Ермек Ерболатович Шегенов

студент специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, dr.emek@yandex.ru

Диана Вильдановна Каримова

старший преподаватель кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, d.v.karimova@utmn.ru

РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ДАННЫХ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

Аннотация. В статье представлена характеристика разведки на основе открытых данных как эффективного способа сбора и анализа информации из общедоступных источников, рассмотрен широкий спектр использования технологий OSINT в современных условиях, представлена классификация источников данных, определены ключевые направления обеспечения экономической безопасности хозяйствующих субъектов, в рамках которых могут успешно применяться приемы OSINT, определены перспективы использования OSINT в условиях активного развития искусственного интеллекта.

Ключевые слова: OSINT-разведка, информация, источники данных, экономическая безопасность.

Ermek Yerbolatovich Shegenov

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, dr.emek@yandex.ru

Diana Vildanovna Karimova

Senior Lecturer at the Department of Economic Security, System Analysis and Control of Tyumen State University, Tyumen, d.v.karimova@utmn.ru

EXPLORATION BASED ON OPEN DATA IN ENSURING THE ECONOMIC SECURITY OF BUSINESS ENTITIES

Abstract. The article presents the characteristics of open data-based intelligence as an effective way to collect and analyze information from open sources, considers a wide range of OSINT technologies in modern conditions, presents a classification of data sources, identifies key areas for ensuring economic security of business entities within which OSINT techniques can be successfully applied, defines the prospects for using OSINT in conditions of active the development of artificial intelligence.

Keywords: OSINT-intelligence, information, data sources, economic security.

OSINT (Open-Source Intelligence, аналитика открытых источников) представляет собой сбор, обработку и анализ информации, полученной из интернета, с помощью открытых средств и источников. Направление OSINT-разведки появилось в 1941 году, когда Соединенные Штаты Америки создали службу мониторинга зарубежного вещания (Foreign Broadcast Monitoring Service, сокращенно FBMS), сотрудники которой записывали и переводили иностранные радиопередачи, а затем отправляли в военные и разведывательные органы в виде отчетов. В 1947 году служба FBMS была переименована в Службу внешней радиовещательной разведки (Foreign Broadcast Intelligence Service, сокращенно FBIS) и подчинена Центральному разведывательному управлению (ЦРУ). С помощью OSINT американские спецслужбы, в частности, определяли ситуацию в высших эшелонах власти СССР по тому, какие лица находились на трибуне Мавзолея, а в 1958 году по фотографии из июль-

ского номера журнала «Огонек» полностью воспроизвели схему электроснабжения Урала и определили местонахождение секретного завода по производству ядерного оружия [1].

Несмотря на то, что зародилась технология в недрах спецслужб, многие из нас, даже не подозревая об этом, применяют приемы OSINT-разведки в своей повседневной жизни в настоящее время. Так, перед покупкой того или иного товара, в особенности на интернет-площадках, мы можем тщательно изучать информацию о его производителе и продавце, качестве, просматривать отзывы других покупателей. При написании статьи, подготовке реферата или доклада мы находим необходимую информацию на сайтах электронных библиотек, баз знаний и на других интернет-ресурсах, изучаем материалы конференций, круглых столов и форумов. Информацию о заинтересовавшем нас человеке мы ищем в его социальных сетях. Читаем отзывы, просматриваем карты и онлайн-камеры перед поездкой в путешествие. Это лишь небольшая часть примеров, когда приемы OSINT используются нами в обычной жизни.

Широкий спектр использования технологий OSINT в различных сферах человеческой деятельности, таких как раскрытие преступлений, обеспечение кибербезопасности, бизнес-аналитика, журналистские расследования, и др., раскрывается в работах многих зарубежных и отечественных исследователей. Так, Юйсюань Сесилия Чжан с соавторами показала растущий объем информации ОСИНТ, используемой злоумышленниками, атакующими промышленные устройства, а также обосновала потребность в программах, обучении и политиках, необходимых для защиты промышленных систем [2]. Мюррей Дарра, Кениг К. и Ивонн Макдермотт провели анализ того, как информация из открытых источников используется на практике миссиями ООН, комиссиями по расследованию и другими официальными расследователями при установлении фактов нарушения прав человека [3]. Стивен Коттен сравнил коммерческие решения для бизнес-аналитики, ориентированные на конкретного поставщика, и методы OSINT для мониторинга бизнес-аналитики [4]. Минченко В.И. и Вильдяйкин Г.Ф. рассмотрели в своей статье разведку на основе открытых источников, ее методологию и этапы в современных реалиях [5]. Тихновецкий Д.И. показал несколько вариантов применения инструментов ОСИНТ для повышения уровня защищенности предприятия [6]. Бессонов А.А. в своей работе подвел итог, что исследования в области поиска и анализа информации из открытых источников могут существенно дополнить теорию информационного обеспечения оперативно-розыскной деятельности, а разработка специальных методов и средств для этой технологии способна повысить эффективность выявления, раскрытия, расследования и профилактики преступлений [7].

Особую значимость методы OSINT приобретают в процессе обеспечения экономической безопасности хозяйствующих субъектов.

Экономическая безопасность хозяйствующего субъекта — это комплекс мер и стратегий, направленных на предотвращение и устранение как внешних, так и внутренних угроз и опасностей хозяйствующему субъекту с целью поддержания его стабильной деятельности. Для предотвращения негативного влияния внешних и внутренних угроз специалистам в области обеспечения экономической безопасности необходимо обладать различной актуальной информацией.

Основные направления обеспечения экономической безопасности бизнеса, в рамках которых, по нашему мнению, могут использоваться приемы OSINT-разведки, представлены на рис. 1.

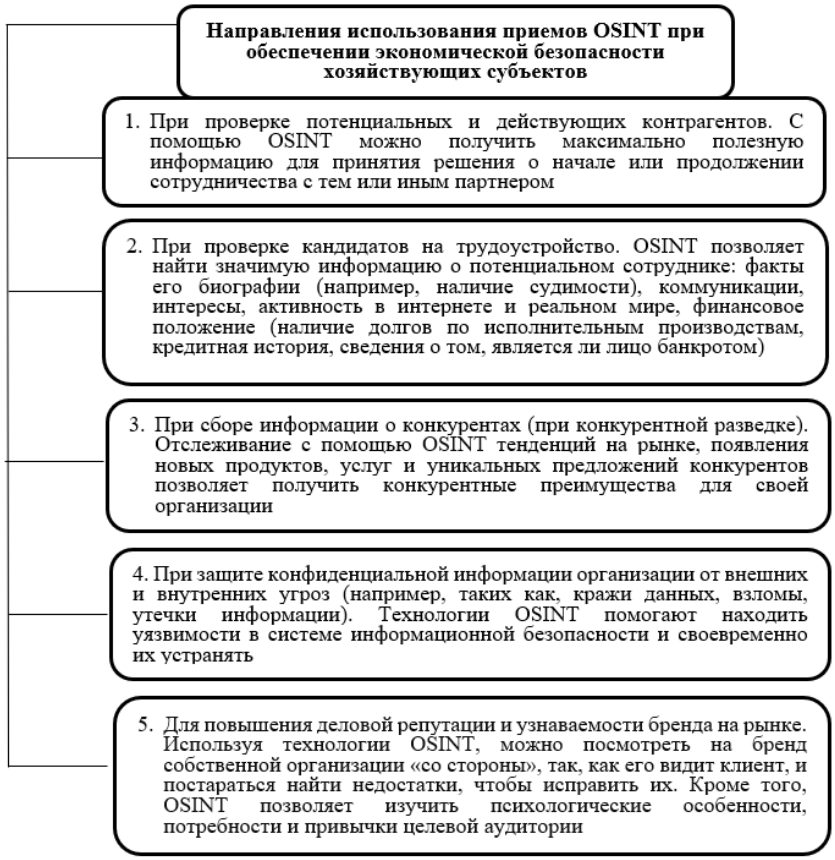

Рис. 1. Направления использования приемов OSINT при обеспечении экономической безопасности хозяйствующих субъектов

Источник: составлено авторами на основе данных [8].

Для того чтобы понять, где осуществляется поиск интересующей информации, рассмотрим существующие виды источников информации:

1. Открытые — источники информации, которые предоставляют ее без требования сохранения ее конфиденциальности [9]. Это, как правило, бесплатные ресурсы, которые находятся в общем доступе. В качестве примера таких источников можно привести публичную корпоративную информацию, размещенную на официальных сайтах организаций (финансовая и нефинансовая отчетность, аудиторские заключения), федеральные государственные и иные публичные реестры сведений и базы данных (Единый государственный реестр юридических лиц или индивидуальных предпринимателей (ЕГРЮЛ/ЕГРИП), Единый реестр субъектов малого и среднего предпринимательства, Реестр дисквалифицированных лиц, Реестр массовых руководителей и массовых

учредителей, Государственный информационный ресурс бухгалтерской (финансовой) отчетности (ГИР БО), Картотека арбитражных дел и др.), открытые СМИ и соцмедиа (газеты «Ведомости», «Коммерсантъ», «Комсомольская правда» и др.; РИА Новости; ресурсы, содержащие компромат-сведения и др.).

2. Полуоткрытые — специализированные сервисы, предлагающие систематизированную информацию о различных юридических и физических лицах. Они оценивают кредитные риски, выявляют бенефициаров, анализируют финансово-экономические показатели и др. Использование данных систем не только упрощает работу сотрудникам, но и значительно повышает безопасность компании в целом, однако большинство из таких сервисов являются платными. В качестве примера полуоткрытых источников информации можно привести информационно-аналитические системы Спарк, СБИС, Контур.Фокус, Rusprofile и др.

3. Полузакрытые — источники, предусматривающие запрос на поиск искомой информации, сведений в свободном доступе нет. Для запроса необходимо уточнить цель поиска, без нее могут не предоставить доступ к искомым данным (базы данных Росфинмониторинга, архивного фонда РФ, Роскомнадзора и др.).

4. Закрытые источники информации — полностью скрытые источники данных, пользоваться которыми могут лишь определенные специалисты, наделенные полномочиями (базы данных ФСБ, МВД, ФБР или Интерпола) [10].

Рассмотрим отдельные инструменты или специализированные программы, с помощью которых можно найти необходимую информацию в открытых источниках.

Google Dorks (также известный, как Google dorking) — это метод, который используется для наилучших результатов поиска необходимой информации в Google. Обычно Google dorks применяется исследователями или хакерами для поиска важной информации о компании, отдельном человеке, программном обеспечении или приложении, теме исследования или о чем-либо еще. Но обычный человек также может использовать Google dorks для различных задач, что сэкономит время и, безусловно, позволит получить более качественную информацию [11]. Например, команда:

cache: используется для поиска кэшированной версии любого веб-сайта;

allintext: выполняет поиск определенного текста, содержащегося на любой веб-странице (allintitle: покажет страницы, содержащие заголовки);

allinurl (inurl): может использоваться для получения результатов, URL-адрес которых содержит введенный текст;

filetype: используется для поиска любых расширений файлов (pdf, doc, txt, xls);

intext: применяется для поиска страниц, содержащих определенные символы или строки внутри их текста;

site: покажет полный список всех проиндексированных URL-адресов для указанного домена и поддомена;

*****: подстановочный знак, используемый для поиска страниц, содержащих «что угодно» перед словом, например, how to * a website, вернет «how to...» design/create/hack, etc... «a website» [12, 13];

I: это логический оператор, с помощью которого можно найти сайты по ключевым словам. Например, при вводе слов «безопасность», «взлом» будут показаны все сайты, которые содержат «безопасность» или «взлом», или оба слова;

+: используется для объединения слов, полезно для обнаружения страниц, использующих более одного определенного ключа, не обязательно идущих друг за другом;

–: минус используется для того, чтобы избежать отображения результатов, содержащих определенные слова, например, «безопасность — взлом» покажет страницы, в тексте которых используется «безопасность», но не те, в которых есть слово «взлом» [14].

Осуществить поиск конкретного пользователя в социальных сетях в короткие сроки позволяет сервис "Instant Username Search", хранящий базы данных более 100 платформ. Для получения информации нужно указать никнейм пользователя в поисковой строке.

Еще одной полезной программой является WHOIS. WHOIS — это общедоступная база данных, в которой хранится информация, собираемая, когда кто-либо регистрирует доменное имя или обновляет настройки своего DNS-сервера. WHOIS помогает демократизировать Интернет. Любой желающий, от предприятий и корпораций до правоохранительных органов и индивидуальных пользователей может получить доступ к базе данных WHOIS и использовать ее, чтобы узнать, кто стоит за доменным именем и любым связанным с ним вебсайтом [15].

Одной из самых эффективных утилит является Maltego. Это программное обеспечение, которое помогает специалистам в области безопасности собирать информацию о людях или компаниях в Интернете. Это позволяет им сопоставлять данные и выявлять связи между профилями в социальных сетях, адресами электронной почты, номерами телефонов, местоположениями, профессиональной принадлежностью и другой информацией. Информация представляется в виде графических ссылок и диаграмм взаимосвязей. Maltego предлагает множество преимуществ для различных организаций. Специалисты по кибербезопасности могут использовать Maltego для сбора ценной информации об угрозах, которые могут снизить безопасность компании [16].

Для нахождения скрытых данных о контрагенте может помочь поисковая система Intelligence X, которая также является архивом большого количества информации. Intelligence X отличается от других поисковых систем следующими особенностями: поиск осуществляется с помощью конкретных поисковых запросов, таких как адреса электронной почты, домены, URL-адреса, IP-адреса, идентификаторы CIDR, биткойн-адреса, хэши IPFS и т. д.; поиск осуществляется в таких местах, как даркнет, платформы обмена документами, утечки общедоступных данных и др. [17].

Для выявления внутренних уязвимостей компании может использоваться интеллектуальная поисковая система Shodan (аббревиатура от Sentient Hyper-Optimized Data Access Network). Она определяет, где размещены устройства, подключенные к Интернету, и кто ими пользуется. Shodan собирает информацию в основном по следующим портам: HTTP, FTP, SSH, Telnet) и SNMP. Shodan позволяет компаниям защищать свои устройства, определяя, какие из

них подвержены внешним атакам или проблемам с конфигурацией. Также эта поисковая система может использоваться для поиска информации о действующих устройствах интернета вещей по всему миру [18].

Информационно-аналитические системы проверки контрагентов и физических лиц, упрощающие сбор, систематизацию и анализ данных (Спарк, Контур. Фокус, СБИС и др.).

Используемые в OSINT-разведке методы и инструменты можно разделить на две категории:

1. Пассивные. Являются упрощенными методами сбора информации. Аналитики получают необходимые сведения через поиск в Интернете вручную или с помощью специальных сервисов и инструментов. Пассивной разведкой могут заниматься абсолютно все, у кого есть компьютер и доступ в Интернет [8]. Главное преимущество пассивного поиска — скрытость проведения OSINT-операций, действия специалистов остаются незамеченными.

2. Активные. Это противоположная сторона поиска в открытых источниках, которая предполагает динамичный подход к нахождению общедоступных данных. Включает в себя проведение различных опросов и анкет, взаимодействие с целью в социальных сетях, проведение онлайн-конференций и участие в них и др. Активный тип поиска информации имеет риск быть обнаруженным, так как для его использования необходимо непосредственно контактировать с целью.

Процедура проведения разведки на основе открытых данных предполагает выполнение следующих этапов:

Этап 1 «Определение цели OSINT-разведки». Работа начинается с определения цели и предмета разведки. Специалисты экономической безопасности определяют соответствующие источники информации, которые могут дать ценную информацию. Этот этап закладывает основу для всестороннего сбора данных путем определения потенциальных каналов и хранилищ для исследования.

Этап 2 «Сбор данных». После определения источников следующий этап включает систематический сбор данных: извлечение информации из общедоступных платформ, баз данных, социальных сетей и других доступных каналов. Цель состоит в том, чтобы собрать широкий спектр данных, подготовив почву для детального анализа на последующих этапах.

Этап 3 «Обработка данных». Как только данные собраны, они подвергаются обработке, которая включает в себя организацию и структурирование информации для получения значимых выводов.

Этап 4 «Анализ данных». Анализ — это критический этап, на котором обработанные данные тщательно анализируются на предмет закономерностей, аномалий и потенциальных индикаторов угроз. Эксперты применяют различные аналитические методы для выявления скрытых связей и оценки достоверности информации. На этом этапе необработанные данные преобразуются в оперативную информацию, которая помогает принимать решения в условиях растущих рисков.

Этап 5 «Конечная аналитика OSINT-сведений». Кульминацией жизненного цикла OSINT является создание готовых интеллектуальных данных. Это

уточненный, проанализированный и пригодный для применения результат, полученный на предыдущих этапах. Готовая аналитика обеспечивает всестороннее представление о потенциальных угрозах, предлагая стратегическую информацию, которая позволяет организациям принимать обоснованные решения и внедрять эффективные меры безопасности.

Реализуя указанные выше этапы, организации могут использовать возможности OSINT для повышения своей безопасности и активного реагирования на возникающие угрозы [19].

Прогресс в направлении разведки на основе открытых источников данных не стоит на месте. Около 15 лет назад все поиски информации делались вручную, приходилось самостоятельно искать информацию и анализировать ее. В настоящее время уже существует много ботов и нейросетей, способных помочь человеку при ОСИНТ-разведке. Такие помощники существенно снижают время на выполнение задач и улучшают качество анализа информации из интернета. По мнению эксперта в области OSINT Александра Есаулова, чат-боты уже сейчас могут автоматизировать задачи OSINT, а также написать отчет о проделанной работе. Он отмечает: «Вскоре умрут традиционные поисковики: мы потеряем доступ к самостоятельному поиску информации — готовые ответы будет нам выдавать нейросеть. Это и хорошо, и плохо. Хорошо — потому что нейросеть можно эффективно использовать, если вы, конечно, умеете это делать. Плохо — потому что нейросеть будет нас цензурировать» [20]. Важно отметить, что будущее в этой сфере будет лежать на плечах нейросетей, то есть можно сказать, что OSINT будет не только развиваться совместно с ними, но и напрямую зависеть от них.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Schneider Florian. The Evolution of Open Source Intelligence (OSINT) / Jan Störger // The Intelligencer. — V.19, num. 3. — 2013. — С. 53-56. — URL: https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf (дата обращения: 25.03.2024).
2. Zhang Y. C., Frank R., Warkentin N., Zakimi N. Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure // Journal of Cybersecurity. — 2022. — № 8. — URL: https://www.researchgate.net/publication/361116049_Accessible_from_the_open_web_a_qualitative_analysis_of_the_available_open-source_information_involving_cyber_security_and_critical_infrastructure (дата обращения: 25.03.2024).
3. Murray D., McDermott Y., Koenig K. Mapping the Use of Open Source Research in UN Human Rights Investigations // Journal of Human Rights Practice. — 2022. — № 14. — URL: https://www.researchgate.net/publication/363184751_Mapping_the_Use_of_Open_Source_Research_in_UN_Human_Rights_Investigations (дата обращения: 25.03.2024).
4. Cotten S. Comparing Commercial, Vendor-Specific vs Open-Source Business Intelligence Dashboard Solutions // The journal of applied laboratory medicine. — 2023. — № 8. — С. 223-225. — URL: https://www.researchgate.net/publication/366958477_Comparing_Commercial_Vendor-Specific_vs_Open-Source_Business_Intelligence_Dashboard_Solutions (дата обращения: 25.03.2024).
5. Минченко В. Разведка на основе открытых источников (OSINT) и ее методология в современных реалиях / В. Минченко, Г.Ф. Вильдяйкин // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: Материалы III

Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых: в 3 ч. (Комсомольск-на-Амуре, 06–10 апреля 2020 года) / редколл.: Э.А. Дмитриев (отв. ред.) [и др.]. Ч. 2. — Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2020. — С. 319-322. — URL: https://elibrary.ru/download/elibrary_43817023_56506173.pdf (дата обращения: 25.03.2024).
6. Тихновецкий Д.И. Применение инструментов OSINT для повышения безопасности предприятия / Д.И. Тихновецкий // Молодой ученый. — 2021. — № 51(393). — С. 31-33. — URL: https://moluch.ru/archive/393/86870 (дата обращения: 26.03.2024).
7. Бессонов А.А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) / А.А. Бессонов // Актуальные вопросы теории и практики оперативно-разыскной деятельности: сборник научных трудов Межведомственной научно-практической конференции (Москва, 16 сентября 2022 года). — Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. — С. 40-45. — URL: https://elibrary.ru/download/elibrary_49747465_12625405.pdf (дата обращения: 27.03.2024).
8. Дворянкин О.А. OSINT, PENTEST И НЕТСТАЛКИНГ — Информационные технологии интернета // НАУ. — 2022. — № 84-2. — URL: https://cyberleninka.ru/article/n/osint-pentest-i-netstalking-informatsionnye-tehnologii-interneta (дата обращения: 02.04.2024).
9. Качалов А.Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А.Г. Качалов, М.М. Лантаев // Юридическая наука: история и современность. — 2021. — № 9. — С. 98-106. — URL: https://www.elibrary.ru/item.asp?id=47609078 (дата обращения: 31.03.2024).
10. Уровни доступа к источникам информации. — URL: https://dzen.ru/a/XiCrdez7gACu44My (дата обращения: 20.03.2024).
11. Google Dorks Simplified. — URL: https://github.com/dheerajydv19/Google-Dorks-Simplified (дата обращения: 31.03.2024).
12. Google dork. — URL: https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06 (дата обращения: 30.03.2024).
13. Что такое Google dork? Как обезапасить себя и свой сайт от взлома? — URL: https://dzen.ru/a/X32uBrSALxxKkuVD (дата обращения: 30.03.2024).
14. Инструменты для разведки и иследования. — URL: https://telegra.ph/Instrumenty-dlya-razvedki-i-sledovaniya-05-29 (дата обращения: 02.04.2024).
15. What is WHOIS and How Is It Used? — URL: https://www.domain.com/blog/what-is-whois-and-how-is-it-used (дата обращения: 31.03.2024).
16. Maltego: Check how exposed you are online. — URL: https://www.welivesecurity.com/2023/06/22/maltego-check-exposed-online/ (дата обращения: 31.03.24).
17. Intelligence X. — URL: https://alternativeto.net/software/intelligence-x/about (дата обращения: 31.03.2024).
18. Introduction to Shodan. — URL: https://mcsi-library.readthedocs.io/articles/2022/07/introduction-to-shodan/introduction-to-shodan.html (дата обращения: 31.03.24).
19. Admin. Power of OSINT in Cybersecurity: A Comprehensive Guide. — URL: https://www.forensicsinsider.com/cybersecurity/osint-in-cybersecurity/ (дата обращения: 17.03.2024).
20. «Пробива» уже мало: OSINT выходит из «тусовки» на большой рынок. — URL: https://dzen.ru/a/ZBmtxE7vaSa4NtO (дата обращения: 31.03.24).