ГЛАВА 1

СПРЯТАНО У ВСЕХ НА ВИДУ: РАСКРЫВАЕМ ВОЗМОЖНОСТИ OSINT

Добро пожаловать в безумную и захватывающую **разведку по открытым источникам (OSINT)**! Мы начинаем главу, где вы раскроете для себя возможности OSINT, познакомитесь с практическими приемами сбора данных и узнаете, почему извлечение информации из открытых источников так ценится в современном цифровом мире. Благодаря изложенным материалам вы научитесь без труда ориентироваться в этой сфере.

В этой главе мы рассмотрим следующие темы:

- Введение в OSINT
- Пассивная и активная разведка
- Почему OSINT так важна в цифровую эпоху
- OSINT Framework
- Начало работы с OSINT и некоторые рекомендации

Я, словно Бэтмен, на всем протяжении главы буду сопровождать вас и приходить на выручку в трудный момент. Вы разберете наглядные примеры и советы профессионалов, узнаете, как не потеряться в общедоступной информации, извлекать данные и применять OSINT для достижения целей. В результате вы получите целый арсенал навыков, которые помогут превзойти конкурентов, усилить информационную защиту и уверенно ориентироваться в бескрайнем цифровом мире.

Готовы отправиться в увлекательное путешествие по OSINT? Скоро вы узнаете, насколько огромен потенциал разведки по открытым источникам!

Введение в OSINT

Разведка по открытым источникам, или, как ее часто называют, **OSINT** (Open Source Intelligence), — процесс сбора, оценки и интерпретации информации, находящейся в открытом доступе, который помогает найти ответы на конкретные вопросы, поставленные перед исследователем.

Поговорим об информации и разведке

На первый взгляд, информация (information) и данные, полученные в результате разведки (intelligence), кажутся одним и тем же, но на деле отличаются так же сильно, как сырые ингредиенты от готового обеда.

1. **Информация: отправная точка.**
   Сначала нужно понять, что такое информация. Это необработанный материал, исходное сырье. Она окружает нас повсюду, принимая множество форм: мы читаем твиты, просматриваем новостные статьи и листаем публикации, переполняющие ленту в социальных сетях. Информации много, она разнообразна, а ее качество варьируется от высочайшего до совершенно непригодного. В мире OSINT все начинается именно с нее.

2. **Данные разведки: готовое блюдо.**
   Если информация — сырые ингредиенты, то данные разведки — полноценный, с любовью приготовленный обед. Чтобы его получить, необходимо собрать информацию, проанализировать ее, понять с учетом контекста и преобразовать в нечто полезное и имеющее смысл. Цель анализа — интерпретировать данные, выявить закономерности, установить связи и, что самое важное, сформулировать выводы, применимые на практике.

3. **Преобразование.**
   Превращение информации в данные разведки и есть OSINT. Это процесс, требующий высокого мастерства. Начав со сбора информации в открытых источниках, мы переходим к решающему этапу: проверяем ее подобно тому, как повар проверяет свежесть ингредиентов.

4. **Анализ.**
   После проверки информацию необходимо проанализировать. Именно здесь происходит настоящее волшебство. Мы выявляем в ней закономерности и аномалии, пытаясь добраться до сути. Сначала разделяем информацию на отдельные факты, а потом вновь объединяем их, чтобы

сформировать целостную картину, — как если бы мы смешивали ингредиенты для создания идеального блюда.

5. **Интерпретация.**
   Наконец наступает этап интерпретации. Мы делаем выводы, оцениваем влияние данных разведки и, опираясь на них, принимаем решение и разрабатываем эффективную стратегию.

Пассивная и активная разведка

Давайте разберемся, в чем разница между пассивной и активной разведкой. Это два подхода к получению данных, но, несмотря на похожие цели, они могут иметь разные последствия для организации.

При пассивной разведке вы, словно призрак, наблюдаете за миром, не взаимодействуя с ним напрямую: перебираете общедоступную информацию, но не комментируете публикации, не пишете личных сообщений, не добавляетесь в друзья и не подписываетесь на других пользователей. Вы, как подводная лодка, залегаете на дно и пеленгуете все вокруг.

В свою очередь, активная разведка подразумевает прямое взаимодействие с целью расследования: дружбу в социальных сетях, комментарии или даже общение в чате. Вы будто агент под прикрытием — и некоторые компании воспринимают активный OSINT именно так. Так что прежде чем бросаться в бой, обязательно заручитесь согласием руководителя.

Если выбор падет на активную разведку, вам придется смешаться с толпой, проявив максимум смекалки. *«Как же это сделать, Дейл?»* Сначала заведите учетные записи на разных платформах. Так вы будете похожи на рядового пользователя.

А дальше начинаются нюансы. В каждой организации может быть собственный регламент насчет того, какие способы разведки считать пассивными, а какие активными. Например, если вы вступите в закрытую группу Facebook, то для одних компаний останетесь сторонним наблюдателем, а другие могут расценить это как явное взаимодействие. Поэтому крайне важно знать, по каким правилам играет именно ваша организация.

Некоторые вообще уверяют, что участие в группе относится к пассивной разведке, пока вы лишь наблюдаете за происходящим и не общаетесь с людьми.

И как здесь не запутаться?

Почему OSINT так важна в цифровую эпоху

Сегодня OSINT используют органы власти, компании, некоммерческие организации и другие структуры. Разведка открывает немыслимые возможности: благодаря ей выявляются угрозы безопасности, проводятся маркетинговые исследования, анализируется деятельность конкурентов и не только.

Вот неполный список того, где пригодится OSINT:

- **Научные исследования.** OSINT помогает собирать данные на различные темы, например изучать общественное мнение, социальные тенденции и экономические показатели.
- **Бизнес и маркетинговые исследования.** Хотите выяснить, чем занимаются конкуренты, определить направление развития отрасли или узнать больше о поведении потребителей? Благодаря OSINT вы найдете информацию, которая подкрепит ваши решения и стратегии.
- **Безопасность и разведка.** С OSINT у вас на службе будет свой личный Шерлок Холмс, способный обнаружить террористическую деятельность или кибератаки. Кроме того, средства разведки пригодятся для слежки за иностранным правительством, различными организациями и преступными группировками.
- **Журналистские расследования.** Прибегая к стратегиям OSINT, журналисты могут распутывать скандалы, связанные с политикой, бизнесом, криминалом и не только.
- **Судебные разбирательства.** OSINT может значительно повлиять на судебный процесс, начиная со сбора доказательств и заканчивая поиском потенциальных свидетелей или обвиняемых.

В чем фишка OSINT?

Основное внимание в OSINT уделяется сбору открытой, официально доступной информации. Вам не придется тратить время и деньги на работу с засекреченными источниками или обход ограничений.

Вместо этого OSINT предлагает на выбор социальные сети, новостные статьи, отчеты правительств, научные работы и многое другое. Этого хватит, чтобы составить полную картину происходящего в различных сферах.

Еще одно достоинство — актуальность информации. Благодаря разведке в режиме реального времени вы будете в курсе последних событий и тенденций.

Кроме того, поиск данных по открытым источникам экономически эффективен. В отличие от агентурной и радиоэлектронной разведки, OSINT не требует дорогостоящего оборудования и специально обученных сотрудников, что существенно повышает его доступность.

Наконец, любую информацию, полученную средствами OSINT, легко перепроверить и подтвердить. Значит, полученные сведения будут достаточно достоверными и на них можно будет положиться.

Как же работает OSINT?

Если вам интересно, как вести разведку по открытым источникам, мы приоткроем для вас завесу тайны.

1. **Поиск.** Соберите информацию из различных источников, включая социальные сети, новостные статьи, отчеты правительств и коммерческие базы данных. Это можно делать вручную или с помощью автоматизированных инструментов.
2. **Обработка.** Отсейте неточные, неактуальные или дублирующиеся данные. Необходимо фильтровать и классифицировать находки с учетом их важности и актуальности.
3. **Анализ.** Изучите обработанную информацию, чтобы выявить закономерности и взаимосвязи. Вам помогут инструменты для визуализации и интеллектуального анализа данных, а также обработки естественного языка.
4. **Распространение.** На последнем этапе поделитесь выводами с теми, кто принимает решения. В зависимости от потребностей организации формат данных разведки может быть разным, например полные отчеты, сжатые обзоры или краткие уведомления.

Весь фокус OSINT — в непрерывности цикла: вы постоянно собираете информацию, совершенствуете ее обработку и анализ, учитывая новые данные и обратную связь. Разумеется, инструмент не идеален, он имеет те же ограничения, что и другие методы исследований. Поэтому необходимо привлекать опытных аналитиков, способных грамотно интерпретировать извлеченные данные.

Под покровом OSINT скрывается масса методов сбора и анализа данных. Вкратце опишем некоторые из них.

- **Социальные сети.** Twitter, Facebook, LinkedIn и другие похожие платформы — не просто площадки для онлайн-тусовок. Благодаря им можно

отслеживать тенденции, оценивать настроение общественности, а иногда выявлять потенциальные угрозы.

- **Веб-скрейпинг.** Это автоматический сбор информации, похожий на работу золотоискателя в цифровом пространстве. В ход идут специализированные программы, позволяющие быстро и систематически извлекать из сайтов тонны данных.
- **Поисковые системы.** В старых добрых поисковых системах вроде Google есть расширенный поиск, который помогает получать более точные результаты. Иногда такой процесс называют Google Dorking[1].
- **Юридические документы.** Сундук, битком набитый ценной информацией. Судебные материалы, свидетельства о собственности и документы компаний могут многое рассказать как об организациях, так и об обычных людях.
- **Новости.** Традиционные СМИ, например газеты, журналы и новостные сайты, — настоящая сокровищница. Они помогают держать руку на пульсе и быть в курсе текущих событий, новых тенденций и потенциальных проблем.
- **Инструменты анализа данных.** Excel, Tableau и R незаменимы при работе с огромными массивами данных. Эти и другие инструменты помогают отсеять лишнюю информацию и выявить закономерности и взаимосвязи.

Помните, что OSINT не стоит на месте. Чтобы эффективно собирать и анализировать данные, необходимо следить за появлением новых технологий и источников данных, а также осваивать новейшие методы и инструменты разведки.

OSINT Framework

Фреймворк разведки по открытым источникам, известный как OSINT Framework (https://osintframework.com/), — потрясающая платформа для тех, кто осваивает сбор информации. Это обновляемый онлайн-каталог ресурсов для OSINT в форме, удобной для восприятия и навигации.

Фреймворк разработал Джастин Нордин (Justin Nordine), уважаемый человек в сфере кибербезопасности. Он хотел систематизировать и рассказать

[1] Google Dorking — использование расширенных поисковых операторов Google для поиска специфической информации, часто такой, которая не предназначена для публичного доступа. — *Примеч. пер.*

всем об имеющемся изобилии инструментов для разведки по открытым источникам. OSINT Framework постоянно обновляется благодаря совместным усилиям специалистов по кибербезопасности и широко используется ими по всему миру.

Открыв сайт OSINT Framework, вы увидите интерактивную диаграмму связей. Она начинается с общих категорий, перейдя по которым вы попадете к спискам конкретных ресурсов и инструментов. Благодаря такой структуре можно без труда найти, например, социальные сети, специализированные поисковые системы, утекшие базы данных, правительственные ресурсы — все что угодно.

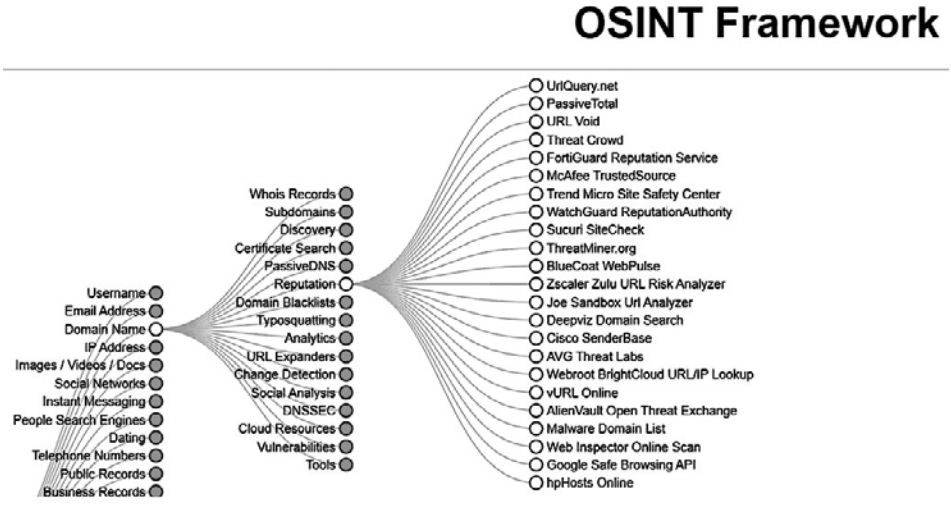

Рис. 1.1. OSINT Framework (https://osintframework.com/)

Для специалистов в сфере безопасности OSINT Framework просто незаменим. Он предлагает множество инструментов для сбора информации, с которых удобно начать расследование или оценку степени защищенности компании. Распределение по категориям помогает быстро находить подходящие ресурсы и тем самым экономит ценное время на ранних этапах разведки.

Стоит отметить, что сам фреймворк не является инструментом. Он, скорее, напоминает карту сокровищ, которая показывает путь к другим полезным ресурсам OSINT. С каждым из них важно обращаться ответственно: помните, что необходимо уважать конфиденциальность других людей и действовать в рамках закона.

OSINT Framework привлекателен из-за своей простоты и широкого охвата ресурсов. Его регулярно обновляют, благодаря чему он остается ценным сайтом для специалистов в области безопасности и всех, кто интересуется разведкой по открытым источникам. OSINT Framework стал ярким примером того, как важно сотрудничать и обмениваться информацией.

Разведка на примере реальных ситуаций

Как насчет фишингового электронного письма? Выявление его отправителя могло бы выглядеть так:

1. **Первичный анализ.** Получатель фишингового письма заметил что-то подозрительное и сообщил об этом в службу безопасности.
2. **Анализ метаданных электронного письма.** Специалисты по безопасности проанализировали заголовок письма и извлекли такие метаданные, как IP-адрес отправителя, метку времени и маршрутную информацию.
3. **Поиск IP-адреса.** Информацию об IP-адресе сопоставили с данными из общедоступных источников OSINT, включая реестры доменных имен, базу данных WHOIS и сервисы репутации IP.
4. **Анализ цифрового следа.** Специалисты изучили социальные сети, онлайн-форумы и сайты, чтобы выявить любое присутствие в Сети, связанное с этим адресом IP или электронной почты.
5. **Анализ собранной информации.** Информацию, полученную из открытых источников, объединили и проанализировали, чтобы найти взаимосвязи и закономерности.
6. **Установление источника и отчетность.** На основе собранных доказательств специалисты определили вероятный источник фишингового письма. Они подготовили подробный отчет, содержащий всю необходимую информацию и рекомендации по устранению угрозы.

А как с помощью OSINT отследить утечку данных?

1. **Обнаружение проблемы.** Организация обнаруживает утечку данных с помощью систем внутренней безопасности или благодаря чьему-то сообщению.
2. **Сбор индикаторов компрометации.** Из взломанной системы или внешних источников собираются фрагменты похищенных данных, псевдонимы хакеров и другие индикаторы.

- **Фрагменты похищенных данных.** Злоумышленники нередко публикуют часть утекших данных, чтобы продемонстрировать доступ к информации и убедить людей в своих возможностях. OSINT помогает найти такие фрагменты на различных платформах, например общедоступных сайтах, форумах или даркнет-рынках, где данные могут продаваться или распространяться. Используя средства разведки по открытым источникам, специалисты по кибербезопасности выявляют и анализируют фрагменты похищенных данных, чтобы определить масштабы и характер взлома.
- **Псевдонимы хакеров.** Киберпреступники часто создают специальный онлайн-образ или действуют под псевдонимами. Информацию о них можно найти с помощью разведки по открытым источникам, включая социальные сети, форумы и чаты. Во время поиска и анализа специалисты по кибербезопасности могут выявить связи, закономерности или историю действий, связанные с псевдонимами. Это, в свою очередь, поможет установить личности злоумышленников или предполагаемые мотивы взлома.
- **Анализ взломанных систем.** OSINT также помогает собрать индикаторы компрометации из самой взломанной системы. Изучая журналы событий, сетевой трафик и другие цифровые артефакты, специалисты могут обнаружить следы злоумышленников, например IP-адреса, инфраструктуру **управления и контроля (C2**[1]**)** и сигнатуры вредоносного ПО, которые дают ценные сведения о взломе. Средства OSINT позволяют сопоставить найденные индикаторы с информацией из общедоступных источников и тем самым узнать больше о преступниках и их методике.

3. **Просмотр даркнета.** С помощью инструментов OSINT просматриваются форумы, маркетплейсы и чаты даркнета в поисках любых упоминаний похищенных данных или связанных с ними действий.
4. **Просмотр социальных сетей.** В общедоступных социальных сетях идет поиск обсуждений, публикаций или комментариев, которые могут дать представление об утечке или злоумышленниках.
5. **Анализ похищенных данных.** Если фрагменты похищенных данных общедоступны, с помощью методов OSINT анализируется их содержание, в том числе имена пользователей, электронные адреса и другие данные, способные раскрыть личность злоумышленников и помочь в расследовании.

[1] C2 — C&C, Command and Control. — *Примеч. пер.*

6. **Установление источника и сотрудничество.** Результаты разведки передаются для совместного расследования заинтересованным сторонам: правоохранительным органам, компаниям, специализирующимся на информационной безопасности, или отраслевым организациям.
7. **Правовые меры или устранение последствий.** На основе разведанной информации и найденных доказательств принимаются правовые меры или устраняются последствия взлома. Это позволяет минимизировать ущерб и предотвратить будущие инциденты.

Возможно, теперь вы лучше понимаете, чем OSINT полезен вам и вашей организации.

Начало работы с OSINT и некоторые рекомендации

Разведка по открытым источникам предоставляет ценную информацию и широкие возможности для расследования. Мы собрали несколько полезных советов, идей и ресурсов, которые помогут вам освоить OSINT и заложить прочную основу для исследований.

Полезные советы по сбору информации

Прежде чем начать сбор сведений, определите цель поиска и результаты, которых хотите достичь. Это поможет сфокусироваться на главном и упростит работу. Не бросайтесь в бескрайние дебри информации без структурированной методологии.

Разбейте исследование на логические этапы, чтобы охватить все важные аспекты. При сборе информации обращайтесь к различным источникам: поисковым системам, социальным сетям, юридическим документам, сайтам правительств, специализированным инструментам OSINT и не только. Проверяя данные в нескольких источниках, вы повысите точность результатов и сократите риск получения недостоверных сведений.

Учитесь составлять более эффективные поисковые запросы. Операторы, фильтры и расширенные функции поисковых систем помогут сократить объем данных и получить более релевантные результаты.

Изучайте метаданные изображений, документов и других файлов. Анализируя их, вы можете обнаружить ценную информацию, например местоположение, метки времени, данные об авторе или особенностях устройства.

Еще одна хитрость: научитесь находить цифровые следы. Профили в социальных сетях, онлайн-форумы, публикации в блогах и общедоступные документы могут дать исчерпывающее представление об объекте. Не волнуйтесь, потом я покажу, как это делать.

Подробно фиксируйте свои находки, включая метки времени, URL, скриншоты и заметки. Такая систематизация повысит эффективность анализа и поможет без труда находить сохраненную информацию.

Ресурсы, которые нам пригодятся

Хотите узнать, чем раньше занимался кандидат на вакансию? Или определить, опасен ли сайт? Популярные инструменты OSINT помогут собрать информацию для различных целей. Пополнив ими свой арсенал, вы сможете оптимизировать исследование и обнаружить ценные факты для принятия решения. Помните, что главное преимущество OSINT заключается в его способности превращать разрозненную общедоступную информацию в полезные данные. Предлагаем вам *список Дейла* — 12 лучших инструментов OSINT, с которыми мы будем работать.

- Maltego: https://www.maltego.com/
- SpiderFoot: https://intel471.com/solutions/attack-surface-protection
- Intelligence X: https://intelx.io/
- Shodan: https://www.shodan.io/
- OSINT Framework: https://osintframework.com/
- Metagoofil: https://github.com/opsdisk/metagoofil
- Lampyre: https://lampyre.io/
- Spokeo: https://www.spokeo.com/
- Recon-ng: https://github.com/lanmaster53/recon-ng
- Mitaka: https://github.com/ninoseki/mitaka
- Babel Street: https://www.babelstreet.com/
- Seon: https://seon.io/

Примечание

Я уже рассказывал о ресурсе OSINT Framework (https://osintframework.com/). На нем представлено впечатляющее изобилие сайтов и инструментов для разведки, список которых постоянно обновляется. В этой книге фреймворк OSINT будет упоминаться часто – уж поверьте.