**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Институт Цифры**

**ОТЧЕТ**

**О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ**

**«Анализ OSINT-инструментов сбора информации»**

по дисциплине «Информационная безопасность»

студентов 4 курса

**Мордвинов Станислава**

**Рябов Виталия**

**Копытов Андрея**

Направление 02.03.02 – «Фундаментальная информатика и информационные технологии»

Преподаватель:

канд. физ.-мат. наук, доцент Рейн Т.С.

Работа защищена

«\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

Кемерово 2025

# Введение

Поставлена цель провести анализ возможностей применения OSINT-инструментов для получения данных о компании «Инновационная мебельная логистика» эффективности OSINT.

С целью оценки защищённости организации применялись OSINT-инструменты, такие как аудит доменной структуры, диагностика сетевых слабостей и анализ рисков, связанных с действиями внутренних и внешних нарушителей. Особое внимание уделено актуальным угрозам: компрометации облачных данных, неконтролируемому стиранию информации и атакам на стратегические узлы инфраструктуры.

## Сбор информации о технологическом стеке

*Источники:* Веб-сайт компании, вакансии на HH.ru, GitHub, форумы (Stack Overflow).

*Цель:* Определение используемого ПО (СУБД, ERP-системы), серверного оборудования, протоколов связи.

*Пример:*

* Вакансия «Сетевой инженер» может требовать навыков работы с PostgreSQL или Cisco-оборудованием, что указывает на используемые технологии;
* Публичные репозитории GitHub с конфигурациями или скриптами могут раскрыть структуру БД или API.

## Поиск утечек данных

*Источники:* Базы утекших данных (Have I Been Pwned), темные веб-форумы.

*Цель:* Получение учетных данных сотрудников, данных клиентов.

*Пример:* Если сотрудники используют корпоративные email-адреса на сторонних сервисах (например, GitHub), их утечка может дать доступ к внутренним системам ИМЛ.

## Анализ сетевой инфраструктуры

*Источники:* WHOIS, DNS-записи, Shodan, Censys.

*Цель:* Обнаружение открытых портов, незащищенных серверов, поддоменов.

*Пример:*

* Поддомен tracking.iml.com может быть связан с системой отслеживания грузов. Если он использует устаревшую версию веб-сервера, это станет точкой входа;
* Shodan может найти IoT-датчики с открытым портом 8080 (веб-интерфейс без аутентификации).

## Социальная инженерия через соцсети

*Источники:* VK, Telegram, WhatsApp.

*Цель:* Фишинг, сбор данных о сотрудниках (роли, проекты).

*Пример:* Сотрудник в WhatsApp упоминает участие во внедрении «системы оптимизации маршрутов на Python». Злоумышленник может имитировать запрос от коллеги, чтобы получить доступ к разрабатываемой системе.

## Геопространственный анализ

*Источники:* Google Maps, спутниковые снимки, публичные отчеты.

*Цель:* Определение расположения, логистических центров, маршрутов.

*Пример:* Фото грузовика с логотипом ИМЛ в VK может быть геотегировано, что раскроет частые точки доставки.

## Анализ метаданных

*Источники:* Документы (PDF, Excel), публикуемые компанией.

*Цель:* Получение имен сотрудников, версий ПО, внутренних IP-адресов.

*Пример:* Отчет для инвесторов в PDF может содержать метаданные («Системный администратор: Сергей Симонов; контактный email: [cooladmin@mail.ru»](mailto:cooladmin@mail.ru)).

## Использование картографических данных

*Источники:* GPS-треки, публикуемые логистическими приложениями.

*Цель:* Предсказание маршрутов грузов для перехвата или кражи.

*Пример:* Если клиентское приложение показывает реальное время доставки, злоумышленник может определить паттерны перемещения грузовиков.

# Рекомендации по усилению защиты

* Ограничить публикацию технических деталей (вакансии, документация);
* Регулярно мониторить утечки в публичных базах данных;
* Проверять конфиденциальность метаданных в документах;
* Защищать API и IoT-устройства аутентификацией и шифрованием;
* Обучать сотрудников кибергигиене (не размещать служебную информацию в соцсетях).

# Заключение

Проведённый анализ демонстрирует, что система «Инновационная мебельная логистика» (ИМЛ) подвержена ряду рисков, связанных с использованием OSINT-методов. Злоумышленники могут получить доступ к критически важным данным (маршруты, клиентская база, производственные процессы) даже без прямого взлома защищённых систем, используя лишь публично доступную информацию.

Ключевыми *слабыми местами* являются:

* Избыточная открытость технической информации (вакансии, документация),
* Недостаточный контроль за метаданными и публичными интерфейсами,
* Уязвимость сотрудников к фишингу из-за публикации служебных данных в открытых источниках.