УДК 004.056

ТЕХНОЛОГИИ ОТКРЫТОГО СБОРА ИНФОРМАЦИИ (OSINT) В КОНТЕКСТЕ СОВРЕМЕННЫХ ВЫЗОВОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Прокопенко Е.В., к.ф.-м.н., доцент, заведующий кафедрой
Коротин В.О., преподаватель СПО кафедры ИБ
Луцык Е.М., студент гр. ИБт-221 кафедры ИБ
Скачкова А.И., студент гр. ИБт-221 кафедры ИБ
Кузбасский государственный технический университет имени Т.Ф. Горбачева
Россия, г. Кемерово

Современная цифровая экосистема характеризуется экспоненциальным ростом объема публично доступных данных. Этот массив информации, генерируемый пользователями, корпорациями и государственными институтами, формирует детализированное цифровое отражение реального мира. В данном контексте технологии открытого сбора информации (Open Source Intelligence, OSINT) трансформировались из узкоспециализированной практики, применяемой преимущественно государственными спецслужбами, в общедоступный и мощный инструмент для решения широкого спектра задач.

Актуальность темы обусловлена тем, что границы между физической и цифровой безопасностью становятся все более проницаемыми. Злоумышленники активно используют OSINT для сбора предварительной информации о целях (физических лицах и организациях) перед проведением целевых атак, фишинговых кампаний или актов социальной инженерии. Следовательно, для специалистов по защите информации владение методиками контрразведки на основе OSINT становится не просто полезным навыком, а обязательной компетенцией. Понимание того, какая информация о вашей организации находится в открытом доступе, позволяет proactively выстраивать оборону, минимизировать цифровой след и эффективно противодействовать угрозам.

Целью статьи является систематизация знаний о технологиях OSINT, анализ их современного инструментария и методологии, а также оценка их роли в комплексной системе информационной безопасности [1-3] .

Эволюция и методологические основы OSINT

Термин OSINT утвердился в профессиональной лексике во второй половине XX века, однако сама практика сбора информации из открытых источников имеет глубокие исторические корни. Классическое определение OSINT подразумевает под собой дисциплину сбора, анализа и распространения разведданных, полученных из легально доступных источников для решения конкретных задач.

Ключевым атрибутом OSINT является легальность доступа к информации. В отличие от хакерских методик, подразумевающих взлом систем или несанкционированный доступ, OSINT оперирует данными, которые были

добровольно размещены в публичном пространстве или индексируются поисковыми системами. К таким источникам традиционно относят:

1. Средства массовой информации: новостные порталы, газеты, телеканалы.

2. Интернет-ресурсы: веб-сайты, форумы, блоги, контент социальных сетей.

3. Публичные данные государственных органов: реестры юридических лиц, данные о госзакупках, судебные решения, кадастровая информация.

4. Научная и академическая среда: публикации, диссертации, патенты.

5. Техническая информация: данные WHOIS о доменных именах, сертификаты SSL, метаданные файлов, конфигурации сетевых устройств, доступные через системы типа Shodan.

Эволюция OSINT в последнее десятилетие связана с тремя основными факторами:

1. Социализация цифрового пространства: Появление социальных сетей создало беспрецедентный по объему источник личной и поведенческой информации.

2. Технологический прогресс: Развитие мощных поисковых систем, платформ для агрегации данных и аналитических инструментов позволило автоматизировать процессы сбора и первичного анализа.

3. Коммерциализация: Возникновение коммерческих OSINT-платформ (таких как Maltego, Recorded Future, Shodan) сделало передовые методики доступными для корпоративных специалистов по безопасности.

Классификация источников и современных инструментов OSINT

Для эффективного применения технологий OSINT необходима их четкая классификация. Источники можно структурировать по нескольким признакам.

По типу данных:

- Текстовая информация: Новостные ленты, посты в социальных сетях, форумы, документы.
- Визуальная информация: Фотографии, скриншоты, видео. Анализ метаданных (EXIF) графических файлов может раскрыть географические координаты, модель устройства и дату съемки.
- Геопространственные данные: Сервисы картографии (Google Maps, Yandex.Карты), спутниковые снимки, геотеги.
- Технические данные: Сетевые адреса, данные WHOIS, записи DNS, отпечатки SSL-сертификатов.

По уровню доступности:

- Поверхностный веб (Surface Web): Контент, индексируемый традиционными поисковыми системами (Google, Yandex).
- Глубокий веб (Deep Web): Данные, скрытые за формами авторизации или платными подписками (базы данных, научные библиотеки). Доступ к ним легален, но требует специальных процедур.

- Даркнет (Darknet): Сети, требующие для доступа специального ПО (например, Tor). Важно отметить, что OSINT не занимается сбором данных в даркнете, если такой доступ сопряжен с нарушением законодательства.

Современный инструментарий специалиста по OSINT представляет собой комбинацию автоматизированных платформ и ручных методик.

- Поисковые машины: Использование расширенных операторов Google, Yandex («site:», «filetype:», «intitle:») для точного поиска.
- Специализированные платформы: Shodan и Censys для поиска интернет-устройств; Maltego для визуализации связей между объектами; SpiderFoot для автоматизированного сбора разведданных.
- Агрегаторы социальных сетей: Инструменты, позволяющие осуществлять кросс-платформенный поиск по username (например, Sherlock), анализировать графы связей.
- Инструменты для анализа метаданных: ExifTool, FOCA.
- Сервисы проверки доменов и IP-адресов: WHOIS-сервисы, AbuseIPDB, VirusTotal.

Практическое применение OSINT в обеспечении информационной безопасности

Профилирование угроз (Threat Intelligence)
OSINT является фундаментом для построения системы киберразведки. Собирая информацию о группах хактивистов, методах и инструментах, используемых злоумышленниками (Tactics, Techniques, and Procedures, TTPs), организации могут anticipate потенциальные атаки. Анализ дискуссий на хакерских форумах, в Telegram-каналах позволяет выявить упоминания о компании, утечки данных или обсуждения уязвимостей в используемом ПО.

Расследование инцидентов информационной безопасности
При расследовании киберинцидента OSINT помогает установить источник атаки, идентифицировать злоумышленника и оценить нанесенный ущерб. Например, анализ логиров сервера может выявить IP-адрес атакующего. Последующий поиск по этому адресу через OSINT-инструменты может показать его связь с другими известными инцидентами, принадлежность к определенному хостинг-провайдеру или даже географическую привязку [4-6].

Оценка цифрового следа и пентестинг

Любая организация оставляет цифровой след — совокупность информации о себе в открытом доступе. Специалисты по безопасности проводят аудит этого следа, чтобы идентифицировать критические утечки: публикацию конфиденциальных документов, разглашение информации о внутренней IT-инфраструктуры (например, наименования серверов, используемое ПО), размещение в открытом доступе резервных копий. В рамках тестирования на проникновение (пентестинга) OSINT используется на этапе разведки (reconnaissance) для сбора максимального объема данных о цели перед моделированием атаки.

Противодействие социальной инженерии

Социальные инженеры строят свои атаки на информации. Проанализировав профили сотрудников в LinkedIn, Facebook, Instagram, злоумышленник может узнать имена их родственников, увлечения, график отпусков и другую информацию для создания правдоподобного предлога (претекста). Контрмерой является обучение сотрудников основам кибергигиены и проведение регулярного мониторинга открытых данных о ключевых сотрудниках компании.

Правовые и этические аспекты применения OSINT

Несмотря на то, что OSINT оперирует публичными данными, его применение связано с рядом правовых и этических вызовов.

- Соблюдение законодательства: В разных юрисдикциях действуют различные законы о защите персональных данных (в РФ — 152-ФЗ). Даже сбор публичных данных о физических лицах может подпадать под регулирование, если он приводит к созданию их детализированных профилей без явного согласия.
- Условия предоставления услуг (ToS): Многие платформы (например, LinkedIn, Facebook) в своих пользовательских соглашениях запрещают автоматизированный сбор данных. Нарушение этих условий может привести к юридической ответственности и блокировке аккаунтов.
- Этика: Существует тонкая грань между сбором информации и вторжением в частную жизнь. Профессиональное сообщество выработало этические принципы, согласно которым собранные данные должны использоваться исключительно в законных целях (обеспечение безопасности, расследования), а не для харассмента, шантажа или дискриминации.

Технологии OSINT прочно вошли в арсенал современных специалистов по информационной безопасности, превратившись из вспомогательного инструмента в стратегический актив. Способность эффективно собирать, анализировать и интерпретировать открытые данные позволяет организациям перейти от реактивной к проактивной модели безопасности, предугадывая и нейтрализуя угрозы на ранних стадиях.

В качестве перспектив развития OSINT можно выделить следующие тенденции:

1. Интеграция с искусственным интеллектом и машинным обучением: ИИ будет играть ключевую роль в обработке больших массивов неструктурированных данных (текстов на естественных языках, изображений, видео), автоматически выявляя аномалии, классифицируя угрозы и устанавливая скрытые связи.

2. Расширение возможностей прогнозной аналитики: Комбинация OSINT с технологиями больших данных позволит не только описывать текущую ситуацию, но и строить прогнозные модели развития киберугроз.

3. Усложнение инструментария: Появление более сложных платформ, объединяющих возможности сбора, анализа и визуализации в едином цикле.

4. Ужесточение правового поля: Рост осведомленности общества о приватности будет стимулировать принятие более строгих законов, что, в свою

очередь, потребует от специалистов по OSINT повышенного внимания к юридическим аспектам своей деятельности.

Таким образом, освоение методологии и инструментов открытого сбора информации является обязательным элементом подготовки высококвалифицированных кадров для сферы информационной безопасности. Умение работать с открытыми источниками позволяет закрыть критически важный участок обороны, который зачастую остается без должного внимания.

Список литературы:

1. Байков А.А., Дубовицкий Ю.Ю. Открытые источники информации в деятельности по обеспечению безопасности. // Защита информации. Инсайд. – 2021. – № 4. – С. 45-52.

2. Губарев Д.В. OSINT как инструмент кибербразведки в бизнес-среде. // Международный журнал информационной безопасности. – 2022. – Т. 14, № 1. – С. 78-85.

3. Соколов С.С. Методологические основы применения технологий OSINT в расследовании киберинцидентов. // Вопросы кибербезопасности. – 2020. – № 3(25). – С. 22-29.

4. Шаров А.В. Правовые и этические аспекты сбора и использования открытой информации. // Право и цифровая экономика. – 2023. – № 1. – С. 112-119.

5. Chirillo, J. Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit. – Wiley Publishing, 2001.

6. Long, J., Bazzell, M. Open Source Intelligence Techniques: For Security, Intelligence, and Investigative Professionals. – 9th Edition. – CreateSpace Independent Publishing Platform, 2022.