информацию, рассуждать, предполагать, аргументировать.

Аналитическая объективность

Прежде чем приступить к анализу, нужно обратить внимание на некоторые особенности восприятия информации человеком. Они вытекают из тех законов, которые мы рассмотрели выше и достаточно сильно влияют на наше мнение о полученной информации, на наши интерпретации, а порой вообще на способность воспринять информацию.

Основные аспекты аналитической объективности включают:

1. Независимость от субъективных факторов: анализ должен проводиться без влияния личных интересов, предвзятых взглядов или ценностных установок исследователя.
2. Использование научной методологии: применение проверенных методов сбора и анализа данных, которые могут быть проверены и воспроизведены другими исследователями.
3. Критическое мышление: способность рассматривать ситуации и явления с разных точек зрения, учитывая различные аргументы и доказательства.
4. Верификация данных: проверка информации на достоверность, использование множества источников для подтверждения фактов.
5. Открытость к учету новых факторов: готовность пересмотреть свои выводы в свете новых данных или аргументов.

Избирательность восприятия

Мы видим (обращаем внимание) только то, что способны понять, с чем сталкивались ранее, что является нашим опытом. Мы замечаем порой только то, о чем имеем

представление. В этом случае, применительно к анализу текстовой информации, мы реагируем на знакомые слова, названия, выражения, опираясь на прошлый опыт, не понимая общего контекста. Иными словами, на первом этапе изучения мы воспринимаем информацию по ее внешним признакам без понимания содержимого.

Настроенность на определенную информацию

Человек видит то, что хочет видеть. Иными словами, люди более открыты определенной информации, на которую настроены. А зная, что человек хочет видеть, проще его обмануть, преподнеся именно такую информацию, которую он ожидает и внедрив в нее немного полезной для себя информации. Но данные, передаваемые с целью обмана, должны не только быть желанными для объекта воздействия, но и быть достаточно правдоподобными.

Авторитетность источников

Значимость для нас мнения определенных людей. У каждого есть круг лиц, мнение которых принимается с меньшей критичностью. А значит и получаемая от таких людей информация будет восприниматься как более соответствующая действительности.

Мнимая скрытность получения информации

Не секрет, что подслушанная информация кажется более достоверной. Используя этот эффект можно создать видимость случайного подслушивания объектом некой важной информации. И тогда никакая сила его не переубедит.

Новостная система

Предположим вам поставили задачу организовать OSINT в компании. Формулировка практически является цитатой. Вы начали что-то делать, выполнять какие-то поручения, общаться с сотрудниками, искать источники. Но кроме всего прочего, вам нужно решить несколько задач, связанных с OSINT не технически, а скорее политически:

1. Быстро повысить ситуационную осведомленность ТОП-ов;
2. Показать свою полезность;
3. Заинтересовать в результатах своей деятельности руководство среднего звена и сотрудников;
4. Разъяснить чем может быть полезен OSINT для разных подразделений компании.

Именно для решения этих, казалось-бы разных задач, прекрасно подходит создание внутрикорпоративной новостной системы. Новости все читают, мало того в новостях все нуждаются. Но при этом поток информации огромен, а времени читать всё подряд и выбирать нужное нет. Часто еще и навыков не хватает. И вот эту потребность новостная система вполне может закрыть. Причем затрат на это не много – обычно хватает одного часа работы аналитика с утра.

Пока у вас нет собственной мониторинговой системы, для формирования потока релевантных новостей можно использовать Дзен-Новости (бывшие Яндекс.Новости) или Google-Новости. В зависимости от того, из какого региона (страны) новости вас интересуют.

Реализовать такую внутреннюю новостную систему можно в формате закрытого телеграм-канала, отдельного раздела на корпоративном портале или в виде ежедневной рассылки. Главное, чтобы пользователям было удобно читать – это важно. Если будет не удобно, то и читать не будут. А для вас такая новостная система это инструмент формирования правильного мнения сотрудников о вас, вашем подразделении и об OSINT вообще.

В результате такой обзор новостей по рынку начнет формировать подборки сообщений по ключевым игрокам, в том числе конкурентам. По технологиям, по сопредельным рынкам. А это начало создания досье (профайлов) на интересующих вас людей и организации, а также формирование основы для выявления тенденций и прогнозирования.

Кроме того, такая работа заставляет ежедневно погружаться в события на рынке, а это приводит к полезным последствиям. Аналитик, который работает с новостями:

1. Постепенно начинает сам ориентироваться в текущей обстановке и порой лучше многих в компании;
2. Постепенно погружается в проблематику рынка и ориентируется в хитросплетениях связей и взаимного влияния;
3. Становится ходячей энциклопедией по рынку, конкурентам, продукту, технологиям, поставщикам.

Предварительная обработка информации

Предварительная обработка информации — это комплекс операций, выполняемых над входными данными для их подготовки к дальнейшему анализу и использованию. Предварительная обработка информации упрощает дальнейший анализ и делает его более точным и быстрым. Она может включать в себя, в зависимости от особенностей задач, следующие действия:

1. Очистка от «шума» в виде рекламы;
2. Устранение дублей информации;
3. Перевод с иностранных языков;
4. Тегирование, извлечение сущностей;
5. Контроль достоверности;
6. Преобразование данных в форму, удобную для дальнейшей работы с ней.

Здесь мы поговорим о специфических вариантах предварительной обработки, характерной для OSINT.

Точная фиксация сообщения (в т.ч. и система архивирования)

Прежде чем начать анализ информации, необходимо эту самую информацию получить и каким-то образом сохранить. При этом нельзя забывать и о том, что на информацию накладывают отпечаток и сам источник, и канал передачи, и на получателя информации, и на особенности ее хранения. Если только это не показания приборов или средств объективного контроля. Поэтому крайне важно сделать так, чтобы при всех действиях до попадания к аналитику информация ни коим образом не подвергалась изменениям, пусть даже незначительным. В том числе и на этапе хранения и извлечения из хранилища.

Иными словами, поступившая к вам информация должна быть зафиксирована и сохранена в том виде, в каком она поступила. При этом должны быть зафиксированы и атрибуты информации. Далее с информацией можно работать: интерпретировать, сравнивать, стыковать, но исходный материал все так же должен быть неизменен.

Архивирование ни что иное как сохранение полученных данных. Архивирование, безусловно, нужно осуществлять таким образом, чтобы можно было быстро найти нужные данные. Удобнее всего это делать в СУБД, но не всякая программа управления для этого подходит. Качественное проведение данного этапа позволит в последствии делать обоснованные выводы об авторе, о редакции, об издательстве и т.п.

Фиксация атрибутов сообщения

Когда у вас несколько задач, то вы прекрасно помните какая задача от кого и при каких обстоятельствах появился. С чем она связан, каковы его особенности и т.п.. Но как только их число перевалит за пару десятков, вы начнете путать, после полсотни проектов перестанете пытаться запомнить эти тонкости. А полсотни проектов (задач) при нормальной работе вы наберете очень быстро. Чтобы не попасть в ситуацию тут помню, тут не помню, необходимо все эти особенности проектов фиксировать. Тоже самое относится и к особенностям сообщений, получаемых в ходе работы над проектом. А это ни что иное как атрибуты сообщений (информации). Таковых атрибутов, характеризующих информацию по разным признакам, может быть очень много, но есть ряд из них, которые необходимы всегда.

Атрибуты информации, необходимые к сохранению могут отличаться в зависимости от задач. Предположим, вы создадите базу данных на основе публикаций из периодики. Например, для отслеживания действий конкурента. В этом случае для вас будут важны следующие атрибуты:

1. Источник информации (откуда);
2. Автор сообщения (кто создал);
3. Дата поступления информации к вам;
4. Дата создания публикации (сообщения);
5. Канал поступления;
6. Тип сообщения.

Возможны и иные (специфические) атрибуты, необходимые для решения тех или иных задач:

1. на каком носителе поступила информация;
2. в какое время поступила информация (а не только дата);
3. когда была внесена в архив;
4. кто принимал информацию;
5. заказная или редакционная (для статей);
6. если заказная – кто заказчик;
7. на какую аудиторию ориентирована (для СМИ);
8. для кого выгодна;
9. и т.п.

Атрибуция сообщения частично может быть возложена на алгоритмы – это присвоение сообщению дополнительных атрибутов на основе анализа самого сообщения. Это теги, а сам процесс присвоения тегов - тегирование. Например, выделение сущностей, упомянутых в тексте. Это могут быть люди, организации, события, время, место, еще что-то.

Когда вы получили какое-то сообщение, обычно возникают дополнительные вопросы, связанные с содержанием новости. Например, упоминание ранее неизвестного объекта, события, свойств или еще чего-то. В таких случаях необходимо (по возможности, конечно) задать дополнительные вопросы и как-то прокомментировать поступившие сведения. Этот комментарий становится дополнительным атрибутом информации, но исходный текст сообщения должен остаться неизменным.

Мало того, бывает полезно сохранить и дополнительную информацию об источнике, и о канале передачи, и об особенностях ее хранения. Именно для того, чтобы в будущем, когда возможно вы вновь обратитесь к этим данным, вы смогли восстановить в памяти нюансы получения информации. А такое повторное обращение к данным уже отработанного проекта периодически происходит.

Выделение утверждений

Следующий этап первичной или предварительной обработки сообщений – это выделение из текста утверждений. Очень похоже на тегирование, но несколько сложнее. Если традиционно тег — это объект (сущность в широком смысле), то утверждение это отношения между объектами. Утверждения также могут быть дополнительными атрибутами сообщения, но это значительно более сложная система как минимум в силу своей вариативности.

Выделение утверждений необходимо для углубленного понимания наличия связи полученной информации с тематикой вашего исследования. А позже для эффективной интерпретации данных из сообщения.

Для этого из текста выделяют несколько компонентов:

1. компоненты, которые могут быть отнесены к разряду фактов (например, подтверждены иными источниками или известны вам);
2. компоненты, которые потенциально могут быть отнесены к разряду фактов (например, могут быть подтверждены после проверки);
3. компоненты, которые не могут быть отнесены к разряду фактов (заранее известно что обман).

Попробуйте выделить утверждения, потенциальные утверждения и явную ложь из текста:

«Вячеслав Иванов, председатель общества Изучения НЛО, обратился к Президенту РФ Х.Х.Хххх с просьбой предоставить для изучения имеющиеся у военного ведомства материалы о так называемых «квакерах» - аномалиях, неоднократно зафиксированных в мировом океане Российскими подводниками»

Утверждения:

Х.Х.Хххххх – Президент РФ (по тому, что мы это знаем из новостей).

Потенциальные утверждения:

1. существование общества изучения НЛО – возможно такая организация есть, а может и нет. Нужно уточнять;
2. В. Иванов – председатель общества Изучения НЛО;
3. то, что В Иванов обратился с соответствующей просьбой;
4. существование аномалии под названием Квакер;
5. то, что Квакеры неоднократно фиксировали;
6. наличие информации о Квакерах у военного ведомства.

Что еще можно отнести к потенциальным утверждениям? Это зависит от того, для кого или для чего осуществляется анализ информации – каковы цели исследования. Но об этом подробнее в разделах «Формализация» и «Интерпретация».

Далее утверждения проверяют, т.е. выясняется соответствуют утверждения действительности или нет. Самая простая проверка – выявление подтверждения в других источниках.

Параллельно выявляются искажения:

1. утверждения с отсутствием аргументации;
2. утверждения с ложной аргументацией;
3. утверждения с неполной аргументацией.

Эти данные помогут в случае, если анализ осуществляется в рамках исследования фактов манипулирования. В частности, это поможет понять целевую аудиторию манипулирования и используемые злоумышленником приёмы.

Формализация текста

Достаточно важным в работе с текстами является умение передавать смысл сообщения без искажений, понимать, что написал автор и что он хотел сказать. Если у вас есть возможность передать точную копию текста – отлично – так и нужно поступить. Но чаще бывает так, что нужно сжать содержимое нескольких страниц в несколько фраз или запомнить их содержимое, а ведь далеко не все обладают столь феноменальной памятью.

В этом случае на помощь приходит методика понимания содержимого. Это ни что иное как выявление из текста неоспоримых фактов; выдвижение гипотез, которые могут подтверждаться наличием опор в тексте; и предположения по поводу невозможного, но также имеющего опоры в тексте.

Упрощая смысл сказанного, видим, что получатель информации должен обосновывать свое мнение (гипотезу) только посредством имеющихся в тексте сигналов (опор) или попросту не выходить в своих суждениях за границы, очерченные текстом – не интерпретировать.

После выявления утверждений можно формализовать текст. Для формализации текста его нужно пересказать сухим языком, удалив любые образования и надстройки (эмоциональные, психологические, рекламно-пропагандистские, ненормативную лексику, сленг и т.п.). Другими словами – перечислить утверждения из данного текста.

Формализация текста зависит от стоящих перед вами задач. Ведь нужно передать основной смысл, а он может меняться в зависимости от интересов получателя информации.

Например, возьмем новостное сообщение:

«ЦБ заявил об отзыве лицензии у банка «ВостокЗападКредитФинанс» в связи выявленными в ходе проверки нарушениями.»

В зависимости от интересов заказчика анализа формализация может выглядеть очень-очень по-разному:

С точки зрения сотрудников Банка:

ЦБ отозвал лицензию. Банк, как минимум теряет доход и будут задержки с зарплатой.

С точки зрения клиентов Банка:

ЦБ отозвал лицензию. Банк разорится, деньги на счетах потеряем.

С точки зрения куратора от силовиков:

ЦБ отозвал лицензию. Есть нарушения. Вероятно, есть и преступления (отмывание, вывод, обналичка, финансирование...).

Оценка информации

Начнем сразу с примера. Представьте гипотетическую ситуацию: Некая компания «X» работает на рынке кондиционеров. Компания растет и нам интересно в каком направлении она будет развиваться. А точнее - какой сегмент рынка компания «X» будет осваивать в ближайшее время? Автомобильные или напольные кондиционеры?

Для построения своей гипотезы мы располагаем ограниченным набором данных. И обосновать свой вывод можно только чем-то из этих данных:

1. компания «X» участвовала в выставке «Офисные технологии»;
2. компания «X» участвовала в конференции по проблемам использования новых технологий в производстве бытовых кондиционеров;
3. компания «X» выпустила пресс-релиз о создании у себя нового направления – автомобильные кондиционеры;
4. компания «X» разместила объявления о поиске руководителя направления автомобильных кондиционеров;
5. компания «X» приступила к строительству нового цеха;
6. компания «X» направила в компанию Хитачи трех своих сотрудников для обучения;
7. по базам ВЭД (таможня) «X» закупила крупную партию комплектующих для напольных кондиционеров, в т.ч. корпуса;
8. компания «X» опубликовала в СМИ статью-обзор рынка автомобильных кондиционеров.

Так какой сегмент рынка компания «X» будет осваивать в ближайшее время? Автомобильные или напольные кондиционеры?

На основании чего вы сделали тот или иной вывод? Почему какое-то сообщение признано значимым?

Вот это сообщение подразумевает, что компания не только что-то продекларировала, но и потратила деньги с четкой направленностью:

«По базам ВЭД (таможня) «X» закупила крупную партию комплектующих для напольных кондиционеров, в т.ч. корпуса»

Критерии оценки информации (важность, точность, значимость)

Теперь несколько слов о критериях оценки информации. По каждому эпизоду (текстовому блоку, сообщению и т.п.) необходимо принять решение о его полезности для вас, хранения и дальнейшем использовании. Ведь собирать и хранить всю окружающую информацию прямо скажем весьма затратно – для этого требуются колоссальные ресурсы. Позволить себе такое может только очень крупная структура.

Сам процесс выбраковки должен иметь четкие критерии. Для принятия решения о нужности информации осуществляется первичная ее оценка. Критерии первичной оценки должны быть немного закруглены для исключения потери важной информации, но незначительно – иначе поток превратиться в неконтролируемый.

Результатом оценки информации должен стать вывод о ее релевантности, важности, точности, значимости. Для решения наших задач, оценка обычно осуществляется по нижеследующим характеристикам:

1. Объективность – субъективность;
2. Достоверность – недостоверность;
3. Полнота – неполнота;
4. Актуальность – неактуальность;
5. Ценность – бесполезность;
6. Понятность – непонятность.

Часто, для ускорения процесса оценки используют упрощенный набор критериев.

Критерии упрощенной оценки информации

Релевантность информации – наличие связи с проблемой, которую вы исследуете, (соответствие вашим интересам) и способность информации внести вклад в процесс понимания проблемы. Иными словами, необходимо сопоставить данную информацию с вашими информационными потребностями и ответить на вопрос сможет ли помочь она вам чем-то сейчас или в ближайшем будущем? Если да – переходите к следующему этапу, если нет – в корзину (если только она вам не пригодится в другом деле...).

Достоверность информации - это характеристика, отражающая степень соответствия информации объективной реальности. Достоверность информации, если это не показания приборов или телеметрия, обычно оценивается по следующим параметрам:

1. наличие подтверждения из других источников
2. стыкование с другой информацией
3. знание источника и его мотивов
4. авторитет или длительная положительная история работы с источником
5. свойства канала передачи информации

Как видно важнейшее место здесь занимает знание об источнике информации и доверие ему.

Значимость информации - это характеристика, отражающая ценность и важность информации для вас или для решения конкретной задачи. Наиболее важные составляющие значимости информации:

1. понимание информации,
2. полнота освещения предмета интереса,
3. своевременность информации и ее достаточность для принятия решения.

В процессе работы с информацией (на любом этапе) возможно возникновение ситуации, когда для понимания происходящего не хватает данных. В этом случае можно воспользоваться приемом восстановления информации. Суть его в том, что любому событию что-то предшествует, какая-то подготовка, какие-то события и везде остается след. Какие-то процессы сопутствуют основному событию, что-то становится следствием этого события. Нужно уметь восстанавливать последовательность событий и выявлять места, где может остаться информация о событии. Но начинать нужно с обработки уже имеющейся информации. И в этом плане очень важным является процесс аттестации источника информации. Кратко процесс аттестации источника описан ниже.

Установление источника, получателя, их пространственных и временных координат.

Данный шаг выполняется в рамках первичной оценки информации при условии достаточности сил и средств и особенно актуально для сообщений СМИ и слухов. Его результатом может стать понимание важности информации, внешне никак не связанной с объектом интереса. Если источник информации, получатель и их пространственные и временные координаты нельзя прямо установить из содержания, то используются следующие приемы.

Для установления источника используется определение специфики лексикона источника:

1. анализ распределения служебных терминов;
2. определение частоты употребления слов и сопоставление с аналогичными показателями известных источников;
3. сопоставление с аналогичными характеристиками профессиональных, социальных, этнических и т.п. групп.

Ценный результат дает сопоставление статистического анализа с:

1. профессиональными эталонами - для определения профессиональной принадлежности
2. образовательными эталонами – для установления уровня образования
3. авторскими эталонами (статьи СМИ) – для определения авторства, для определения того, что статья писалась под диктовку, для определения подложного авторства

Для установления временного интервала исследуются все имеющиеся в сообщении указания на его принадлежность к некоторому временному интервалу, указанных прямо

или отраженному в ссылках на те события, даты которых известны или могут быть установлены.

Для установления получателя определяем кому может быть интересна данная информация, кто читает данный источник (если это СМИ) и т.д.

На основании собранных данных каждой вновь поступающей порции сведений присваиваются дополнительные атрибуты (см «Фиксация атрибутов сообщения»):

1. кто или что является первоначальным источником информации (или другими словами абсолютный источник данной информации);
2. кто предал огласке информацию (СМИ, автор);
3. когда впервые информация передана огласке (задержка обнародования от времени события);
4. когда опубликована полученная вами информация;
5. статус публикации (редакционная или оплаченная (рекламная) и т.п. если оплаченная то, кем);
6. кому выгодно, а кому нет и почему;
7. однотипные публикации в других СМИ.

Также собирается комментирующая (вспомогательная) информация:

1. другие высказывания или публикации того-же автора (издания, темы, оценка);
2. соавторы и оппоненты по другим выступлениям (если есть);
3. другие публикации в данном СМИ на заданную и близкие темы (авторы, цель, содержание, эмоциональная окраска, оценка);
4. общее отношение автора и источника к данной теме;
5. публикации, сходные по цели, смыслу, содержанию (СМИ, авторы);
6. реакции на публикацию их источники, содержание, эмоциональная окраска (комментарии, контрвыпады, критика и т.п.).

Установление фактографической составляющей текста, его тематики.

Данный шаг так же необходим для понимания корреляции полученной информации с тематикой исследования и ее полезности, а по тому выполняется в рамках настоящего этапа. Вначале, как и в формализации из текста выделяют:

1. компоненты, которые могут быть отнесены к разряду фактов (например, подтверждены иными источниками);

2. компоненты, которые потенциально могут быть отнесены к разряду фактов;
3. компоненты, которые не могут быть отнесены к разряду фактов.

Соответственно выявляются направления для дополнительного исследования и направления, на которые не стоит тратить силы. Далее определяется каким образом можно подтвердить или опровергнуть потенциальные факты. При этом нельзя забывать об искажениях, вносимых в текст:

1. непреднамеренные логические ошибки;
2. некорректное построение грамматических конструкций;
3. преднамеренное искажение;
4. эмоциональные искажения.

Поэтому важно выявить в тексте наличие причинно-следственных связей.

Например, возьмем всё тоже сообщение:

«Вячеслав Иванов, председатель общества Изучения НЛО, обратился к Президенту РФ В.В. Путину с просьбой предоставить для изучения имеющиеся у военного ведомства материалы о так называемых «квакерах» аномалиях, неоднократно зафиксированных в мировом океане Российскими подводниками»

К потенциальным фактам (после проверки) мы отнесли:

- В Иванов – председатель общества Изучения НЛО
- то, что В Иванов обратился с соответствующей просьбой
- существование аномалии под названием Квакер
- наличие информации о Квакерах у военного ведомства

Нужно определить как проверить выявленные потенциальные факты:

1. где можно получить подтверждающую или опровергающую информацию;
2. кто может подсказать;

Также анализируется полнота и непротиворечивость аргументации. Вначале текст нужно привести в формализованный вид. Иными словами, его нужно пересказать сухим языком, удалив любые образования и надстройки (эмоциональные, психологические, рекламно-пропагандистские, ненормативная лексика, слэнг и т.п.). Очень похоже на резюмирование.

У вас получится перечень аргументов (утверждений). Далее выявляются искажения (отсутствие аргументации, ложная аргументация, неполная аргументация и т.п.).

Пример, берем тоже сообщение в расширенном виде:

«Недавно, после необъяснимых событий в Северной Атлантике, приведших к неоправданным человеческим жертвам, Вячеслав Иванов, председатель общества Изучения НЛО, направил Президенту РФ В.В. Путину письмо с требованием незамедлительно предоставить для изучения имеющиеся у военного ведомства материалы о так называемых «квакерах» аномалиях, неоднократно зафиксированных в мировом океане Российскими подводниками. В данном послании, в частности говорится, что замалчивание данных фактов является одной из основных причин гибели людей и вся ответственность за это лежит на военных и на президенте России.»

Попробуем формализовать сообщение:

- в Северной Атлантике произошел инцидент с гибелью людей;
- В Иванов – председатель общества изучения НЛО – направил Президенту РФ письмо
- в письме присутствует требование предоставить информацию и обвинение военного ведомства и Президента в замалчивании информации и в гибели людей

Что я упустил?

- наличие у военных информации об аномалии под названием Квакеры
- связь Квакеров с подводниками
- связь Квакеров с инцидентом в Северной Атлантике

Далее проверяется аргументация. В приведенном примере аргументации нет. А есть попытка на эмоциональном уровне очернить руководство страны и Министерство Обороны. Чтобы сообщение было аргументировано в нем должны присутствовать неопровержимые (или легко проверяемые) факты.

При углубленных или специализированных исследованиях устанавливается эмоциональная составляющая текста и системы оценочных суждений - текст анализируется на наличие слов, терминов, словообразований способных воздействовать на эмоциональное состояние потребителя сообщения. Это позволяет, в сочетании с анализом специфики лексики источника, выявить систему ценностей источника и определить поведенческие особенности этого источника. Второй составляющей данного этапа является фильтрация оценочных суждений источника.

Также устанавливается цель генерации текста. Данный этап возможен если установлен потребитель текста (по аудитории того СМИ, которое его опубликовало). Тогда анализируется модель окружающего мира потребителя (в части содержимого сообщения) и сравнивается с предлагаемой моделью в тексте сообщения. Под моделью окружающего

мира подразумевается представление этого самого мира (мироустройства) или его части, - то как человек для себя понимает что происходит вокруг него.

Если модели совпадают или отличаются незначительно – обычное общение. Если модели различаются значительно – источник преследует цель побуждения потребителя к неким действиям. Если в модели окружающего мира потребителя никак не отражена описываемая источником область (потребитель ничего не знает об этом) – налицо формирование модели (представления), а вот с какой целью – в данном случае необходимо разбираться отдельно.

В случае с приведенным выше примером сообщение было опубликовано в газете «НЛО». Основная аудитория – обыватели, не имеющие высшего образования, работающие исполнителями, в возрасте от 20 до 30 лет. Их ключевые представления (модель мира):

1. правительство заботится только о собственном кармане
2. все предприниматели сволочи, а всем руководителям наплевать на подчиненных
3. мы никому не нужны
4. главное выжить в данный момент

В приведенном тексте предлагается следующая модель мира:

1. руководству страны безразлична судьба моряков

А параллельно внедрено несколько нарративов:

1. В Иванов проявляет заботу о моряках
2. В Иванов не боится самого Президента

А теперь ваши выводы – какова цель генерации текста? Варианты:

1. показать наличие организации, борющейся за права обездоленных;
2. показать В Иванова как лидера в данной борьбе;
3. заявить о себе, привлечь внимание к себе через привлечение внимания к ситуации;
4. популяризировать деятельность Общества изучения НЛО;
5. привлечь внимание к себе возможных спонсоров из-за океана;

Оценка сведений (вне контекста)

Параллельно с оценкой сообщения и установлением фактографических данных происходит и оценка сведений (вне контекста):

1. эмоциональная напряженность и окраска текста;
2. стиль сообщения;
3. совпадение стиля с другими текстами того-же автора;
4. заимствования (и естественно откуда);
5. внутренняя непротиворечивость сведений;
6. непротиворечивость сведений по отношению к известными данными.

Приведенный метод достаточно обширен и требует определенного времени и опыта. При недостатке ресурсов использовать его следует эпизодически – по отношению к конкретным проектам, а в некоторых ситуациях к конкретным группам сообщений.

Анализ текстовой информации

Если откинуть академические формулировки, то анализ информации такое преобразование полученных сведений, в результате которого появляется новый информационный продукт. Как минимум краткий обзор, а лучше прогноз возможных изменений (развития) и рекомендации по использованию возможностей или нивелированию угроз.

Простые методы анализа

Начнем с совсем простых технологий. Вы наверняка их уже используете каждый день и не один раз, но попробуйте взглянуть на эти технологии с точки зрения анализа.

Реферирование информации.

Реферирование заключается в выборке из всего массива информации ключевых моментов и их фиксации. Умение быстро составить качественный реферат достаточно непростое свойство. В настоящее GenAI хорошо справляется с этой задачей при условии правильно составленного промта. Но если вы планируете заниматься анализом, то должны научиться делать это своей головой.

Реферирование особенно полезно в случае большого объема информации из разных источников (СМИ, БД, опер установки и т.п.) и при необходимости дальнейшего цитирования. Но реферирование всегда ориентировано на объект интереса, т.е. при реферировании информация делится на полезные и не важные элементы. Мало того, тот, кто реферировать - определенным образом сам искажает информацию.

Мы уже частично попробовали реферирование при формализации текста, когда удаляли из сообщения элементы, не несущие полезной информационной нагрузки для решаемой задачи. Теперь же взглянем на эту процедуру как на один из вариантов анализа.

Обычно при реферировании исследуемый текст читается три раза. При первом прочтении выделяются слова, несущие основную смысловую нагрузку – ключевые слова – они выделяются. Это могут быть имена, названия, даты, профессиональные выражения и т.п. – зависит от задачи.

При втором прочтении внимание концентрируется на ключевых словах, при этом выделяются короткие, не содержащие ничего лишнего словообразования (словосочетания), отражающие основные мысли исследуемого текста и характеризующие ключевые слова – также выделяются.

На третьем прочтении внимание обращается только на выделенные словообразования и на их основе строятся простые, краткие предложения, описывающие смысл сообщения. После чего делается вывод об основном смысле изучаемого текста.

Есть иной способ резюмирования – текст делится на законченные блоки (например абзац) и содержание этих блоков пересказывается каждый в одном предложении. Перечень этих предложений становится рефератом текста.

Аналогия

Аналогия - от греч. сходство, подобие, близость. Аналогия - вид умозаключения, при котором знание, полученное при изучении объекта «А», переносится на менее изученный объект «В», сходный с объектом «А» по существенным для вас свойствам. Рассуждая по аналогии, мы начинаем с явления, о котором хотим получить дополнительные сведения. В поисках этих сведений мы обращаемся к подобному явлению, имевшему место в прошлом. Например, мы хотим понять жарко ли будет в августе этого года в Анапе. Мы обращаемся к данным по Анапе за тот же период в прошлом году и делаем соответствующее заключение.

Пример использования аналогии. Если мы знаем, как и из чего складывается себестоимость продукции на нашем предприятии, то, зная некоторые нюансы производственного процесса, можем предположить структуру себестоимости на аналогичном предприятии конкурента.

Другой пример аналогии. Изучая некое физическое лицо можно понять его взгляды, отношения к определенным проблемам по аналогичным показателям его друзей (лиц, с кем объект поддерживает стабильные дружеские отношения). И спрогнозировать его действия в той или иной ситуации.

Серьезный недостаток аналогии - опасность распространения выводов далеко за действительно оправданные пределы.

Преимущество аналогии - простота, легкость освоения и скорость использования.

Сопоставление информации

Это ни что иное как сравнение двух и более предметов (объектов) с целью выявления расхождений, соответствия или совпадающих элементов. В нашем случае -нахождение в тексте данных, указывающих на связь с вашими интересами (время, место, участники и т.п.). Сопоставление имеет важное значение для последующего хранения и использования материала и осуществляется в два приема:

- систематизация сведений – разбиение всего массива информации на блоки по какому-то признаку – выделение фактов;
- собственно сопоставление – поверхностный анализ с целью выявления явных и возможных связей с объектом изучения и с иными «кусочками» информации.

При использовании компьютерного анализа такие связи можно выявлять по упоминаемым сущностям, по датам, по действующим лицам, по месту свершения события, по названиям, по сферам интересов, по телефонам и т.д..

Например, сфера наших интересов – некая организация с названием «Общество изучения НЛО». Мы получили сообщение (для простоты то-же что и ранее, но более развернутое):

«08.047.2001 в 300 милях южнее острова Гренландия пропал авианесущий крейсер Слава. Последний сеанс связи состоялся в 7:00 по Гринвичу и носил эпизодический характер. Было получено три обрывка передаваемой информации, содержание которых не разглашается. Как стало известно нашему источнику, в этих отрывках сообщалось о множестве квакеров в непосредственной близости от корабля и необъяснимых переboях в работе бортовой аппаратуры. После чего связь прервалась, а космические системы слежения перестали фиксировать корабль. В тот же Вячеслав Иванов, председатель общества Изучения НЛО, направил Президенту РФ В.В. Путину письмо с требованием незамедлительно предоставить для изучения имеющиеся у военного ведомства материалы о так называемых «квакерах», аномалиях, неоднократно зафиксированных в мировом океане Российскими подводниками. В данном послании, в частности говорится, что замалчивание этих фактов является одной из основных причин гибели людей и вся ответственность за это лежит на военных и на президенте России. Интерес к данному происшествию проявляют спецслужбы всех ведущих держав. В предыдущих заявлениях В Иванов заметил, что в области изучения подобных феноменов его организация тесно сотрудничает с Британской МИ-6 и Американским ЦРУ.»

Что в тексте указывает на то, что данное сообщение нам интересно? - прямое указание Общества изучения НЛО;

Далее выясняем, что может идентифицировать это общество или, иначе говоря, стать его смысловым синонимом?

1. поскольку олицетворением Общества является его руководитель В Иванов, то он автоматически становится объектом изучения;
2. далее мы видим явный интерес общества к феномену Квакеров;
3. также просматривается связь Общества с МИ-6 и ЦРУ, хотя она может оказаться блефом.

После этого начинаем поиск подтверждающей или опровергающей информации в доступном массиве по выявленным фактам и признакам:

1. информация о И Иванове
2. информация о феномене квакеров

После сбора сопоставляем полученную информацию и:

1. подтверждаем или опровергаем данные;
2. обогащаем свои знания об объекте интереса.

Описание и его методы.

Описание — это словесная модель исследуемого объекта. Описание производится в рамках той задачи, которую аналитик ставит перед собой. Описание служит лишь умозрительному познанию, показу различных сторон изучаемого объекта или события. С помощью описания информация приводятся к такому виду, который позволяет использовать ее в качестве материала для объяснения происходящего.

Описывать событие – значит отвечать на вопросы о его качественных и количественных сторонах. Эти вопросы формулируются очень просто: "какой, какое, какая, сколько" и т.д. Поэтому описание отличается от простой констатации фактов, которая лишь отвечает на вопросы: "что", "где", "когда". При констатации аналитик показывает наличие или отсутствие некоего объекта или события. А при описании он обращает внимание на их свойства.

Главное при описании заключается в характеристике объекта интереса, то есть в выяснении качеств, а особый интерес при этом уделяется качествам, свойственным только этому объекту, либо узкому кругу объектов. Иными словами, тому, что выделяет его из общей массы подобных. Аналитик прежде всего должен выявить те особенные качества явления, которые дают наиболее полное представление об исследуемой стороне этого предмета. Чем детальнее, правильнее в этом смысле описание, тем больше сведений дает оно о том, что описывается. Описание есть извлечение утверждений об описываемом объекте (явлении) из имеющегося материала (текста). По сути, это та же формализация текста, но с поправкой на объект вашего интереса.

Например, наш объект интереса все то-же Общество изучения НЛО. Пока это все что мы знаем о данном объекте. У нас есть единственное сообщение и на основе него нужно составить описание Объекта интереса:

«08.07.2001 в 300 милях южнее острова Гренландия пропал ракетный крейсер «Новгород». Последний сеанс связи состоялся в 7:00 по Гринвичу и носил эпизодический характер. Было получено три обрывка передаваемой информации, содержание которых не разглашается. В тот же день Вячеслав Иванов, председатель общества Изучения НЛО, направил Президенту РФ В.В. Путину письмо с требованием незамедлительно предоставить для изучения имеющиеся у военного ведомства материалы о так называемых «квакерах», аномалиях, неоднократно зафиксированных в мировом океане Российскими подводниками. В данном послании, в частности говорится, что замалчивание этих фактов является одной из основных причин гибели людей и вся ответственность за это лежит на военных и на Президенте России.»

Интерес к данному происшествию проявляют спецслужбы всех ведущих держав. В предыдущих заявлениях В Иванов указал, что в области изучения подобных феноменов его организация тесно сотрудничает с Британской МИ-6 и Американским ЦРУ.»

Какими качествами (свойствами) обладает наш объект интереса, исходя из данного сообщения:

1. руководитель Общества И Иванов;
2. Общество занимается изучением необъяснимых феноменов, по крайней мере внешне;
3. руководитель Общества не боится громких заявлений и старается привлечь внимание (к себе, к Обществу, к проблеме);
4. Общество проявляет значительный интерес к тому же событию, что и спецслужбы ведущих держав;
5. вероятна связь между Обществом и МИ-6 и ЦРУ.

Группировка данных.

Этот метод заключается в упорядочивании данных по определенным признакам. Группировка позволяет связать разрозненные факты в единую систему, соответствующую тому или иному предположению, рабочей гипотезе и т.п.. Группировка может производиться по разным признакам в зависимости от задачи, поставленной автором. Например, по датам, по месту происшествия, по связи с неким объектом.

Получая информацию о некой компании, мы обычно группируем эту информацию в следующие блоки:

1. Идентифицирующая информация;
2. Контактная информация;
3. Ресурсы компании;
4. Проблемы и конфликты;
5. Персонал компании;

и т.д....

В результате получаем справку (отчет) с простым и понятным содержанием, в котором удобно ориентироваться.

Исторический метод (ретроспективный анализ) — это один из вариантов группировки данных. Все поступающие данные группируются по времени описываемых событий. Так формальное (по документам) изучение кандидата это в первую очередь структурирование данных о нем из разных источников по времени – ретроспективный анализ, а уж после этого выявление угроз, формулирование прогнозов по кандидату и т.п..

Декомпозиция

Декомпозиция или другое название - последовательное решение более простых проблем. Начинается такой анализ с четкой формулировки цели. Эта цель формулируется в виде вопроса, ответ на который и есть то, что вы хотите получить.

Например «как поведет себя господин А в такой-то ситуации?» или «какого уровня может достичь в своем развитии предприятие Б?» или более приземленное «какие силы могут противодействовать при покупке бизнеса Л и как их нейтрализовать?».

И чем четче сформулирован вопрос, тем точнее и дешевле будет ответ.

После того как сформулирована основная цель нужно определить ее подцели, без которых нельзя ответить на основной вопрос. Другими словами, отвечаете на вопрос «что вам нужно что бы достичь основной цели (или ответить на основной вопрос)».

Определив подцели спускайтесь на следующий уровень по тому же принципу и так пока не дойдете до элементарных вопросов, ответы на которые можно получить простыми действиями.

Причинно – следственный анализ и его методы.

Причинная зависимость — это связь явлений, одно из которых порождает другое. Первое явление называется причиной, а второе следствием. Во времени причина всегда предшествует следствию. Но причинно–следственную связь нельзя сводить к простой последовательности событий. Из того, например, что самолет взлетает после того, как в него загружают багаж, не следует, что факт появления багажа на борту есть причина полета воздушного судна.

Логические методы причинно–следственного анализа

Метод исключения

Суть этого метода заключается в том, что, анализируя сложный комплекс причинно–следственных отношений, можно обнаружить непосредственную причину путем исключения всех предполагаемых обстоятельств (реально не влияющих, хотя и присутствующих), способных вызвать сходные события, кроме одного фактора, который после тщательной проверки и принимается за причину изучаемого явления.

Метод сходства

Использование метода сходства обусловлено тем, что интересующие события, причину которых аналитик хочет установить, возникают в самых разных обстоятельствах, но при этом всегда при наличии одного и того же фактора. Сущность этого метода сводится к следующему: если наблюдаемое событие возникает в различных обстоятельствах, но при наличии одного общего фактора, то этот фактор и есть причина происходящего. Используя данный метод, можно изучить разные условия возникновения одного и того же события и вычислить из них один и тот же общий фактор, вызывающий это явление. С определенной долей вероятности можно утверждать, что этот фактор и есть причина, интересующая аналитика.

Метод одного различия

Сей метод сводится к сопоставлению случая, когда интересующее событие наступает, со случаем, когда оно не наступает. В обоих случаях должны быть одни и те же условия, за исключением одного, которое в одном из случаев отсутствует. Иначе говоря - если в одних и тех же обстоятельствах при наличии какого-то фактора событие наступает, а при его отсутствии исследуемое явление не происходит, то этот фактор и есть причина изучаемого явления.

Гипотетический метод

Началом объяснения причины события чаще всего становится гипотеза. Под гипотезой понимается неким образом обоснованное, но нуждающееся в более глубоком доказывании предположение о причине исследуемого аналитиком факта. Гипотеза представляет собой умозаключение, в котором есть неизвестные элементы. Создавая гипотезу, пользуются аналогией, индуктивным, дедуктивным методами. Часто, при выяснении причины исследуемых событий аналитик прибегает к аналогии.

Интерпретация данных

Интерпретация данных — это разъяснение неясного или скрытого, установление содержания, смысла или значения данных, их истолкование.

Первый этап интерпретация данных — это **понимание полученной информации** - выделение утверждений и формализация текста. Формализуйте полученный материал - составьте список утверждений из текста. На данном этапе вы отвечаете на вопрос – что это такое или что произошло? Если вы смогли на основании выбранных утверждений ответить на этот вопрос, то можно переходить к следующему этапу.

На втором этапе вы **объясняете выбранные утверждения** – оцениваете возможность данного события и описываете его свойства. При этом отвечаете на вопросы какой, зачем?...

И в заключении **определяете возможные причины и последствия** – строите наиболее вероятную гипотезу, объясняющую смысл произошедшего, предлагаете рекомендации как использовать открывающиеся возможности или как избежать рисков.

Но результат интерпретации данных сильно зависит от потребностей заказчика и знаний аналитика. Возьмем пример с Африканским конфликтом:

Между Африканскими странами Мон-Дисо и Бовия вновь обострился конфликт из-за спорной провинции Хайдо. Этот конфликт в свое время унес жизни на менее полутора миллионов людей и длился долгих семь лет. Но усилиями ООН, последние шесть лет, удавалось не допускать прямых столкновений. Однако вчера войска Бовии перешли демаркационную линию, захватили несколько населенных пунктов, но были остановлены ополчением Мон-Дисо.

Как это сообщение интерпретировать точки зрения поставщиков оружия?

Понимание ситуации

Между странами Мон-Дисо и Бовия начались военные действия, которые являются продолжением застарелого конфликта.

Объяснение (свойства, особенности, причины)

В прошлом эта война потребовала большое количество легкого стрелкового вооружения и мин (конфликт унес жизни на менее полутора миллионов людей и длился долгих семь лет).

Гипотеза (прогноз, рекомендации)

- 1 Новый конфликт будет не менее кровопролитным и потребует серьезных ресурсов у обеих сторон.
- 2 Можно хорошо заработать на поставках оружия обеим воющим сторонам.

Возьмем тот-же пример:

Между Африканскими странами Мон-Дисо и Бовия вновь обострился конфликт из-за спорной провинции Хайдо. Этот конфликт в свое время унес жизни на менее полутора миллионов людей и длился долгих семь лет. Но усилиями ООН, последние шесть лет, удавалось не допускать прямых столкновений. Однако вчера войска Бовии перешли демаркационную линию, захватили несколько населенных пунктов, но были остановлены ополчением Мон-Дисо.

А как это сообщение интерпретировать с точки зрения авиаперевозчиков?

Понимание

Между странами Мон-Дисо и Бовия начались военные действия.

Объяснение

- 1 В прошлом в этом конфликте не замечено применение авиации и средств ПВО.
- 2 У обеих сторон нет средств для закупки авиации и средств ПВО.

Гипотеза

- 1 Новый конфликт будет без применения авиации и ПВО, их нет у сторон конфликта.
- 2 Максимум, чего можно опасаться, это обстрел стрелковыми вооружениями, потолок которых составляет 5000 метров.
- 3 Самолетам, над этими территориями, нельзя снижаться ниже 6000 метров. В этом случае нет необходимости изменять курс и тратить дополнительное топливо.

Видите, как сильно отличается интерпретация данных в зависимости от потребностей заказчика и знаний аналитика?

Творческие методы

Этот набор методов анализа неструктурированной информации называют так по тому, что они требуют наличия воображения и подразумевают творческий процесс.

Построение последовательности событий

Еще его называют Исторический метод. Все поступающие данные выстраиваются по времени описываемых событий. После чего определяется, что за чем следует, какой факт какое событие предопределяет, что чему сопутствует и т.п., Иначе говоря, восстанавливается хронология событий. Это один из наиболее простых способов и достаточно эффективных.

При построении цепочки событий, особенно если аналогично рассматриваются и параллельные происшествия, становится многое понятно. Используя данный метод можно выяснить как развивались события, что за чем следует и что чему предшествует, можно выявить определенные закономерности.

Анализ связей

Определение всего, что так или иначе связано с изучаемым объектом или событием. Такие связи могут быть явными и неявными. К явным относятся прямо установленные, то как учредитель – учрежденный, продавец – покупатель, родственники и т.п. К неявным относятся те связи, которые нельзя доказать фактами, но которые могут существовать. Например, один юридический адрес у нескольких организаций может указывать на то, что они созданы одной юридической конторой, а на основе этого можно предположить и более значимую связь, которая безусловно требует дополнительной проверки. Неявные связи не являются фактами, но они указывают на то, в каком направлении нужно вести поиск. А это уже задание оперативникам. Результат анализа связей отображается в виде схемы связей.

Простой пример. У нас есть некий текст:

ООО Василек учредили Петя и Федя поровну еще в период совместной учебы в институте. А ООО Гог поставляет в ООО Василек сырье, беря его неизвестно откуда. В своё время Петя учредил ООО Газ и вместе с Ваней очень необычное ООО Бум. Позднее ООО Газ и ООО Бум учредили ООО Фобос. ООО Фобос, для оптимизации налогообложения, учредило ООО Серп и с Ваней ООО Бриг для более эффективной работы на параллельных рынках. Как стало известно недавно, ООО Бриг поставляет сырье в ООО Гог.

Для начала формализуем его:

1. ООО Василек учредили Петя и Федя поровну
2. А ООО Гог поставляет в ООО Василек сырье
3. Петя учредил ООО Газ и вместе с Ваней ООО Бум
4. ООО Газ и ООО Бум учредили ООО Фобос
5. ООО Фобос учредило ООО Серп и с Ваней ООО Бриг
6. ООО Бриг поставляет сырье в ООО Гог

А затем, на основе этих формализованных данных, рисуем диаграмму связей.

Анализ силы связей.

Данный прием хорошо иллюстрируется анализом телефонных контактов. Все контакты (связи) между объектами сортируются в зависимости от того, между кем они возникают. Затем оцениваются по частоте возникновения либо по продолжительности действия. На основе данных о силе связей строятся гипотезы и вырабатываются рекомендации для дальнейшего поиска.

Таким образом хорошо анализировать детализацию телефонных контактов. Если у вас есть такая детализация за определенный период вы можете определить с каким абонентом у исследуемого наиболее тесные контакты, с кем контакты в нерабочее время, с кем в рабочее. Если такую статистику сравнить со статистикой одного из контактеров исследуемого лица, то можно выявить еще и их общие контакты, и их плотность.

Например

Иванов за исследуемый период общался:

- с Петровым 4 раза
- с Сидоровым 2 раза
- с Сергеевым 7 раз

Напрашивается вывод о том, у Иванова с Сергеевым наиболее плотные контакты. Далее можно строить гипотезы и собирать дополнительную информацию. Например, посмотреть повнимательнее на Сергеева и Петрова.

Анализ возможностей

Это выявление всех благоприятных возможностей в исследуемой проблеме, которые могут быть использованы для достижения поставленной цели или слабых мест (угроз), которые могут помешать такому достижению.

Результатом анализа возможностей является перечень этих возможностей или угроз с их краткой характеристикой, вариантами использования и возможными результатами использования.

Выполнение анализа возможностей полезно по тому, что:

1. вы видите все возможные варианты развития событий;
2. вы можете заранее спланировать свои действия в случае развития событий по тому или иному сценарию;
3. вы можете выбрать наиболее простой способ и эффективнее распределить ограниченные ресурсы для достижения поставленной цели;
4. вы можете прогнозировать действия оппонента.

Ситуация:

Вы действуете на рынке пластиковых панелей для отделки помещений. Основных игроков два – ваше предприятие и один из ваших конкурентов. Весь объем продукции импортируется. Ваш основной конкурент планирует инвестировать в новое производство панелей на территории РФ. Вам известно, что такое инвестирование потребует от него вывода из оборота до четверти денежной массы.

Перечень возможности, которые предоставляет вашему предприятию такая ситуация.:

У конкурента некоторый (не малый) период времени будут серьезные затруднения с оборотными средствами – он не сможет кредитовать клиентов так же как и вы, а значит ваши условия будут более интересны – вы сможете увеличить свое присутствие на рынке.

Перечень угроз:

После ввода в действие производства себестоимость продукции конкурента скорее всего будет ниже вашей и его условия станут для клиентов более привлекательными.

Анализ сценариев

В данном случае, основываясь на существующих положении дел и тенденциях, аналитик пытается нарисовать картину развития ситуации. Наиболее распространен способ, при котором рассматривается три варианта развития событий: пессимистический, реалистический и оптимистический сценарии.

Перед тем как начать рисовать сценарии нужно тщательно изучить силы, влияющие на исследуемый объект (или ситуацию):

1. что за силы могут влиять, посредством чего происходит влияние,
2. с какой активностью происходит влияние,
3. устанавливаются причинно-следственные связи самой процедуры влияния.

А в процессе описания сценариев полезно иметь перед глазами список этих сил. Обычно написание сценариев начинается с вопроса типа «если объект X почувствует, что его компания теряет рынок, что он предпримет?»

Прогнозирование

Прогнозирование – это обоснованное суждение о возможном состоянии какого-либо явления в будущем. Именно обоснованность суждений отличает прогноз от гадания. Фактически мы уже занимались прогнозированием в ходе работы с использованием творческих методов (Анализ сценариев, Анализ возможностей). Но есть одна интересная методика – построение диаграммы развития событий.

Такая диаграмма является визуализацией анализа возможностей и анализа сценариев. Поэтому переходить к ее построению полезно после использования указанных технологий.

Построение диаграммы развития осуществляется следующим образом. Вначале отмечается исходная точка, из которой начинается анализ. Обычно это известное вам состояние объекта либо ситуации.

После чего определяются возможные варианты воздействия сил на объект (ситуацию). Затем, исходя из возможных вариантов воздействия (давления) сил, определяются варианты развития – обычно берется три: реалистичный, пессимистичный и оптимистичный и определяются следующие точки, которые изучаются также и результат наносится на диаграмму.

И так до достижения одной из ветвей диаграммы цели вашего исследования (требуемого состояния).

Комплексный инструмент анализа

Обычно одной технологии редко бывает достаточно для обработки неструктурированной информации и поэтому чаще всего используется комплексный подход.

Определение цели

Начиная работу по анализу, с самого первого шага, необходимо четко представлять цель, к которой идете. Эта цель формулируется в виде вопроса, ответ на который и есть то что вы хотите получить.

Например «как поведет себя господин А в такой-то ситуации?» или «какого уровня может достичь в своем развитии предприятие Б?» или более приземленное «какие силы могут противодействовать при покупке бизнеса Л и как их нейтрализовать?». И чем четче сформулирован вопрос, тем точнее и дешевле будет ответ.

Иногда бывает непросто сформулировать цель. Но это необходимо делать по тому, что невозможно достигнуть цели не зная ее.

Построение дерева целей

После того как сформулирована основная цель нужно определить подцели, без которых нельзя ответить на основной вопрос. Определив подцели спускайтесь на следующий уровень и так пока не дойдете до элементарных вопросов, ответы на которые можно получить простыми действиями. Таким образом формируются группы вопросов со своим главным вопросом, а из групп главных вопросов формируется основной вопрос, ответ на который нам и нужен.

Возьмем уже озвученный вопрос - «какого уровня может достичь в своем развитии предприятие Ч?». Для ответа на него нужно выяснить следующее:

1. каково текущее состояние предприятия?
2. каковы возможности и преимущества предприятия?
3. каковы угрозы и слабости предприятия?
4. каковы намерения сил, влияющих на предприятие?

А далее надо выяснить что нужно для ответа на эти вопросы:

Каково текущее состояние предприятия (описание состояния объекта в настоящий момент)

1. Руководство (ТОП менеджмент)
2. Владельцы (учредители, акционеры)
3. Создаваемый продукт (продукция или услуга)
4. Краткая история объекта
5. Имущество (земля, здания и сооружения, станки и оборудование, не реализованная продукция, незаконченное производство, сырье и материалы, ценные бумаги и обязательства и т.д. и т.п.)
6. Партнеры (поставщики, клиенты и т.п.)

7. Показатели (финансовые, производственные и т.п.)

Каковы возможности и преимущества (описание всех ресурсов предприятия и его преимуществ)

Возможности:

1. Административные возможности (лобби, связь со властью, зависимость власти от предприятия, возможность влиять на решения властных структур и т.п.)
2. Экономические возможности (возможности по наращиванию объемов производства, по переориентации производства, по повышению качества, по снижению цены, по привлечению инвестиций и получению кредитов и т.п.)
3. Криминальные возможности (возможность использовать криминал, зависимость от криминала, заинтересованность криминала в предприятии, планы криминала по отношению к предприятию и т.п.)
4. Научно-технические возможности (взаимодействие с НИИ, модернизация технологий, вложения в науку, иное участие в научной деятельности)
5. Рыночные возможности (сильная конкурентная позиция, рост спроса, рыночная власть производителя, отсутствие товаров-заменителей)

Преимущества:

1. Продукция (высокое качество, низкая себестоимость)
2. Ценообразование (четко выработанная цена)
3. Продвижение (сильная реклама, лобби в среде основных потребителей)
4. Сервис/персонал (высокий профессионализм персонала, развитие сотрудников, социальные программы, сервисная поддержка, торговые марки и позиционирование)
5. Инжиниринг и разработка новых продуктов (модернизация оборудования, совершенствование технологий, повышение качества)
6. Сбыт и маркетинг (непрерывный мониторинг рынка, стимулирование сбыта)
7. Менеджмент (низкие расходы на управление, мобильная структура, единая координация, быстрое прохождение управляющих сигналов)

Каковы угрозы и слабости (описание слабых сторон бизнеса и существующих угроз)

Угрозы:

1. Административные (лобби конкурентов, недовольство власти, зависимость предприятия от власти, конфликты с властью)

2. Экономические (перегруженность оборудования, невозможность переориентации производства, невозможность повышения качества и снижения цены, трудности привлечения инвестиций и получения кредитов)
3. Криминальные (давление криминала, зависимость от криминала, заинтересованность криминала в предприятии, планы криминала по отношению к предприятию, конфликты с криминалом)
4. Научно-технические (отсутствие взаимодействия с НИИ, нет модернизации технологий)
5. Рыночные (интенсивность конкуренции, угроза появления новых конкурентов, потребности покупателей на рынке, рыночная власть покупателей, дистрибьюторов, поставщиков, давление со стороны товаров-заменителей)

Слабости:

1. Продукция (низкое качество, высокая себестоимость, моральное устаревание, невостребованность)
2. Ценообразование (необоснованная цена)
3. Продвижение (слабая реклама, отсутствие лобби)
4. Сервис/персонал (низкий профессионализм, притеснение сотрудников, отсутствие социальных программ, нет программы сервисной поддержки)
5. Торговые марки и позиционирование
6. Инжиниринг и разработка новых продуктов
7. Сбыт и маркетинг (рынок не изучается, сбыт не стимулируется)
8. Менеджмент (высокие расходы на управление, неповоротливость структуры, отсутствие единой координации, долгое прохождение управляющих сигналов)

Каковы намерения сил влияющих на предприятие

1. Какие силы влияют или могут влиять на предприятие
2. Ресурсы этих сил
3. Деловая репутация этих сил (история взаимоотношений с партнерами, клиентами, конкурентами)
4. Кредитная история этих сил (история возврата своих долгов и работы с должниками)
5. Поведение в критических ситуациях этих сил (какие шаги предпринимались в кризисных ситуациях, к кому обращались за помощью, кто как проявлялся)
6. Планы этих сил (краткосрочные, долгосрочные, стратегические, в том числе частные планы владельцев и руководства)

Вопросы стали более определенными. Теперь по каждому пункту нужно сказать где информацию можно взять и как. Если источники определены, а затраты приемлемы – можно приступать к сбору данных и описательной стадии работы. При необходимости разложение на составляющие идет дальше.

Синтез данных по пирамиде снизу вверх

После получения всех ответов на подвопросы одной группы можно приступать к формулированию ответа на главный вопрос этой группы. На этой стадии начинается творчество. Хорошо если есть группа людей, которых можно использовать в качестве экспертов. В таком случае можно, основываясь на экспертных оценках, свести к минимуму вероятность ошибки. Но увы – чаще всего приходится работать одному. А раз так – приступаем к присвоению весовых коэффициентов каждому ответу на подвопрос в рамках его группы. Иначе говоря определяем в цифрах (баллах) силу влияния данного ответа на главный вопрос его подгруппы. И в зависимости от результатов выявляем наиболее вероятный ответ. И так пока не дойдем до исходного вопроса.

Прогнозирование как завершающий этап

Безусловно данный метод имеет свои ограничения и дает не однозначный ответ и это необходимо всегда учитывать. Также нельзя забывать и о том, что изучается состояние на сейчас, а в будущем возможны любые изменения. Поэтому давая прогноз необходимо оговаривать условия и границы развития конкретной ситуации:

Прогноз развития:

1. Сценарии воздействия на предприятие возможностей, преимуществ, угроз, слабостей и заинтересованных сил
2. Сравнение с аналогичными ситуациями и объектами
3. Возможные сценарии поведения в тех или иных ситуациях
4. Определение верхних и нижних пределов развития объекта с учетом возможностей, преимуществ, угроз и слабостей

Рекомендации:

1. Что из слабостей и угроз целесообразнее использовать для достижения своих целей
2. Какие возможности и преимущества объекта необходимо нейтрализовать для достижения своих целей

Также нужно отметить и то, что при разложении на 10 составных вопросов, процедура ранжирования и синтеза может проводиться в уме. А при определенном опыте и большее количество ответов на подвопросы может обрабатываться без бумаги. Но когда их число измеряется сотнями – рекомендую все-таки не полагаться на свою память.

А еще...

Не забывайте, что есть специфические методы анализа информации, которые вполне могут пригодиться для решения узкопрофильных задач. Поэтому о них как минимум нужно знать.

SWOT-анализ

Этот метод позволяет выявить сильные и слабые стороны компании, а также возможности и угрозы, исходящие от конкурентов. Он помогает понять, в чем компания превосходит соперников и где у нее есть недостатки. По сути, это общий взгляд на положение компании на рынке.

PEST-анализ

Оценивает влияние политических, экономических, социальных и технологических факторов на бизнес. Это помогает определить внешние условия, которые могут повлиять на конкурентоспособность.

Анализ событий (Event Analysis)

Этот метод выделяет ключевые события во внешней среде компании и показывает тенденции, что может служить средством раннего предупреждения о возможных изменениях в конкурентной среде.

Кластерный анализ

Используется для сегментации рынка и выявления групп потребителей с похожими характеристиками или поведением, что помогает в целевом маркетинге.

Бенчмаркинг

Сравнение показателей компании с лучшими практиками в отрасли для выявления областей для улучшения.

Анализ больших данных

Применение технологий машинного обучения и искусственного интеллекта для обработки больших объемов данных из различных источников с целью выявления скрытых закономерностей и прогнозирования поведения конкурентов.

Метод альтернативных исходов

Позволяет рассмотреть несколько сценариев развития событий на основе имеющихся данных, что может быть полезно при принятии решений в условиях неопределенности.

РЕСУРСЫ

Список литературы

- Dale Meredith – «The OSINT Handbook. A practical guide to gathering and analyzing online information»
- Loch K. Johnson "Intelligence and National Security" 2008
- Michael Bazzell - "Open Source Intelligence Techniques"
- Michael Bazzell - "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence"
- Michael Bazzell - "OSINT Techniques: Resources for Uncovering Online Information" 2023 г.
- Nihad A. Hassan, Rami Hijazi - "Open Source Intelligence Methods and Tools", 2018
- Rob Botwright "OSINT Commando: Penetrating Networks With Spokeo, Spiderfoot, Seon, And Lampyre" 2024
- Varin Khera, Anand R. Prasad, Suksit Kwanoran "Open Source Intelligence (OSINT) – A Practical Introduction" 2024
- Абсхаген К.Х. – Канарис – за линией фронта – Центролиграф 2006
- Алексеенко В.Н., Сокольский Б.Е. Система защиты коммерческих объектов - Москва 1992
- Антонов А.В. Системный анализ – Высшая школа 2004
- Бабец О.А. Опыт военной разведки на службе в коммерческой фирме – Харвест 2003
- Балабанов И.Т. Риск-менеджмент - «Финансы и статистика» 1996
- Барбара Минто Золотые правила Гарварда и mckinsey. Правила магической пирамиды для делового письма - Росмэн-Пресс 2004
- Баунов Александр Германович – «Wikileaks: дипломатия с черного хода»
- Баяндин Н.И. Технологии безопасности бизнеса – Юрист 2002
- Байгушев А. Партийная разведка – Алгоритм 2007
- Белановский С. А. Глубокое интервью. - Никколо-Медиа 2001
- Белановский С. А. Методика и техника фокусированного интервью – Наука 1993
- Болтунов Михаил Ефимович - "Разведка «под крышей». Из истории спецслужбы"
- Вакуленко Р.Я. Защита бизнеса и стратегия предприятия – Юркнига 2005
- Весенин В.Р. Практический менеджмент персонала. – М. Юрист 1998
- Волкова В.Н. Козлов В.Н. Системный анализ и принятие решений – Высшая школа 2004
- Воронов Ю.П. Конкурентная разведка Учебное пособие - Москва 2007
- Гаврюшин Е.И. Линдер И.Б. Хрестоматия. Практическая аналитика в службах безопасности – ИСТТА 2006
- Гарифуллин Р.Р. Психология блефа, манипуляций, иллюзий – АСТ 2007
- Глазунов О. Китайская разведка – Алгоритм 2008
- Гохан П.А. Слияния, поглощения и реструктуризация компаний -Альпина-бизнес-букс 2004
- Годин В.В. Модульная программа для менеджеров – инфрам 2000
- Гончаренко Л.П. Куценко Е.С. Управление безопасностью – Кнорус 2005
- Гордукалова Г.Ф. Анализ информации: методы, технологии, организация – Профессия 2009
- Даллес А. Искусство разведки - Международные отношения 1992
- Деревицкий А. Коммерческая разведка – Питер 2006
- Джошуа Пиколет "Operator Handbook: Red Team + OSINT + Blue Team Reference" 2020 г.

- Диев С.А. Шаваев А.Г. Банковский Организация и современные методы защиты информации - Деловой Центр 1998
- Доблаев Л. П. Логико-психологический анализ текста - Саратов 1971
- Добротворский И.Л. Искусство войны в бизнесе: стратегия и тактика – Дело и сервис 2003
- Доронин А.И. Бизнес-разведка – Ось-89 2003
- Доронин А.И. Основы экономической разведки и контрразведки - Тула 2000
- Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия – Тула 2000
- Дридзе Т.М. Текстовая деятельность в структуре социальной коммуникации - Наука 1984
- Дрогобыцкий И.Н. Системный анализ в экономике – Финансы и статистика 2007
- Духихин В.В. Конкурентная разведка в Интернет – советы аналитика – ДМК 2002
- Духов В.Е. Экономическая разведка и безопасность бизнеса - НВФ Студцентр 1997
- Зайцов А.А. Служба генерального штаба – Куликово поле 2003
- Звонарев К.К. Агентурная разведка - БДЦ-пресс 2003
- Зданович А.А. Отечественная контрразведка 1914-1920 - Крафт+ 2004
- Землянов В.М. Своя контрразведка - Харвест 2002
- Землянов В.М. Агентура в разведке и контрразведке – Харвест 2007
- Землянов В.М. Основы сыскного ремесла – Харвест 2004
- Ивахин А.Е., Прыгунов П.Я. Оперативная деятельность и вопросы конспирации в работе спецслужб – Киев КНТ 2008
- Ионцев М.Г. Корпоративные захваты. Слияния, поглощения, гринмейл. – Ось-89 2008
- Канн Д. «Война кодов и шрифтов» – Рипол 2004
- Кара-Мурза С.Г. «Манипуляция сознанием» - Алгоритм 2005
- Касперски Крис «Секретное оружие социальной инженерии» – 2008
- Каценеленбаум Б. «Демагогия: опыт классификации»
- Кибанов А.Я. «Управление персоналом» – Экзамен 2001
- Кириллов В.И., Старченко А.А. «Логика» - Юрист 1996
- Ковалев Е. М., Штейнберг И. Е. «Качественные методы в полевых социологических исследованиях» – Логос 1999
- Косоруков О.А. «Методы количественного анализа в бизнесе» – Инфра-М 2005
- Козлов С.Б. Иванов Е.В. «Предпринимательство и безопасность» - Универсум 1991
- Колпаков А.И. «Все о внешней разведке» – Олимп 2002
- Корж П.А. «Негосударственная безопасность» – Феникс 2002
- Коуз Р. «Природа фирмы» – Дело 2002
- Кузин А. Нежданов И. Ющук Е. «Дезинформация и активные мероприятия в бизнесе»
- Куцеля Давид - "OSINT - искусство получения информации"
- Лабоцкий В.В. «Управление знаниями» – Современная школа 2006
- Ландэ Д.В. «Поиск знаний в Интернет» – Диалектика 2005
- Латышова Л.С. Пантелеева Е.К. «Маркетинговый анализ» – Экономист 2007
- Лемке Г.Э. «Нелинейный стратегический менеджмент или искусство конкуренции» – Дело и сервис 2006
- Лемке Г.Э. «Конкурентная война. Нелинейные методы и стратегии» – Ось 89 2007
- Лемке Г.Э. «Секреты коммерческой разведки» – Ось 89 2008
- Мак Мак В.П. «Служба безопасности предприятия» – Мир безопасности 1999
- Матанцев А.Н. «Стратегия, тактика и практика маркетинга» – Юрист 2002
- Матвейчев О. «Уши машут хвостом»
- Мелтон Х.К. «Офисный шпионаж» – Феникс 2005
- Мироничев С. «Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ним» - «Дружок» 1995
- Минто Барбара «Золотые правила Гарварда и mckinsey. Правила магической пирамиды для делового письма» - Росмэн-Пресс 2004
- Митник Кевин «Искусство вторжения»

- Митник Кевин «Искусство обмана» Компания - айти 2004
Мелисс Клеммонс Румизен «Управление знаниями» – АСТ 2004
Мескон М., Альберт М., Хедоури Ф. «Основы менеджмента» - М. Дело 1992
Моргунов Е.Б. Модели и методы управления персоналом - Интел-Синтез 2001
Мухин А.А. Информационная война в России – Москва 2000
Наумов В.В. Лингвистическая идентификация личности – комкнига 2006
Нежданов И.Ю. «Аналитическая разведка»
Нежданов И.Ю. «Технологии разведки для бизнеса»
Одинцов А.А. Экономическая и информационная безопасность – Экзамен 2005
Орлов А. Покупка и продажа бизнеса. Российская практика – Вершина 2006
Остапенко П.В. Тайная война в древнем мире –Харвест2004
Парад Б. Коммерческий шпионаж – Проспект 2005
Петраков А.В. Лагутин В.С. Утечка и защита информации в телефонных линиях – Энергоатом 1998
Петров М.Н. Механизмы государственных переворотов – Харвест 2005
Прескотт Д.Е., Миллер С.Х. Конкурентная разведка уроки из окопов - Альпина-паблишер 2003
Пол Уоттерс, Роберт Лейтон "Automating Open Source Intelligence: Algorithms for OSINT" 2015 г.
Поповская Л.В. Лингвистический анализ художественного текста в вузе – Феникс 2006
Портер Майкл Конкуренция – Вильямс 2006
Почепцов Г.Г. Теория коммуникаций – Релф-бук 2001
Почепцов Г.Г. Стратегический анализ – Дзвин 2004
Почепцов Г.Г. Революция.com – Основы протестной инженерии – Европа 2005
Райс Э. Траут Д. Маркетинговые войны – Питер 2000
Ричардс Дж. Хойер мл. - "Психология разведывательного анализа"
Роберт Б. Чалдини - "Психология влияния. Убеждай, воздействуй, защищайся"
Ромачев Нежданов Конкурентная разведка – Ось-89 2007
Ронин Р. Своя разведка - Харвест 1999
Ронин Р. Это тонкое дело – разведка - Гинлайт 2008
Рубин Ю.Б. Теория и практика предпринимательской конкуренции – Маркет ДС 2007
Рушайло В.Б. Основы оперативно-розыскной деятельности – Лань 2000
Рыбаков Антон и Вадим Челпанов - "Анализ личности через профиль соцсетей. Интернет-разведка"
Садердинов А.А. Информационная безопасность предприятия – Дашков и К 2004
Сойма В.М. Советская контрразведка в годы Великой Отечественной войны - Крафт 2005
Соклакова Н.А. Криминалистическое исследование материалов документов – Питер 2005
Сотников А.В. Антикиллер – как предупредить заказное убийство – Харвест 2006
Стрикленд А.Д. и Томпсон А.А. Стратегический менеджмент – Юнити 1999
Судоплатов А.П. Безопасность предпринимательской деятельности – Олма пресс 2001
Таганов Д.Н. Информация как основной фактор формирования конкурентной стратегии – Менеджмент в России и за рубежом 2005 №1
Тарас А.С. Своя контрразведка – Харвест 2002
Тарас А.С. Спутник разведчика и партизана – Харвест 2005
Тарас А.С. Методы и приемы психологической войны – Харвест 2006
Тарас А.С. Секреты психологической войны – Харвест 1999
Тарас А.С. Подготовка разведчика – Харвест 2000
Тарас А.С. Телохранитель – Харвест 2000
Тарас А.С. Управление войсками – Харвест 2006
Тарасов В.К Искусство управленческой борьбы – Хорошая книга 2003
Токарев Б.Е. Методы сбора и использования маркетинговой информации – Юрист 2001

- Федько Н.Г. Поведение потребителей – Феникс 2001
- Федотова Л.Н. Контент-аналитические исследования средств массовой информации и пропаганды - Изд-во Моск. Ун-та 1988
- Фляйшер К. Бенсуссан Б. Стратегический и конкурентный анализ – Бином 2005
- Халяпин Д.Б. Основы защиты информации – Москва 1994
- Харский К.В. Благонадежность и лояльность персонала – Питер 2003
- Хенриетта Уилсон, Оламайд Сэмюэл, Дэниел Плеш "Open Source Investigations In The Age Of Google" 2024 г.
- Хохлов Н.В. Управление риском - Юнити 2001
- Хлобустов О. Госбезопасность от Александра 1 до Путина Яуза 2005
- Шалак В.И. Современный контент-анализ – Омега 2004
- Шиян А.А. Руководство по социальным технологиям – Украина 2001
- Шкатулла В.И. Настольная книга менеджера по кадрам – Норма 2000
- Чатфилд Том - "Критическое мышление: Анализируй, сомневайся, формируй свое мнение"
- Чичельник Н.А. Проверка предприятия органами надзора – Феникс 2003
- Черчилль К.А. Маркетинговые исследования – Питер 2003
- Чуфаровский Ю.В. Психология оперативно-розыскной деятельности
- Эванс Ф.Ч. Оценка компании при слияниях и поглощениях – Альпина 2004
- Ющук Е.Л. Конкурентная разведка – маркетинг рисков и возможностей – Вершина 2006
- Ющук Е.Л. Интернет-разведка руководство к действию – Вершина 2007
- Ющук Е.Л. Блог. Создать и раскрутить – Вершина 2007
- Ющук Е.Л. и Кузин А.В. Противодействие черному PR в Интернете – Вершина 2008
- Ядов В. А. Стратегия социологического исследования - Москва 2000
- Яковец Е.Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел – Издательский дом Шумиловой 2005
- Ярославский В. Военные методы в бизнесе. Тактика – Крылов 2003
- Ярочкин В.И. Бузанова Я.В. Системы защиты предпринимательства Мир 2005
- Ярочкин В.И. Бузанова Я.В. Корпоративная разведка – Ось89 2005
- Ярочкин В.И. Безопасность банковских систем – Ось-89 2004
- Яскевич В.И. Секьюрити – организационные основы безопасности фирмы – Ось-89 2005
- Методическое пособие по курсу "Конкурентная разведка" Консалтингового центра "Лекс" - "Деловая и конкурентная разведка" 2001 год

OSINT- каталоги, подборки инструментов

Здесь предложены некоторые подборки источников, литературы и документов в формате каталога закладок или в виде автономных сайтов с перечнем полезностей.

AML Toolbox (каталог полезных он-лайн сервисов) <https://start.me/p/rxeRqr/aml-toolbox>

AsINT_Collection (каталог полезных он-лайн сервисов)
https://start.me/p/b5Aow7/asint_collection

Aware Online OSINT Tools (каталог полезных он-лайн сервисов) <https://www.aware-online.com/en/osint-tools>

BooleanStrings Tools <https://booleanstrings.com/tools>

Bruno Mortier GEOINT (каталог полезных он-лайн сервисов)
<https://start.me/p/W1kDAj/geoint>

Bruno Mortier IMINT (каталог полезных он-лайн сервисов) <https://start.me/p/ZMXLlA/imint-vi>

Bruno Mortier INT.INFRA (каталог полезных он-лайн сервисов)
<https://start.me/p/V0PXgr/int-infra>

Bruno Mortier Keywords (каталог полезных он-лайн сервисов)
<https://start.me/p/VvGz56/keywords>

Bruno Mortier Monitoring (каталог полезных он-лайн сервисов)
<https://start.me/p/3xMXnP/monitoring>

Bruno Mortier OSINT (каталог полезных он-лайн сервисов) <https://start.me/p/ZME8nR/osint>

Bruno Mortier OSTER (каталог полезных он-лайн сервисов) <https://start.me/p/7kmvEK/oster>

Bruno Mortier Security (каталог полезных он-лайн сервисов)
<https://start.me/p/Zz4gyM/security>

Bruno Mortier SOCMINT (каталог полезных он-лайн сервисов)
<https://start.me/p/Wp1kpe/socmint>

Bruno Mortier Sources (каталог полезных он-лайн сервисов)
<https://start.me/p/3g0aKK/sources>

Bruno Mortier Toolkit (каталог полезных он-лайн сервисов)
<https://start.me/p/W1AXYo/toolkit>

CNTY USA <https://start.me/p/kxMBv9/cnty-usa>

Hun-OSINT <https://start.me/p/kxGLzd/hun-osint>

IntelligenceX (каталог сервисов и поисковиков) <https://intelx.io/tools>

IntelTechniques OSINT Packet 2019 <https://inteltechniques.com/tools/index.html>

Julia Bayer Verification Toolset <https://start.me/p/ZGAzN7/verification-toolset>

Jungla OSINT <https://start.me/p/7k48PK/jungla-osint-por-ra1000>

Lorand Bodo <https://start.me/u/1kmODD/lorand-bodo>

Marc Kranat OSINT <https://300m.com/osint>

MIDASearch <https://midasearch.org>

OSINT Essentials <https://www.osintessentials.com>

OSINT for Finding People by cybersecstu
https://docs.google.com/spreadsheets/d/1JxBbMt4JvGr--G0Pk13jP9VDTBunR2uD3_faZXDvhxc/edit#gid=603724104

OSINT Framework <http://osintframework.com>

OSINT Geek Tools <https://osintgeek.de/tools>

OSINT Link <http://osint.link>

OSINT Links <https://start.me/p/q6naJo/osint-links>

OSINT Tools by Lorand Bodo <https://start.me/p/7kxyy2/osint-tools-curated-bylorand-bodo>

OSINT Toolset <https://start.me/p/MEw7be/1-osint-toolset>

OSTER <https://start.me/p/7kmvEK/oster>

RBA Business Information Resources <http://www.rba.co.uk/sources>

Research Clinic <http://www.researchclinic.net>

Reuser OSINT Discovery Toolkit <http://rr.reuser.biz>

Search Social Media <https://start.me/p/RMKeQv/search-social-media>

Social Media <https://start.me/p/4K0DXg/social-media>

Social Media Intelligence Dashboard <https://start.me/p/m6MbeM/social-mediainelligence-dashboard>

Sprp77's OSINT Resources <https://drive.google.com/drive/folders/1CBcemFdorkAqJ-Stsh67OVHgH4FQF05>

Startme Open Source Investigative Tools by Malachy Browne <https://start.me/p/gyvaAJ/open-source-investigativetools>

Start page <https://start.me/p/rx6Qj8/start-page>

TDiDDY OSINT <https://start.me/p/b56xX8/osint>

Technisette <https://start.me/u/Z9Oamm/technisette>

Telegram: HowToFind Bot https://t.me/HowToFind_bot

Threat Intelligence <https://start.me/p/rxRbpo/ti>

UK OSINT <https://www.uk-osint.net>

The Ultimate OSINT Collection <https://start.me/p/DPYPMz/the-ultimate-osintcollection>

Verification Toolkit <https://start.me/p/ZGAzN7/verification-toolset>

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	2
OSINT, как много в этом слове.....	2
Что такое анализ.....	4
ОРГАНИЗАЦИЯ РАБОТ.....	6
Общение с руководителем (заказчиком информации).....	6
Как помочь заказчику точно сформулировать задачу.....	6
Понятность и точность в формулировании задачи.....	7
Обсудите выполнимость поставленной задачи.....	7
Поставьте реальные сроки.....	7
Перспектива или тенденция.....	7
Поддержка обратной связи.....	8
Постановка задачи.....	9
Беседа с заказчиком.....	11
Формулировка задачи.....	12
Планирование.....	13
Определение информационных потребностей.....	13
Что вы уже знаете об объекте интереса?.....	13
Что можете узнать прямо сейчас?.....	14
Определение приоритетов.....	14
Составление плана.....	15
Дезинформация.....	18
Что такое деза и откуда она берется.....	18
Как дезинформируют.....	19
Выявление дезинформации.....	24
Как создать эффективную систему OSINT.....	27
Понять потребности компании в информации.....	27
Подобрать источники.....	28
Как выбрать нужные источники в инете.....	28
Что сделать в первую очередь.....	29
СБОР ИНФОРМАЦИИ.....	31
Ошибки.....	31
Организация сбора информации.....	32
Источники информации.....	32
Сбор информации из баз данных.....	37
Работа с людьми.....	38
Побуждение человека делиться с вами полезной информацией.....	39
Проверка кандидата на роль источника.....	40
Организация первого контакта и его углубление.....	41
Связь с человеком, обладающим нужной вам информацией.....	43
Особенности вывода из операции.....	44
Поиск данных в интернете поисковыми сервисами.....	44
Поисковики.....	44

Правила формирования запроса поисковику.....	50
Сбор удаленных или измененных данных в интернете.....	53
Сбор данных в интернете с помощью ИИ.....	54
Как создать качественный промпт	55
Основные рекомендации для создания промптов.....	58
Примеры	58
Методика сбора информации о человеке.....	67
Что ищем	67
Как ищем.....	74
Методика сбора информации об организации	92
Что ищем	92
Как ищем.....	93
Методика поиска объекта	115
Что ищем	115
Как ищем.....	117
Методика выявления угроз со стороны соседнего государства	123
Что ищем	123
Сбор информации с помощью сервисов ИИ	125
Инструменты для сбора информации	128
Поиск данных.....	128
Поиск в социальных сетях.....	129
Геоданные.....	129
Почтовые ящики	131
Номера телефонов.....	132
Изображения и сбор информации по фотографиям.....	134
Организация хранения информации	135
Файловая система	136
Сторонние сервисы	137
Своя БД.....	138
Готовые решения для хранения.....	139
Формирование отчета	139
АНАЛИЗ ИНФОРМАЦИИ.....	142
С чего начать	142
Аналитическая объективность.....	142
Новостная система.....	143
Предварительная обработка информации	144
Точная фиксация сообщения (в т.ч. и система архивирования)	145
Фиксация атрибутов сообщения	145
Выделение утверждений	146
Оценка информации	149
Критерии оценки информации (важность, точность, значимость)	149
Установление источника, получателя, их пространственных и временных координат.....	151
Установление фактографической составляющей текста, его тематики.	152
Оценка сведений (вне контекста).....	156
Анализ текстовой информации.....	156
Простые методы анализа.....	156
Творческие методы	164

Комплексный инструмент анализа	167
А еще... ..	172
РЕСУРСЫ	174
Список литературы.....	174
OSINT- каталоги, подборки, закладки инструментов.....	177
ОГЛАВЛЕНИЕ	180