Вдовченко Г.П. Сбор информации из открытых источников (SHODAN, MALTEGO, SPIDERFOOT) // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 17–22

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.53

СБОР ИНФОРМАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ (SHODAN, MALTEGO, SPIDERFOOT)

Вдовченко Г.П.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: vdovchenko2003@gmail.com

Современные инструменты сбора данных из открытых источников (OSINT) стали незаменимыми в сфере кибербезопасности и анализа угроз. В статье рассматриваются три ключевых платформы — Shodan, Maltego и SpiderFoot, — их функциональные возможности, применение для поиска уязвимостей, анализа сетевой инфраструктуры и цифровых следов. Особое внимание уделено этическим и правовым аспектам работы с OSINT. Материал предназначен для специалистов по информационной безопасности, аналитиков и исследователей, работающих с открытыми данными.

Ключевые слова: OSINT, Shodan, Maltego, SpiderFoot, кибербезопасность, сетевые устройства, уязвимости, IoT-гаджеты, визуализация данных, автоматизация, GDPR, этический хакинг, фишинг, анализ угроз.

OPEN SOURCE INTELLIGENCE GATHERING (SHODAN, MALTEGO, SPIDERFOOT)

Vdovchenko G.P.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: vdovchenko2003@gmail.com

Modern tools for gathering data from open sources (OSINT) have become indispensable in the field of cybersecurity and threat analysis. The article explores three key platforms—Shodan, Maltego, and SpiderFoot—their functionalities, applications in identifying vulnerabilities, analyzing network infrastructure, and tracing digital footprints. Special attention is paid to the ethical and legal aspects of working with OSINT. The material is intended for information security specialists, analysts, and researchers dealing with open data.

Keywords: OSINT, Shodan, Maltego, SpiderFoot, cyber intelligence, network devices, vulnerabilities, IoT gadgets, data visualization, automation, GDPR, ethical hacking, phishing, threat analysis.

Введение

В условиях цифровой трансформации сбор информации из открытых источников (OSINT) превратился в критически важный инструмент для предотвращения кибератак, аудита безопасности и управления рисками. Такие платформы, как Shodan, Maltego и SpiderFoot, автоматизируют процессы разведки, позволяя выявлять уязвимости, анализировать сетевые инфраструктуры и прогнозировать угрозы. Однако их использование требует не только технических навыков, но и соблюдения правовых норм. В статье подробно разбираются принципы работы этих инструментов, их сильные стороны и ограничения.

Сбор информации из открытых источников (Shodan, Maltego, SpiderFoot)

В современном мире, где объемы открытых данных растут экспоненциально, инструменты OSINT (Open Source Intelligence) становятся ключевым элементом стратегий кибербезопасности. Платформы Shodan, Maltego и SpiderFoot предоставляют специалистам уникальные возможности для сбора, анализа и интерпретации информации, доступной в публичном пространстве. Эти инструменты позволяют не только реагировать на уже существующие угрозы, но и предугадывать потенциальные риски, основываясь на данных из интернета, социальных сетей и сетевых инфраструктур. Их применение охватывает широкий спектр задач — от выявления уязвимых устройств до расследования сложных кибератак, однако требует внимательного подхода к правовым и этическим аспектам.

Shodan, известный как «поисковая система для интернета вещей», представляет собой мощный инструмент для индексации устройств, подключенных к глобальной сети. В отличие от традиционных поисковиков, таких как Google, Shodan специализируется на сборе метаданных о сетевых устройствах — серверах, веб-камерах, IoT-гаджетах и даже промышленных системах управления [2]. Он предоставляет информацию об открытых портах (например, HTTP на порту 80 или SSH на порту 22), версиях программного обеспечения, геолокации и владельцах устройств. Простой запрос вроде «webcam country:RU» позволяет найти тысячи веб-камер в России, а более специфичный — «port:21 Anonymous user logged in» — выявляет FTP-серверы с анонимным доступом, которые могут быть уязвимы для атак [4]. В сфере кибербезопасности Shodan используется для аудита корпоративных сетей, помогая обнаружить устройства, которые случайно или намеренно остались открытыми для внешнего доступа. Например, компании могут проверить, не подключены ли их серверы к интернету без должной защиты, что особенно актуально для критической инфраструктуры, такой как электростанции или медицинские учреждения [2]. Однако возможности Shodan имеют и обратную сторону: злоумышленники могут использовать его для поиска целей, таких как незащищенные IoT-устройства в больницах, как это было зафиксировано в Европе в 2023 году [4]. Чтобы минимизировать риски, эксперты рекомендуют ограничивать публичный доступ к устройствам, регулярно обновлять прошивки и использовать брандмауэры для фильтрации трафика.

Maltego, в свою очередь, выделяется как инструмент для визуализации связей между различными объектами в рамках OSINT-разведки. Эта платформа позволяет аналитикам строить графы, связывающие людей, домены, IP-адреса и другие сущности, используя так называемые трансформы — скрипты, которые собирают данные из множества источников, включая WHOIS, Shodan, Twitter и LinkedIn [3]. Например, начав с домена, такого как example.com, пользователь может запустить трансформ «Domain to DNS Records», чтобы получить связанные IP-адреса, а затем расширить граф до SSL-сертификатов, субдоменов и даже владельцев этих ресурсов. Такой подход особенно полезен для расследования фишинговых атак, где необходимо выявить сеть клоновых доменов, созданных для обмана пользователей [5]. Maltego также применяется в борьбе с кибершпионажем, помогая отслеживать IP-адреса, связанные с APT-группами (Advanced Persistent Threats), и выявлять их инфраструктуру [4]. Однако работа с Maltego требует определённых навыков: без понимания OSINT-методик интерпретация графов может быть затруднена, а бесплатная версия (Maltego CE) ограничивает доступ к продвинутым трансформам, что снижает её

эффективность для сложных задач [3]. Несмотря на это, способность инструмента визуализировать сложные взаимосвязи делает его незаменимым для аналитиков, стремящихся понять структуру атакующего или защитить свою организацию от скрытых угроз.

SpiderFoot дополняет арсенал OSINT-инструментов, предлагая автоматизированный подход к сбору данных. Этот open-source фреймворк объединяет более 200 модулей, которые собирают информацию из самых разных источников — от DNS-записей и социальных сетей до VirusTotal и HaveIBeenPwned [1]. Например, запустив сканирование корпоративного домена, аналитик может обнаружить субдомены, утекшие учетные данные сотрудников или даже подозрительные файлы, связанные с этим доменом [5]. Основное преимущество SpiderFoot — экономия времени: вместо ручного поиска данных из десятков источников инструмент выполняет эту задачу автоматически, предоставляя результаты в удобном формате. Его гибкость позволяет настраивать модули под конкретные цели, будь то проверка безопасности внутренней сети или анализ внешних угроз [1]. Однако у SpiderFoot есть и слабые стороны: из-за большого объёма собираемой информации высока вероятность ложноположительных результатов, а интерпретация данных требует дополнительной фильтрации и проверки [3]. Это делает его особенно полезным для опытных аналитиков, способных отделить значимые сигналы от шума, но менее удобным для новичков.

Каждый из этих инструментов обладает уникальными характеристиками, которые определяют их применение в кибербезопасности. Shodan идеально подходит для поиска устройств и анализа их уязвимостей, особенно в контексте интернета вещей и критической инфраструктуры [2]. Его простота делает инструмент доступным даже для пользователей с минимальным опытом, хотя платный API необходим для получения полного функционала. Maltego, напротив, требует более глубокого подхода, но компенсирует это способностью раскрывать сложные взаимосвязи, что критично для расследований фишинга или кибершпионажа [4]. SpiderFoot выделяется своей автоматизацией, что делает его незаменимым для масштабных проектов разведки, хотя аналитикам приходится тратить время на проверку результатов [1]. Сравнение этих платформ по ключевым критериям — цели, сложности, стоимости и этическим рискам — показывает, что они дополняют друг друга, покрывая разные аспекты OSINT. Например, Shodan может выявить уязвимое устройство, Maltego — связать его с атакующим, а SpiderFoot — собрать дополнительные данные для полного анализа.

Важным аспектом работы с этими инструментами является соблюдение правовых и этических норм. Использование OSINT регулируется такими законами, как GDPR в Европе или ст. 272 УК РФ в России, которые запрещают несанкционированное сканирование сетей или сбор персональных данных без согласия [1]. Например, сканирование корпоративной сети с помощью Shodan без разрешения владельца может быть расценено как нарушение закона, даже если данные находятся в открытом доступе. Аналогично, применение Maltego для анализа социальных сетей или SpiderFoot для проверки утечек email требует строгого соблюдения конфиденциальности — использование собранной информации для атак или личной выгоды недопустимо [5]. Этические риски особенно высоки для Shodan, так как его данные могут быть легко направлены на поиск уязвимых целей, тогда как SpiderFoot, будучи менее ориентированным на прямое сканирование, представляет меньшую угрозу в этом плане [2]. Чтобы минимизировать риски, специалисты должны строго следовать принципам этического хакинга, получать разрешения на тестирование и документировать свои действия.

Интеграция Shodan, Maltego и SpiderFoot в рабочие процессы позволяет создать мощную систему киберразведки. Например, организация может начать с Shodan для обнаружения уязвимых IoT-устройств в своей сети, затем использовать Maltego для анализа связанных доменов и IP-адресов, а завершить процесс SpiderFoot, собрав дополнительные данные из открытых источников [3]. Такой подход особенно эффективен при расследовании сложных атак, таких как фишинг или инсайдерские угрозы, где требуется объединить данные из разных источников для построения полной картины [5]. Однако успех зависит от способности аналитиков комбинировать возможности инструментов, избегая при этом избыточности и юридических нарушений.

Будущее этих платформ связано с развитием технологий искусственного интеллекта, которые могут повысить их эффективность. Например, ИИ-алгоритмы в Shodan могли бы автоматически классифицировать устройства по уровню риска, в Maltego — предлагать гипотезы связей на основе исторических данных, а в SpiderFoot — фильтровать ложноположительные результаты [4]. Это снизило бы нагрузку на аналитиков и ускорило процесс принятия решений. Однако даже с такими улучшениями человеческий фактор останется ключевым — способность критически оценивать данные и принимать этически обоснованные решения будет определять успех OSINT-разведки в условиях всё более сложных киберугроз.

Заключение

Shodan, Maltego и SpiderFoot подтверждают, что инструменты OSINT стали незаменимым ресурсом в арсенале специалистов по кибербезопасности. Их эффективность, однако, зависит не только от технологических возможностей, но и от профессионализма пользователей, а также строгого следования правовым нормам. Например, Shodan способен выявить тысячи незащищенных IoT-устройств, но без умения аналитика интерпретировать эти данные в контексте конкретной организации или инфраструктуры, такая информация теряет практическую ценность. Кроме того, злоупотребление возможностями Maltego для сбора персональных данных или SpiderFoot для массового сканирования сторонних сетей без разрешения может привести к юридическим последствиям, включая нарушения GDPR или локальных законов о конфиденциальности. Будущее развития OSINT-инструментов тесно связано с интеграцией искусственного интеллекта и машинного обучения. ИИ-алгоритмы смогут автоматизировать рутинные задачи, такие как фильтрация ложных срабатываний в SpiderFoot, прогнозирование киберугроз на основе исторических данных Shodan или ускорение анализа сложных связей в Maltego. Это не только повысит скорость обработки информации, но и снизит нагрузку на специалистов, позволяя сосредоточиться на стратегических аспектах расследований. Однако даже с внедрением ИИ критически важным останется человеческий фактор — способность критически оценивать результаты, выявлять скрытые паттерны и принимать этически взвешенные решения. Для организаций, внедряющих OSINT-практики, ключевым приоритетом должно стать обучение сотрудников. Программы подготовки должны включать не только технические навыки работы с инструментами, но и основы киберэтики, понимание регуляторных требований (таких как HIPAA в медицине или PCI DSS в финансовом секторе) и управление рисками. Например, политики компании могут запрещать использование Shodan для сканирования сетей партнеров без письменного согласия или требовать многоуровневой проверки данных, полученных через Maltego. Такие меры

помогут избежать случайных нарушений и минимизировать репутационные потери. Рост числа подключенных устройств, усложнение фишинговых атак и увеличение объемов открытых данных ставят перед OSINT новые вызовы. Платформы вроде Shodan сталкиваются с проблемой информационной перегрузки, где даже простой поиск по ключевым словам возвращает десятки тысяч результатов, требующих ручной верификации. В ответ на это разработчики активно внедряют системы категоризации на основе ИИ, которые автоматически классифицируют устройства по типу, уровню уязвимости или географическому расположению. Одновременно Maltego и SpiderFoot эволюционируют в сторону междисциплинарного использования — от расследований киберпреступлений до журналистских расследований и аудита цепочек поставок. В конечном счете, сила OSINT-инструментов заключается не в их технологической сложности, а в способности специалистов сочетать их возможности с критическим мышлением, креативностью и ответственностью. Shodan, Maltego и SpiderFoot — это не «волшебные палочки», решающие все проблемы кибербезопасности, а инструменты, которые требуют осознанного подхода. Их дальнейшее развитие будет определяться балансом между автоматизацией и человеческим контролем, между скоростью сбора данных и соблюдением правовых границ. В мире, где киберугрозы становятся все более изощренными, именно этот баланс позволит превратить открытую информацию из потенциальной уязвимости в надежный щит для организаций и общества в целом.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
2. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Региональная информатика (РИ-2022). – 2022. – С. 572-573
3. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии // Телекоммуникации. – 2020. – №. 8. – С. 14-20.
4. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
5. Голубов Н. А., Косов Н. А. Внутренние угрозы: Разнообразие и профилактика инсайдеров в организациях. – 2023.

References

1. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems // Actual problems of infotelec communications in science and education (APINO 2019). – 2019. – pp. 266-270.
2. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network // Regional Informatics (RI-2022). – 2022. – pp. 572-573

3. Akhrameeva K. A. and others. Analysis of the means of exchanging hidden data by intruders on the Internet using steganography methods // Telecommunications. – 2020. – No. 8. – pp. 14-20.
4. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system // Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 406-411.
5. Golubev N. A., Kosov N. A. Internal threats: Diversity and prevention of insiders in organizations. – 2023.