КЦПН

МЕРЫ ЗАЩИТЫ ОТ OSINT РАЗВЕДКИ ПРОТИВНИКА

ПОДГОТОВЛЕНО КООРДИНАЦИОННЫМ ЦЕНТРОМ ПОМОЩИ НОВОРОССИИ

2025 Г.

ОГЛАВЛЕНИЕ

Раздел 1: Основные принципы OSINT и методы анализа.

Что такое OSINT?

OSINT (Open-Source Intelligence) — это метод сбора, анализа и интерпретации данных из открытых источников. Он широко применяется в военной сфере, журналистике, бизнес-аналитике и кибербезопасности.

Основные источники информации:

- **Социальные сети** (Facebook, Twitter, Instagram, Telegram, TikTok и др.)
- **Средства массовой информации** (новостные сайты, блоги, форумы)
- **Государственные и коммерческие базы данных** (регистры компаний, судебные документы)
- **Геолокационные сервисы** (Google Maps, OpenStreetMap, сервисы обратного поиска по фото)
- **Темные и закрытые сети** (DarkNet, специализированные форумы)

OSINT является мощным инструментом, но несет и угрозы — злоумышленники могут собирать личную или военную информацию для разведки и деструктивных действий.

Методы анализа OSINT

1. Обратный поиск изображений

Этот метод позволяет идентифицировать местоположение, объекты и даже людей по фотографиям. Используются такие сервисы, как:

- **Google Images** — поиск по фото с автоматическим анализом содержимого.
- **TinEye, Pimeyes** — поиск оригинальных версий изображений и сопоставление лиц.
- **Яндекс.картинки** — лучше распознает лица и объекты в русскоязычном интернете.

2. Анализ метаданных фото и видео

Каждый цифровой файл содержит скрытую информацию, те самые метаданные (EXIF, IPTC, XMP), они включают в себя:

- **Дата и время съемки**
- **Геолокация/местоположение** (если опция включена в камере)
- **Модель устройства, с помощью которого фотография выполнена**
- **Настройки камеры и авторство файла**

3. Метаданные можно просмотреть с помощью:

- **ExifTool** (командная строка, анализ EXIF)
- **Metapicz** (онлайн-сервис)
- **Opanda IExif** (просмотрщик метаданных)

Перед публикацией фото и видео **необходимо очищать метаданные**, иначе противник сможет определить местоположение, время съемки и личность автора.

4. Идентификация объектов по фону и окружению

Анализ заднего плана может раскрыть важные данные о месте съемки:

- **Архитектурные объекты** (характерные здания, мосты, дороги)
- **Природные особенности** (горы, реки, тип растительности)
- **Знаки, указатели, билборды** (могут содержать названия улиц, городов)

Противник использует **геолокационный анализ** для поиска объектов в реальном мире, сопоставляя изображения с картами и спутниковыми снимками.

5. Перекрестный анализ данных

Комбинирование информации из нескольких источников позволяет получать точную разведывательную картину.

Примеры:

- Анализ постов в соцсетях: публикация о путешествии + фото билета = место и дата поездки.
- Сопоставление данных из форумов и базы данных регистраций автомобилей.
- Слежка за активностью пользователя через лайки, подписки, комментарии.

Лучший способ защиты — **избегать создания цифрового следа**, который можно проанализировать.

Раздел 2: Что нельзя снимать и публиковать

Публикация определенных типов информации в открытых источниках может представлять серьезную угрозу безопасности. В условиях военного положения и повышенной активности разведки противника важно понимать, какие данные нельзя выкладывать в интернет, чтобы не дать врагу тактического преимущества.

Одной из ключевых категорий запрещенного к публикации контента являются военные объекты и инфраструктура. Съемка штабов, казарм, складов боеприпасов, аэродромов, контрольно-пропускных пунктов и фортификационных сооружений может привести к раскрытию расположения войск и планов их передвижения. Кроме того, публикация фото военной техники, особенно с видимыми номерами, маркировкой и знаками отличия, позволяет идентифицировать подразделения, их численность и оснащение. Любая информация о местоположении, эксплуатации и техническом состоянии вооружения и транспорта может быть использована противником.

Особую опасность представляют кадры, на которых запечатлены лица военнослужащих, их знаки различия, нашивки и медали. По этим деталям можно не только определить личность человека, но и его принадлежность к конкретным подразделениям. Еще большей угрозой является распространение информации о численности войск,

маршрутах передвижения и текущих операциях. Даже если такие сведения случайно попадают в кадр во время разговора, важно понимать, что их можно восстановить с помощью технологий анализа звука или даже прочитать с губ на видеозаписях, если аудио было удалено.

Проблемой также является раскрытие географического положения съемки. Вид из окон военных объектов, ориентиры в городской застройке, уличные таблички, рекламные билборды или даже уникальные природные объекты могут помочь врагу установить точное местоположение автора снимка. Еще большую угрозу несет съемка с беспилотников, поскольку такие кадры дают детальное представление о позициях войск, рельефе местности и потенциальных уязвимостях обороны.

При публикации видео и аудиоматериалов следует учитывать не только содержание основных событий, но и фоновые элементы. Шумы транспорта, сирены, звонки, голоса людей могут выдать стратегически важные сведения. Кроме того, случайные предметы в кадре, такие как документы, списки, QR-коды, могут стать источником утечки данных. Даже отражения в зеркалах, стеклах автомобилей или экранах мониторов способны раскрыть информацию, которая казалась незаметной на первый взгляд.

Опасность представляют и кадры, связанные с гражданской инфраструктурой, если они могут быть использованы для нанесения ударов по важным объектам. Электростанции, мосты, железнодорожные узлы, склады горючего, медицинские учреждения — все это критические точки, которые враг может взять на прицел. Не менее важно следить за содержанием публикаций, касающихся общественного транспорта и маршрутов передвижения, так как подобные данные могут использоваться для планирования диверсий или атак.

Особую бдительность следует проявлять при публикациях в социальных сетях. Размещение снимков в режиме реального времени, особенно с включенной геолокацией, позволяет легко определить текущее местоположение пользователя. Опасность представляют и комментарии к постам, где люди могут случайно выдать критически важные сведения. Даже простые отметки на картах или теги в постах способны раскрыть стратегически значимые локации.

Разберём на примерах:

Пример №1: Танк ВС РФ

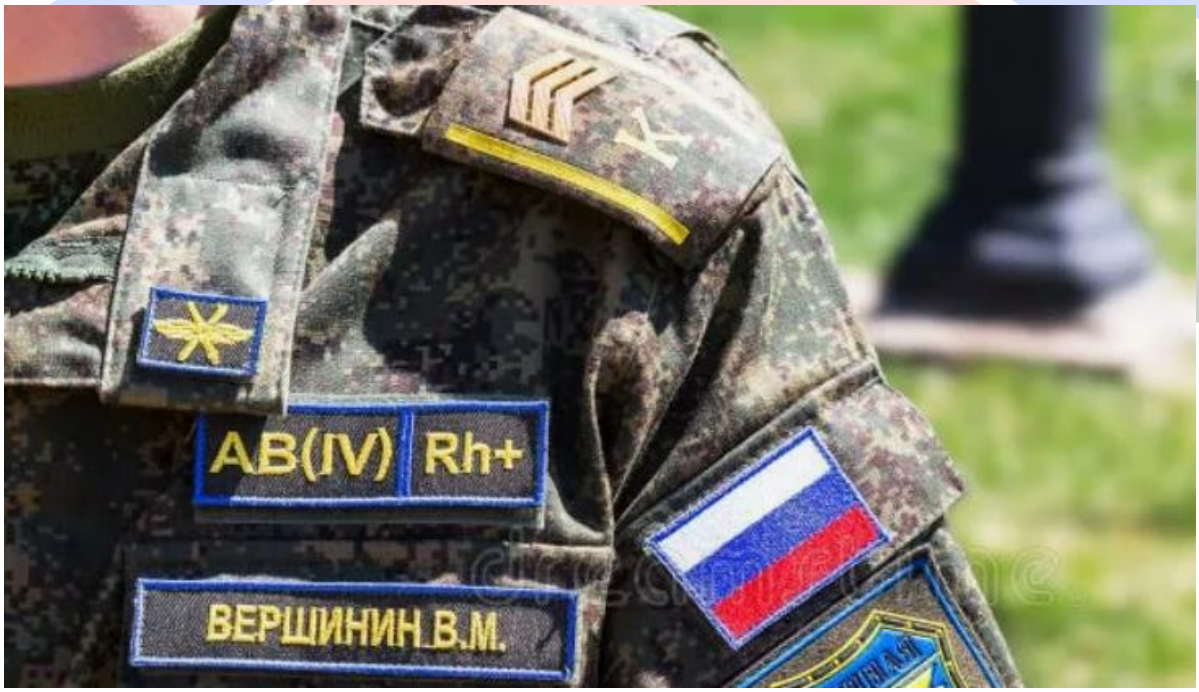
Маркировка и собственные обозначения на танке, дают общее понимание о расчёте боевой машины.

Пример №2: Фотография военной базы.

Хотя какие-либо условные знаки не бросаются сразу в глаза. По заднему фону специалисты с лёгкостью определят точное местонахождение военной части.

Пример №3: Фото военнослужащего с шевронами

По шевронам бойцов можно с лёгкостью определить какое именно подразделение находится на фото. Это может дать понимание о примерном количестве личного состава и роде войск.



Пример № 4 Фотография работы системы ПВО

Через обратную картографию, даже по фотографии неба, противник выясняет местоположение наших систем ПВО, после чего уничтожает их или продумывает маршруты с учётом их обхода.

Раздел 3: Методы защиты от OSINT-разведки

Сегодня почти любая информация, которую мы выкладываем в интернет, может быть использована против нас. Даже обычное фото может рассказать о местоположении, времени съемки и деталях жизни. Чтобы не стать жертвой OSINT-разведки, важно соблюдать простые правила безопасности.

Одно из главных правил — **удалять скрытые данные из фото и видео**. Каждая картинка или ролик могут содержать информацию о времени съемки, геолокации и модели устройства. Перед публикацией **нужно удалить метаданные** с помощью специальных программ или настроек телефона. Это поможет скрыть ваше местоположение и другие личные данные.

Еще один важный шаг — **маскировать детали, которые могут раскрыть важную информацию**. Простое размытие лица или номеров машин может быть недостаточным, так как современные технологии умеют восстанавливать размытые изображения. Лучше использовать:

- **Пикселизацию в несколько слоев**, чтобы скрытые элементы нельзя было восстановить.
- **Обрезку изображения**, чтобы удалить подозрительные детали из кадра.
- **Физическую маскировку** (очки, балаклавы), если фото все-таки нужно сделать.

Очень важно **не передавать свое местоположение**. Современные телефоны автоматически добавляют геотеги (координаты) к фотографиям. Даже если функция отключена, враг может определить место по фону, знакам или погоде. Чтобы защититься, стоит:

- **Выключить геолокацию в камере и соцсетях.**
- **Не публиковать фото сразу после съемки. В идеале всегда использовать отложенную публикацию**
- **Следить за деталями фона на снимке.**

Ваши цифровые следы тоже могут многое рассказать о вас. Некоторые приложения, такие как GetContact или TrueCaller, собирают данные и раскрывают ваш номер телефона и подписи в контактах других людей. Чтобы не попасть в эту ловушку, нужно:

- **Не устанавливать сомнительные приложения, которые собирают личные данные.**
- **Периодически менять аватарки и никнеймы, чтобы усложнить поиск вашей информации.**
- **Ограничить доступ к личным данным в соцсетях.**

Социальные сети — это один из главных источников информации для разведки. Если вы выкладываете фото или пост, особенно в режиме реального времени, враг может вычислить ваше местоположение и маршруты передвижения. Чтобы этого избежать, лучше:

- **Публиковать снимки с помощью функции отложенная публикация (В телеграмме необходимо, зажать кнопку отправки сообщения и выбрать «Отправить позже».**
- **Закрывать свой профиль от посторонних.**
- **Удалять старые посты, которые могут рассказать о вас слишком много.**

Безопасность также зависит от того, **как вы передаете информацию**. Обычные SMS и звонки не защищены, поэтому лучше использовать мессенджеры с **сквозным шифрованием** или секретные чаты в Telegram. Чтобы защитить свои переписки, рекомендуется:

- **Регулярно удалять сообщения и файлы.**
- **Не сохранять резервные копии в облаке.**
- **Использовать сложные пароли и двухфакторную аутентификацию.**

И наконец, **следите за своими устройствами**. Некоторые функции смартфонов могут передавать данные без вашего ведома. Чтобы минимизировать риски, нужно:

- **Выключать Bluetooth, Wi-Fi и NFC, когда они не используются.**
- **Использовать VPN для защиты интернет-трафика.**
- **Регулярно обновлять операционную систему и приложения.**

Раздел 4: Продвинутые методы защиты

Если основные способы защиты помогают скрыть очевидные вещи, то расширенные методы делают вас почти невидимыми для разведки. Они требуют немного больше усилий, но значительно снижают риск утечки информации.

1. Стирание цифровых следов

Каждый оставляет следы в интернете: старые профили, лайки, комментарии, подписки. Все это можно использовать, чтобы собрать о вас информацию. Чтобы усложнить задачу врагу, нужно:

- **Удалять или закрывать старые аккаунты.** Даже если вы давно ими не пользовались, в них могут быть ваши личные данные.

- **Менять стиль поведения в соцсетях.** Например, не отмечать геолокацию и не писать подробности о себе.
- **Использовать разные фото и имена в разных сервисах.** Так сложнее связать ваши профили между собой.

2. Защита данных на телефоне и компьютере

Даже если вы не выкладываете личную информацию, она может попасть в чужие руки через ваше устройство. Чтобы этого не случилось, важно:

- **Не сохранять пароли в браузере, вводить их вручную.**
- **Не подключаться к неизвестным Wi-Fi-сетям без VPN.** Через них могут украсть ваши данные.
- **Удалять ненужные приложения.** Некоторые программы следят за вами, даже когда вы ими не пользуетесь.
- **Использовать специальные приложения на подобии KillApps для полноценного удаления/выключения приложений**

3. Создание ложных следов

Если враг все же ищет информацию о вас, можно его запутать. Это не значит, что нужно врать, просто стоит усложнить анализ:

- **Создавать учетные записи на ненастоящие данные.**
- **Подписываться на паблики других регионов.** Это сбивает с толку тех, кто пытается вас отследить.
- **Использовать анонимные аккаунты для обсуждения важных тем.**

4. Проверка информации перед публикацией

Перед тем как что-то выложить, подумайте: **"Что это может обо мне рассказать?"** Даже обычное фото может выдать ваше местоположение или привычки. Поэтому:

- **Проверяйте фон на снимках.** Нет ли там уличных табличек, чеков, личных данных?
- **Обрезайте фото, если на нем есть лишние детали.**
- **Не выкладывайте снимки в момент съемки.** Лучше подождать несколько дней.

5. Проверка утечки данных

Есть специальные сервисы, которые помогают узнать, какие данные о вас уже есть в интернете:

- **PimEyes, TinEye** — ищут ваши фото в сети.
- **Google Dorks** — помогает найти утекшие данные через поисковик.
- **Shodan** — показывает, какие устройства в вашей сети открыты для посторонних.

COGITO ERGO VINCO

МЫСЛЮ, СЛЕДОВАТЕЛЬНО, ПОБЕЖДАЮ!

Приложение: Чек-листы или же шпаргалки

Чтобы защитить себя от OSINT-разведки, важно не только знать теорию, но и применять ее на практике. Ниже собраны простые и понятные рекомендации, которые помогут избежать утечки информации.

1. Чек-лист перед публикацией фото и видео

Перед тем как выложить снимок или видео в интернет, задайте себе несколько вопросов:
☑ **Есть ли на фото что-то, что может выдать мое местоположение?** (Уличные таблички, знаковые здания, пейзаж, билеты, чеки)
☑ **Удалены ли метаданные?** (Геолокация, дата съемки, модель устройства)
☑ **Нет ли в кадре лиц людей, техники, номеров машин, военной формы?**
☑ **Можно ли по фото понять, где я живу или работаю?**
☑ **Не сделано ли оно в режиме реального времени?** (Лучше публиковать снимки с задержкой)

Если хоть на один вопрос ответ «Да», **лучше не выкладывать фото или обработать его перед публикацией.**

2. Чек-лист для защиты аккаунтов и данных

🔒 Защита соцсетей

- **Сделайте профили закрытыми, уберите из открытого доступа личные данные.**
- **Ограничьте круг подписчиков, удалите неизвестных людей.**
- **Отключите автоматическую геолокацию в постах и фото.**
- **Не публикуйте информацию о поездках в режиме реального времени.**

📱 Безопасность телефона и компьютера

- **Удалите ненужные приложения, особенно те, которые запрашивают много разрешений.**
- **Отключите Bluetooth, Wi-Fi и NFC, если они не используются.**
- **Не сохраняйте пароли в браузере, используйте менеджеры паролей.**
- **Включите двухфакторную аутентификацию (2FA) на важных аккаунтах.**

🛡️ Защита личных данных

- **Не используйте одно и то же имя и фото для всех сервисов.**
- **Периодически меняйте пароли, особенно после утечек данных.**
- **Проверяйте свои данные через сервисы вроде haveibeenpwned.com.**

3. Чек-лист действий если данные уже утекли?

Если вы обнаружили, что ваша личная информация оказалась в открытом доступе:

- **Удалите или измените информацию в своих аккаунтах.**
- **Поменяйте пароли и включите двухфакторную защиту.**
- **Свяжитесь с администрацией сайта и попросите удалить ваши данные.**
- **Если речь идет о важной информации (например, домашний адрес, номер паспорта), будьте особенно осторожны и минимизируйте риск утечек в будущем.**

4. Чек-лист того, что нельзя публиковать

1) Военная информация

- Военные объекты и инфраструктура
- Штабы, казармы, склады боеприпасов, аэродромы, военные базы.
- Контрольно-пропускные пункты (КПП), места дислокации войск.
- Инженерные сооружения (фортификации, бункеры, укрытия).
- Военная техника и оборудование
- Боевая техника (танки, бронетранспортеры, артиллерия, авиация).
- Маркировка и номера на технике.
- Эксплуатация техники, передвижение колонн.
- Военнослужащие и их атрибутика
- Лица военнослужащих, знаки различия, нашивки, медали.
- Специальные подразделения и их опознавательные знаки.
- Разговоры, касающиеся дислокации, численности, планов.
- Производственные мощности
- Заводы по производству оружия, боеприпасов, беспилотников.
- Склады с оборудованием, логистические узлы.

2) Геолокация и ориентиры

- Опасные элементы на фотографиях
- Вид из окон военных зданий (по нему можно определить расположение).
- Ориентиры, которые помогают идентифицировать местоположение (телебашни, церкви, мосты, особенные здания).
- Дорожные знаки, билборды, адресные таблички.
- Съемка с дронов
- Фото и видео, снятые с воздуха, могут раскрыть позиции войск и техники.
- Дроновые кадры позволяют противнику анализировать рельеф, пути подъезда.

- Анализ погодных условий и теней
- Сезонность (наличие снега, осенней листвы) может указать на время года.
- Длина теней помогает определить время суток и стороны света.

3) Анализ видео и аудиофайлов

- Идентификация по звукам
- Фоновые шумы (голоса, транспорт, железная дорога, авиация).
- Опознавательные сигналы (сирены, звонки).
- Риски «читаемых губ»
- Даже если аудио заглушено, текст можно восстановить по движению губ.
- Если в видео упоминаются конфиденциальные данные (количество войск, маршруты, операции), рекомендуется закрывать рот говорящего черным прямоугольником.
- Опасность случайных деталей в кадре
- Документы, списки, пароли, QR-коды могут быть замечены в кадре.
- Отражения в зеркалах, стеклах, экранах мониторов.

4) Гражданские объекты, имеющие стратегическое значение

- Инфраструктура
- Электростанции, ГЭС, ТЭЦ, линии электропередач.
- Железнодорожные узлы, мосты, тоннели.
- Газопроводы, нефтехранилища.
- Медицинские учреждения
- Военные госпитали, эвакуационные пункты.
- Размещение пострадавших и медперсонала.
- Общественный транспорт и маршруты
- Транспортные узлы, логистические центры.
- Перевозка военных грузов.

5) Социальные сети и личные данные

- Опасность публикации в реальном времени
- Выдача текущего местоположения при съемке и трансляции.
- Противник может использовать данные о передвижениях.
- Раскрытие информации в комментариях и сообщениях
- Даже личная переписка может быть перехвачена и проанализирована.
- Посторонние могут сопоставить публичные комментарии и личные данные.
- Опасность «геотегов» и отметок
- Отмеченные места могут указать на военные объекты.
- По истории отметок можно восстановить маршрут передвижения