**Методические указания к лабораторной работе № 2**

**"Сбор информации о компании"**

**1. Цель работы**

Ознакомить студентов с методами сбора открытой информации об организациях. Студенты научатся анализировать источники информации, оценивать их надежность и разрабатывать рекомендации по защите персональных данных.

**Важное замечание:** Все действия в рамках лабораторной работы должны проводиться исключительно с использованием открытых источников (OSINT - Open Source Intelligence) и в образовательных целях. Запрещено собирать конфиденциальную информацию, нарушать privacy или использовать данные в реальных атаках. Работа направлена на повышение осведомленности о рисках, а не на их эксплуатацию. Соблюдайте этические нормы и законодательство (например, Закон Республики Казахстан “О персональных данных и их защите» от 21 мая 2013 года N 94-V.)

**2. Теоретическая часть**

**2.1. Основные понятия**

* **OSINT (Open Source Intelligence):** Сбор и анализ информации из общедоступных источников, таких как социальные сети, сайты компаний, поисковые системы, базы данных и т.д.

OSINT (Open Source Intelligence), или разведка по открытым источникам - это процесс сбора, анализа и использования разведывательной информации из общедоступных, легальных источников.

OSINT применяется в самых разных областях, от журналистских расследований и корпоративной безопасности до правоохранительной деятельности и даже преступных целей, позволяя находить и изучать информацию, которую люди сами добровольно публикуют в интернете.

**Ключевые аспекты OSINT:**

*Открытые источники:* Информация собирается из общедоступных ресурсов, таких как социальные сети, новостные сайты, форумы, блоги, открытые базы данных и государственные реестры.

*Процесс:* Включает поиск, сбор, выбор и последующий анализ данных для получения нужной информации.

*Цели:* Может использоваться для решения самых разных задач, например:

* *Кибербезопасность:* Выявление утечек данных, профилирование злоумышленников и анализ угроз.
* *Журналистика:* Расследование громких дел, поиск доказательств и проверка фактов.
* *Безопасность:* Проверка кандидатов, изучение компаний и предотвращение мошенничества.

**Пример из жизни:**

Покупая ноутбук, вы ищете отзывы на форумах, читаете статьи в СМИ и изучаете профили компании в соцсетях, чтобы убедиться в ее надежности - это элементарный пример применения OSINT.

Кто использует OSINT:

* Службы разведки и правоохранительные органы.
* Журналисты-расследователи.
* Аналитические агентства и специалисты по кибербезопасности.
* Киберпреступники.
* Люди, ищущие информацию о компаниях или частных лицах.
* **Социальная инженерия:** Методы манипуляции людьми для получения конфиденциальной информации. В контексте сбора данных о сотрудниках это может включать анализ профилей для выявления слабых мест (например, для фишинга).
* **Риски сбора информации:** Утечка данных может привести к шантажу, краже идентичности, корпоративному шпионажу или кибератакам. Защита включает минимизацию онлайн-присутствия, использование приватных настроек и корпоративные политики.
* **Источники информации:**
* Социальные сети (VK, LinkedIn, Facebook, Instagram).
* Корпоративные сайты и пресс-релизы.
* Поисковые системы (Yandex, Google).
* Открытые базы данных (например, реестры компаний, публикации в СМИ).
* Профессиональные сети и форумы.

**2.2. Этапы сбора информации**

1. **Определение цели:** Выбрать "цель" (компания) для анализа.
2. **Поиск базовой информации:** ФИО, должность, контакты.
3. **Расширенный анализ:** Семья, хобби, геолокация, связи.
4. **Оценка рисков:** Как эта информация может быть использована злоумышленниками.
5. **Рекомендации по защите:** Шаги для снижения уязвимостей.

**Порядок выполнения работы**

Выберите реальную организацию (например, Kolesa Group, Kaspi, Yandex Qazaqstan, EPAM Kazakhstan, Wooppay, Beeline Kazakhstan и Freedom Bank, InDrive, Air Astana, Documentolog, Tele2/Altel, Parqour, Aviata.kz, DataArt, Cerebra, Clockster, Sergek Group, Акционерное общество «Национальные информационные технологии» и т.д.).

**Задания**

**Задание 1: Сбор базовой информации.**

Используя поисковые системы, найти:

1. Общая информация:

* **Сфера деятельности:** торговая, производственная, финансовая и т.д.
* **История компании**.
* **Конкурентные преимущества**.
* **Миссия и ценности** компании.

2 Юридическая и контактная информация:

* **Полное и сокращенное наименование компании.**
* **Юридический адрес:** (местонахождение юридического лица).
* **Фактический адрес:** (место осуществления деятельности).
* **Контактные данные:** телефоны, электронная почта, сайт.

3 **ФИО руководителя**, email и телефон.

5. Финансовая информация:

* **Доход, выручка, прибыль**.
* **Зарплата сотрудников.**

**Задание 2: Анализ отзывов о работе компании.**

1. Собрать отзывы с различных площадок о работе компании (Яндекс Карты, Google, 2ГИС, социальные сети и форумы, отзовики (IRecommend, Otzovik), т.д.).

2. Сгруппируйте отзывы по темам: обслуживание, качество продукта, цена, условия труда.

3. Определите преимущества и недостатки компании, сделайте выводы о надёжности.

**Контрольные вопросы**

1. Что такое OSINT и почему он важен для защиты информации?
2. Какие риски несет разглашение личных данных в соцсетях?
3. Как злоумышленник может использовать собранную информацию?
4. Перечислите способы минимизации утечек данных о сотрудниках.

**Требования к отчету**

Отчет должен быть оформлен в электронном виде (Word или PDF) и включать:

1. Титульный лист (ФИО студента, группа, дата).
2. Цель и теоретическую часть (кратко).
3. Описание выполненных заданий **со скриншотами**.
4. Ответы на контрольные вопросы.
5. Список использованных источников.

**Объем:** 5–10 страниц.

**Критерии оценки выполнения заданий**

* Полнота выполнения заданий (40%).
* Качество анализа (30%).
* Соблюдение этических норм (20%).
* Оформление отчета (10%).