OSINT – Тренды на три года. Прогноз Кибердеда.

Андрей Масалович, Конференция IAPD, сентябрь 2024

СОДЕРЖАНИЕ

применения сотрудниками специальных тактических методов, приемов и способов ведения наблюдения.

Тактика скрытого наблюдения — это совокупность индивидуальных и групповых действий сменного наряда в процессе стационарного и подвижного наблюдения, основанных на применении определенных построений и комбинаций с использованием специальных способов и приемов, направленных на конспиративное получение полной объективной информации об объекте наблюдения и его связей.

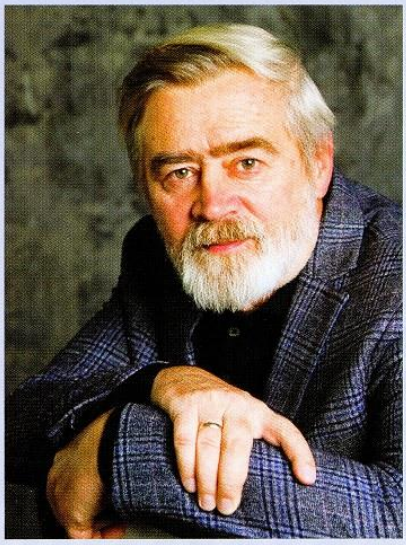
Методы ведения скрытого наблюдения:

— Стационарный метод предполагает наблюдение за определенными территориями, домами, квартирами осуществляемые с специально подобранных мест — постов скрытого наблюдения.

— Подвижный метод предполагает осуществление наблюдения за действиями объектов и их связей при их перемещениях.

Стационарное и подвижное наблюдение ведется с использованием разнообразных способов и приемов, выработанных практикой и рекомендованных специальными инструкциями по организации и проведению скрытого наблюдения. Приемы ведения скрытого наблюдения составляют качественное содержание процесса наблюдения. Работа в группе значительно повышает её качество и конспиративность, однако при этом сотрудники смены должны уверенно владеть приёмами одиночного (индивидуального) наблюдения, при установлении связей от разрабатываемых лиц. Необходимо подчеркнуть, что групповые и индивидуальные тактические действия сотрудников, направленные на решение задач, стоящих перед скрытым наблюдением, должны носить строго конспиративный характер. При выборе методов, способов и приёмов наблюдения необходимо понимать личность объекта. Например лица, ранее судимые, как правило, пытаются выявить наблюдение, прибегая к изощренным приемам, а лица, не осведомленные о методах негласной работы, ведут себя спокойнее и их проверочные действия не столь опасны для опытных сотрудников. Успешное выполнение целей скрытого наблюдения зависит от четкого выполнения каждым сотрудником своих обязанностей.

OSINT — ТРЕНДЫ НА ТРИ ГОДА. МОЙ ПРОГНОЗ



Андрей Игоревич Масалович

Вице-президент IAPD (МОД)

Разведка по открытым источникам, или OSINT (Open Source INTelligence) жизненно важна для решения задач обеспечения информационной безопасности и выполнения миссий разведывательного сообщества. Использование методов OSINT расширяет инструментарий разведки, дисциплинирует и обеспечивает уникальную разведывательную ценность, позволяя

более эффективно и действенно использовать широкий спектр возможностей сбора и сопоставления данных. Как следствие, в ближайшие годы OSINT продолжит расширяться и развиваться с головокружительной скоростью. При этом уже сформировались явные тренды развития, которые сохранятся в ближайшие три года:

- Скоординированный сбор и накопление данных в форме **частно-государственного партнерства** под патронажем профильных спецслужб и Министерства обороны. Для этого государственные ведомства должны будут переосмыслить свои отношения с промышленностью, научными и академическими кругами и гармонизировать схемы взаимодействия (включая отработку реалистичных схем финансирования и планирования ресурсов);
- **Появление и развитие многодоменных каталогов данных**, что в свою очередь будет стимулировать развитие стандартов по очистке, обогащению и маркировке данных, а также улучшение совместимости коллекций данных различных прикладных систем;
- **Расширение и углубление** (пусть и со скрипом) **межведомственного взаимодействия** в планировании, координации и осуществлении разведывательных задач. Как следствие — устранение дублирования и повышение прозрачности в планировании и исполнении миссий и задач (хотя это уже какая-то фантастика);
- **Создание аналитических центров регионального, отраслевого и федерального уровней,** обладающих достаточной экспертностью для решения задач обеспечения национальной безопасности и способных предоставлять своевременную и достоверную информацию из открытых источников. политикам и военным силам быстро и масштабно, а также в различных форматах, адаптированных к различным миссиям и потребительским требованиям;
- Создание семейства **совместимых систем с открытым исходным кодом** и гибким расширяемым функционалом для интегрированного управления коллекциями данных;
- Быстрый **прогресс** в практическом использовании систем **искусственного интеллекта** и машинного обучения. Опережающими темпами будет развиваться **генеративный ИИ**;
- **Опережающее развитие алгоритмов автоматического определения происхождения и проверки достоверности данных** различной природы — текстовых, графических, акустических, видео и т.д. (включая автоматическое выявление deepfakes);
- Возникнет новый тренд — повсеместное появление **специализированных голосовых помощников и чат-ботов** для управления прикладными процессами и платформами решения аналитических задач, а также задачами контроля обстановки;
- Окончательно будет решена проблема встроенных многоязыковых автоматических переводчиков — как для текстовых данных, так и для аудиопотоков (включая возможность нативной коммуникации разноязычных собеседников);
- В полный рост встанет проблема **создания доверенной среды разработки систем машинного обучения, включая автоматизированный аудит** исходных данных, процессов настройки и обучения и условий применения ИИ;
- Наибольшие прорывы в использовании ИИ будут связаны с практическим **переходом на более совершенные модели нейронных сетей — Сети Колмогорова-Арнольда** (KAN — Kolmogorov-Arnold's Network));
- **Дальнейшая профессионализация OSINT как дисциплины**, в том числе — появление библиотек формализованных, стандартизованных и документированных рабочих процессов OSINT, а также внедрение показателей эффективности операций по сбору и аналитической обработке данных;
- Окончательное оформление дисциплины **OSINT как отдельного направления хакатонов и CTF;**
- **Развитие кадрового потенциала OSINT** и становление отдельной дисциплины — с формированием общих профессиональных стандартов, структуры учебных курсов подготовки кадров и методик тестирования сотрудников;

- **Распространение парадигмы динамического обучения** и регулярной профессиональной переподготовки ИТ-специалистов, обладающих навыками и опытом, чтобы идти в ногу с быстро развивающейся цифровой средой.

Профессиональные площадки обмена передовым опытом и мастерством в сфере OSINT (семинары и конференции) будут расширяться, **выйдут на международный уровень** и там закрепятся.

КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПОМОГАЕТ В РАССЛЕДОВАНИЯХ

Марат Салимуллович Габидуллин

Действительный член IAPD (МОД)

Компьютерный сыщик в арсенале современного детектива. Чтобы собрать информацию о персоне или компании, приходится вводить одни и те же данные на нескольких сайтах и повторять это до бесконечности. Как приятно было бы не тратить время на рутину, а заниматься делом. В этом уже сейчас может помочь искусственный интеллект, например:

- составить досье на человека;
- найти человека в другом регионе;
- проверить благонадежность фирмы или персоны;
- провести предварительный анализ в корпоративном расследовании.

Нейронная сеть помогает не только соберет нужные документы, но и установит скрытые связи. При чем поиск идет с соблюдением формальностей и норм законодательства, то есть по открытым государственным источникам.

Почему стоит отказаться от ручного поиска информации. Почему не получать информацию на сайтах государственных органов самостоятельно, ведь это бесплатно? Представим: мы собираем информацию о человеке.

Без использования системы это минимум 10 запросов. Необходимо вводить одни и те же данные, тратить время на распознавание капчи. Используя средние значения, получаем 17 однообразных действий в отношении одного лица. Если отдельно рассмотреть суды общей юрисдикции, мировые суды и т.п., то количество действий можно умножить еще как минимум на 10, если мы рассматриваем только один регион и хотим получить действительно полные данные. А если проверять по нескольким регионам или по всей России, то число запросов становится неподъемным. И самое главное, все эти данные надо изучить и проанализировать, что увеличивает время проверки еще на несколько порядков.

Минимум 17 действий, которые в результате дадут необработанную и некачественную информацию, против 1 действия через систему проверки контрагентов, такую как «Ирбис», ведь информация там вводится 1 раз. Какое количество информации можно упустить при