**Слайд 1. Титульный лист**

Добрый день, уважаемые коллеги. Я – Владимир Лазарев и тема моей работы «Исследование методов OSINT для поиска информации о человеке».

**Слайд 2. Что такое OSINT?**

Точного определения OSINT нет, но его можно сформулировать следующим образом. Разведка по открытым источникам (OSINT) - это разведка, проводимая на основе общедоступной информации, которая своевременно собирается, используются и распространяется среди соответствующей аудитории, с целью удовлетворения конкретных потребностей потановщика задачи.

**Слайд 3. С какими источниками работает OSINT?**

OSINT включает в себя все общедоступные источники информации. Эту информацию можно найти онлайн или офлайн:

* Интернет, который включает в себя следующее (и многое другое): форумы, блоги, сайты социальных сетей, сайты обмена видео, такие как YouTube.com, Википедия, записи Whois зарегистрированных доменных имен, метаданные и цифровые файлы, веб-ресурсы Даркнета, данные геолокации, IP-адреса , люди, поисковые системы, и все, что можно найти в Интернете.
* Традиционные средства массовой информации (например, телевидение, радио, газеты, книги, журналы).
* Специализированные журналы, научные публикации, диссертации, материалы конференций, профили компаний, годовые отчеты, новости компаний, профили сотрудников и резюме.
* Фотографии и видео, включая метаданные.
* Геопространственная информация (например, карты и коммерческие изображения).

**Слайд 4. Для чего нужен OSINT?**

Давайте рассмотрим одну ситуацию или сценарий, в котором нам нужно найти информацию, относящуюся к какой-либо теме в Интернете.

Для этого вам нужно сначала выполнить поиск и выполнить анализ, пока вы не получите точные результаты, а это отнимает много времени.

Это основная причина, по которой нам нужны инструменты с открытым исходным кодом, потому что упомянутый выше процесс может быть выполнен за несколько секунд с использованием этих инструментов.

Мы даже можем запустить несколько инструментов для сбора всей информации, относящейся к цели, которую можно сопоставить и использовать позже

Например, используя обыкновенный поисковик (Google, Яндекс), после ввода поиского запроса необходимо вручную проанализировать полученные результаты. В случае работы с OSINT-системами пользователь может задавать определенные дополнительные фильтры – это позволит получить корректную информацию без последующего анализа.

**Слайд 5. Кому интересен OSINT?**

ОСИНТ может быть полезен для разных структур. Мы кратко перечислим их и упомянем, что побуждает каждого искать ресурсы OSINT.

* Правительство: государственные органы, особенно военные ведомства, считаются крупнейшим потребителем источников OSINT.  
  Правительствам нужны источники OSINT для различных целей, таких как национальная безопасность, борьба с терроризмом, кибер-слежка за террористами, понимание взглядов отечественной и зарубежной общественности по различным вопросам, обеспечение политиков необходимой информацией для влияния на их внутреннюю и внешнюю политику и использование иностранных средств массовой информации, таких как телевидение, для получения информации. мгновенные переводы различных событий, происходящих на улице.
* Международные организации: Международные организации, такие как ООН, используют источники OSINT для поддержки миротворческих операций.
* Гуманитарные организации, такие как Международный Красный Крест, используют источники OSINT, чтобы помочь им в их усилиях по оказанию помощи во время кризиса или катастрофы. Они используют данные OSINT для защиты своей цепочки поставок от террористических групп, анализируя сайты социальных сетей и приложения для обмена сообщениями в Интернете, чтобы предсказать будущие террористические действия.
* Правоохранительные органы: полиция использует источники OSINT для защиты граждан от жестокого обращения, сексуального насилия, кражи личных данных и других преступлений. Это можно сделать, отслеживая каналы социальных сетей на наличие интересных ключевых слов и изображений, чтобы помочь предотвратить преступления до их обострения.
* Бизнес-корпорации: информация - это сила, и корпорации используют источники OSINT для исследования новых рынков, мониторинга деятельности конкурентов, планирования маркетинговой деятельности и прогнозирования всего, что может повлиять на их текущую деятельность и будущий рост.

**Слайд 6. Постановка задачи**

Цель: Исследовать текущие методы, приложения и сервисы, которые работают по принципу OSINT. !!Реализовать свою OSINT систему!!

P.S. Задача еще не полностью сформулирована, на текущий момент требуется только провести анализ существующих решений.

**Слайд 7. Анализ существующих решений**

**Maltego** является специализированным разведывательным ПО. Она предназначена для сбора информации с различных баз данных, а также представления в удобном для понимания формате. Также она позволяет выявить основные связи между кусками информации и установить ранее неизвестные отношения между ними.

1. Может нарыть информацию и указать взаимосвязи между
   * людьми(группами людей), их контактами(email, аккаунты на социалках, телефонные номера, адреса)
   * компаниями
   * веб-сайтами
   * Элементами интернет-инфраструктуры(доменные имена, DNS записи, IP адреса, сетевые блоки)
   * документами
   * фразами, надписями
2. Это все линкуется с помощью встроенного ИИ
3. Написана на Java, что есть очень гуд в плане переносимости
4. Удобный GUI, управления визуализацией взаимосвязей
5. Система организована в виде фреймворка, что позволяет полностью адаптировать ее под свои нужды

**theHarvester** — это инструмент для сбора e-mail адресов, имён поддоменов, виртуальных хостов, открытых портов/банеров и имён работников из различных открытых источников (поисковые системы, сервера ключей pgp). Это по-настоящему простой инструмент, но эффективный на ранних этапах тестирования на проникновение или чтобы узнать, какую информацию могут собрать о вашей компании через Интернет.

**Creepy** - это инструмент OSINT для определения местоположения. Собирает информацию, связанную с геолокацией, из онлайн-источников и позволяет отображать ее на карте, фильтровать результаты поиска по точному местоположению и / или дате, экспортировать в формат csv или kml для дальнейшего анализа в Google Maps.