DOI: 10.18137/RNU.V9187.23.01.P.61 УДК 004.056

М.Е. Сидорова, А.Р. Кузьмин

РАЗВЕДКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ ДАННЫХ И ЕЕ ПРИМЕНЕНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Разведка по открытым источникам данных (от англ. Open Source Intelligence, OSINT) – это концепция, описывающая поиск, сбор, анализ и использование информации из открытых источников, а также совокупность методов и инструментов для решения этих задач. С развитием инфокоммуникационных технологий области применения OSINT также существенно расширились – от проверки благонадежности и личных связей отдельного физического лица, конкурентной разведки субъектов предпринимательской деятельности до поиска брешей в национальной обороне противоборствующих сторон и выявлении слабых мест в обеспечении информационной безопасности объектов критической инфраструктуры. Целью настоящей статьи является систематизация актуальных методов разведки по открытым источникам данных и анализ их применимости для решения задач кибербезопасности. Контент-анализ общедоступных источников информации и исследований по теме OSINT позволил сформировать систему методов разведки по открытым источникам данных для задач кибербезопасности, которая приведена в виде таблицы в конце статьи.

Ключевые слова: разведка по открытым источникам, OSINT, информационная безопасность, кибербезопасность, кибертерроризм.

M.E. Sidorova, A.R. Kuzmin

OSINT AND ITS APPLICATION FOR CYBER SECURITY

Abstract. Open source intelligence (OSINT) is a concept that describes the search, collection, analysis and use of information from open sources, as well as a set of methods and tools. With the development of infocomm technologies, the areas of OSINT application have also expanded significantly. For instance, from checking the reliability and personal connections of an individual user, competitive intelligence of business entities to finding gaps in the national defense of the warring parties and identifying weaknesses in ensuring the critical infrastructure information security. The aim of the article is to systematize the OSINT methods and analyze their applicability in the context of cybersecurity tasks. The proposed system of OSINT methods for cybersecurity tasks is based on the content analysis of open source resources and research results on the topic of OSINT.

Keywords: open source intelligence, OSINT, information security, cybersecurity, cyber terrorism.

Разведка по открытым источникам

История использования открытых источников информации для поддержки принятия важных управленческих, политических или военных решений восходит к истокам возникновения органов разведки. Пионером методологизации и институционализации разведки по открытым источникам данных считаются Соединенные Штаты Америки. Правительство США создало Службу мониторинга зарубежного вещания (Foreign Broadcast Monitoring Service, FBMS), которая выросла из исследовательской инициативы Принстонского Университета и быстро набрала обороты после атаки сил Японии на Перл-Харбор в 1941 году. После своего переименования в Службу внешней радиовещательной разведки (Foreign Broadcast Intelligence Service, FBIS) в 1947-м служба вошла в состав только что созданного Центрального разведывательного управления (Central

© Сидорова М.Е., Кузьмин А.Р., 2023

Сидорова Мария Евгеньевна
преподаватель 10-й кафедры, Михайловская военная артиллерийская академия, Санкт-Петербург. Сфера научных интересов: разведка по открытым источникам; криптоанализ; теория игр. Электронный адрес: m.e.sidorova@gmail.com

Кузьмин Александр Ростиславович
аспирант кафедры информационной безопасности, Санкт-Петербургский государственный электротехнический университет «ЛэТИ», Санкт-Петербург. Сфера научных интересов: информационная безопасность киберфизических систем; распределенные реестры; разведка по открытым источникам. Автор 5 опубликованных научных работ. ORCID: 0000-0002-0393-412X Электронный адрес: alexander.kouzmin@gmail.com

Intelligence Agency, CIA). В настоящее время методы и инструменты OSINT доступны не только государственным организациям и спецслужбам, но и частным компаниям и энтузиастам-исследователям.

На Рисунке 1 показаны основные вехи в истории OSINT.

Рисунок 1. Основные вехи в истории OSINT*
*Здесь и далее рисунки составлены авторами.

Разведывательный цикл

Взаимосвязанные действия частных и государственных разведывательных структур представляют собой систематический процесс, называемый разведывательным циклом.

Разведывательный цикл – процесс превращения необработанной информации в готовые разведданные для использования политиками, военными и другими потребителями при принятии решений [1, p. 4]. В литературе и на практике существует несколько версий разведывательного цикла, отличающихся по количеству этапов процесса.

Так, М. Минкина [2] перечисляет четыре этапа: управление/запрос, приобретение/собирание, обработка/анализ, распространение/разработка и передача получателю. В официальной публикации «Национальная разведка США. Обзор за 2013 год» указано шесть этапов: планирование и руководство, сбор, обработка и эксплуатация, анализ и производство, распространение, оценка [3]. О важности этапа сбора информации (разведданных) лучше всего свидетельствует тот факт, что в публикациях его называют осно-

вой разведки или «сердцем разведки». В США средства сбора разведданных называются дисциплинами сбора, или INTs [4]. Сбор разведданных осуществляется с использованием различных источников и методов разведки. Согласно Голдману источниками могут быть люди, изображения, сигналы, документы, базы данных и средства связи, от которых можно получить информацию с помощью определенных методов сбора и анализа [5]. Методы разведки включают стратегию и тактику разведдеятельности.

В Таблице 1 представлены дисциплины сбора информации и их краткое описание [6].

Таблица 1

Дисциплины сбора разведданных*

Название дисциплины сбора разведданных	Описание дисциплины
COMINT	Коммуникационная разведка, иногда радиоразведка (Communication Intelligence)
CULTINT	Разведка культурных особенностей (Cultural Intelligence)
DFINT	Разведка на основе форензики (Digital Forensics Intelligence)
ELINT	Радиотехническая разведка (Electronic Intelligence)
GEOINT	Геопространственная разведка (Geospatial Intelligence)
HUMINT	Разведка по людям (Human Intelligence)
IMINT	Разведка изображений (Image Intelligence)
MARKINT	Маркетинговая разведка (Market Intelligence)
MASINT	Измерительно-сигнатурная разведка (Measurement and Signature Intelligence)
OSINT	Разведка по открытым источникам (Open source intelligence)
SIGINT	Радиоэлектронная разведка (Signal Intelligence)
SOCMINT	Разведка социальных сетей (Social Media Intelligence)
TECHINT	Техническая разведка (Technical Intelligence)
TELINT	Разведка сигналов телеметрии (Telemetry Intelligence)

** Здесь и далее таблицы составлены авторами.*

Каждая из этих дисциплин решает конкретные задачи для разведывательных служб. Кроме того, OSINT непосредственно может быть основным инструментом для решения тех или иных задач, например, поиска геопространственной информации для GEOINT с использованием таких ресурсов, как Google Maps. Дж. Виртц [7] отмечает, что термин «методы разведки» относится к технике, используемой оперативными сотрудниками и аналитиками при выполнении своих обязанностей. Методы оперативной работы включают создание сети тайных агентов, противодействие обнаружению агентами контрразведки, поддержание секретных каналов связи, а также вербовку и работу с тайными агентами, но не ограничиваются этим. Методы работы аналитиков включают элементы методологии социальных наук, компьютерные аналитические инструменты, командную работу с использованием новых информационных технологий и др.

Основные дисциплины сбора разведданных

Человеческие источники информации – самая старая форма сбора разведданных, и до технической революции XX века они были основным средством разведывательной работы.

В официальной публикации американского разведывательного сообщества «Национальная разведка США. Обзор за 2013 год» подчеркивается, что HUMINT (разведка по людям) – это единственный источник разведданных, где лица, собирающие разведданные, напрямую общаются с людьми, контролируют тему обсуждения и руководят их действиями, что благодаря человеческому интеллекту можно получить доступ к информации, которую невозможно получить другим способом [2].

Термин «геопространственная разведка» определен в Кодексе США как использование и анализ изображений и геопространственной информации для описания, оценки и визуального изображения физических особенностей и деятельности с географической привязкой. Геопространственная разведка (GEOINT) состоит из снимков, разведывательной информации и геопространственной информации [8]. Изображение означает совокупность полученных от различных типов датчиков отображений объектов, воспроизведенных электронным или оптическим способом на пленке, электронных устройствах отображения или других носителях. Корреляция изображений представляет собой взаимную связь между различными с точки зрения положения и физических характеристик изображениями. Изображения чаще всего получают с воздуха с помощью спутников, беспилотных летательных аппаратов и самолетов-разведчиков, и они не включают фотографии, сделанные человеческими источниками (HUMINT). Геопространственная разведка характеризуется более широким понятием, определяющим географическое расположение природных или рукотворно созданных объектов и границ на земле, и включает статистические данные и информацию, полученную с помощью технологий дистанционного зондирования, картографирования и съемки, а также картографирование, составление карт, геодезические данные и соответствующие продукты [9]. Для ввода, сбора, обработки и визуализации географических данных GEOINT использует географическую информационную систему (ГИС). Следует подчеркнуть, что геопространственная информация – это также геолокация объектов или людей. Например, американские спецслужбы использовали геолокацию пользователей социальных сетей для составления карты беженцев, покидающих Сирию [4]. Термин «разведка изображений» (IMINT) использовался в прошлом и до сих пор используется как взаимозаменяемый с GEOINT для описания разведывательных функций геопространственных источников. Однако, по мнению многих экспертов, данный термин устарел и не отражает того, чем сегодня является GEOINT [10]. В настоящее время IMINT является частью GEOINT в области получения изображений с использованием визуальной фотографии, радиолокационных и инфракрасных датчиков, лазеров и электрооптики [1]. Таким образом, Imagery Intelligence – это техническая, географическая и разведывательная информация, полученная в результате интерпретации или анализа изображений и дополнительных материалов.

Полная полезность GEOINT достигается взаимодействием трех элементов: изображений, разведки изображений (IMINT) и геопространственных данных, что позволяет получить комплексную перспективу и глубже понять оперативную обстановку. Геопространственные источники включают задачи, действия и события, используемые для сбора, управления, анализа, генерации, визуализации и доставки изображений, источников изображений (IMINT) и геопространственной информации, необходимой для поддержки принятия решения.

Радиоэлектронная разведка – это сбор информации с помощью средств связи, радаров и измерительных приборов. Традиционно она делится на две категории: коммуникационная разведка (COMINT) и радиотехническая разведка (ELINT).

Коммуникационная разведка (COMINT) – это разведданные, полученные из электромагнитных коммуникаций и систем связи другими получателями или пользователями, то есть результат перехвата коммуникаций между людьми, включая телефонные звонки, обмен мгновенными сообщениями, электронную почту и др. [11]. Также важен анализ трафика (геопространственных метаданных), который включает идентификацию вызывающих сторон и определение их подробного местоположения, используемых устройств и методов, технических параметров передатчиков, способа общения, частоты звонков и др.

Разведка измерений и сигнатур (MASINT) – это разведданные, полученные путем количественного и качественного анализа физических атрибутов целей и событий для характеристики и идентификации этих целей и событий. Согласно словарю НАТО, MASINT – «научно-техническая разведка с целью выявления отличительных особенностей источника, излучателя или отправителя для облегчения их измерения и идентификации в результате анализа данных, полученных от приборов зондирования».

Разведка измерений и сигнатур также является источником технической разведки. Примерами MASINT могут быть отличительные радиолокационные сигнатуры конкретных авиационных систем или химический состав проб воздуха и воды.

Разведка по открытым источникам информации (OSINT) – важный элемент в процессе сбора информации хотя информация собирается из несекретных источников.

Согласно Sands [12], OSINT можно разделить на четыре основные категории:

- широкодоступные данные и информация;
- целевые коммерческие данные;
- мнение отдельных публичных экспертов;
- «серая литература», доступ к которой возможен только для определенной аудитории [12, p. 64].

Информация может быть собрана из следующих источников:

- средства массовой информации;
- публичные данные (правительственные отчеты, официальные данные о бюджетах и демографии, слушания, законодательные дебаты, пресс-конференции и выступления и др.);
- «серая литература» (материалы научных, политических, социально-экономических и военных дисциплин, исследовательские и технические отчеты, неофициальные правительственные и рабочие документы, препринты, исследования, диссертации и др.);
- наблюдения и отчетность: значимая информация, которую предоставляют наблюдающие за самолетами (плейнспоттеры), радиолюбители, наблюдатели за спутниками и судами.

Информация из открытых источников также может включать информацию, которая считается собственностью компании, финансово чувствительную, охраняемую законом информацию или наносящую вред личности при ее обнародовании [13]. Все больше информации разведка получает из открытых источников и социальных сетей. Американские спецслужбы использовали такую информацию во время «арабской весны» в Египте (2011) и после теракта на Бостонском марафоне (2013) [4].

Как подчеркивает М. Минкина [2], признавая важность OSINT, разведывательные учреждения выделяют все больше ресурсов на применение специализированных информационных технологий, таких как большие данные и машинное обучение, с целью их использования в своих целях. По различным оценкам, OSINT составляет около 80 % всей информации, доступной аналитикам разведывательных структур, и около 95 % экономически значимой информации.

В завершение описания разведки по открытым источникам следует отметить, что в некоторых публикациях OSINT отрицается как отдельная дисциплина сбора разведданных [14]. Однако А. Халник, например, подчеркивает, что «OSINT – это действительно разведка. В разведывательной работе используются различные источники, поскольку информация из нескольких источников имеет гораздо бóльшую ценность» [15, p. 234]. Примером использования такой разведки стала совместная операция спецслужб США и Израиля «Олимпийские игры», целью которой была задержка ядерной программы Ирана. Хотя для основной атаки были использованы кибернетические средства (вредоносное программное обеспечение Stuxnet), очевидно, что в операции также использовались различные источники разведданных. Вероятно, GEOINT, SIGINT и MASINT были задействованы для получения информации об инфраструктуре центра в Натанзе, где иранцы использовали центрифуги в процессе обогащения урана [16].

Сбор информации является ключевым элементом процесса разведывательного цикла и основой для эффективного функционирования разведки. Агентства, ведомства и частные разведывательные компании, входящие в состав разведывательного сообщества, получают информацию из широкого спектра источников. Классический перечень дисциплин сбора разведданных включает технические средства (GEOINT, SIGINT и MASINT), тайные источники (HUMINT) и материалы из открытых источников (OSINT).

Методы разведки по открытым источникам

На практике OSINT заключается в процессе постановки задачи и планирования, сбора, систематизации и анализа информации из открытых источников, выработки выводов и создании отчета.

Определимся с основными терминами.

Данные из открытых источников (Open-Source Data, OSD) – необработанные данные, доступ к которым имеет любой неавторизованный пользователь. Примеры таких данных включают видеозаписи без следов монтажа, изображения и графики, данные соцопросов и открытой статистики, аудиоданные и метаданные из общедоступной информации.

Информация из открытых источников (Open-Source Information, OSINF) – информация, которая была отфильтрована на основе повторных критериев поиска из OSD (книги, статьи, заметки, документы на определенные темы). Такие данные перед анализом подвергаются систематизации.

Валидированный OSINT (Validated OSINT, OSINT-V) – информация высокой степени достоверности; ее может подготовить только специалист по разведке с персональной ответственностью. Может быть получена из достоверного гарантированно открытого источника (пример, изображение самолета, прибывающего в аэропорт, которое транслируется в средствах массовой информации) [17].

Найти эффективные способы поиска и использования огромного количества нужной информации – основная задача OSINT. Для ее решения применяются структурированный, последовательный и систематический поиск [18]. Для эффективного сбора данных в Интернете необходимо определить веб-ресурсы, в том числе относящиеся к так называемому «глубинному веб» (Deep Web). Ключевую роль здесь играет организация и актуализация списка необходимых веб-ресурсов. Их URL получают из библиотечного поиска, ссылок в соответствующих книгах и статьях, отчетов экспертов и интервью. Данные OSINT собираются путем создания отдельных списков полезных веб-ресурсов или онлайн-информации и управления ими [18; 19]. Каждое разведсообщество имеет свои

требования к данным OSINT. В целом процесс работы с данными OSINT состоит из следующих этапов.

Этап 1. Определение источника. Необходимо среди множества данных установить информацию для конечного пользователя или успешного выполнения миссии, определить, где и как получить эту информацию.

Этап 2. Сбор данных. Получение связанных данных путем идентификации источника. Классифицируется на два типа – активный или пассивный в зависимости от метода сбора данных. На этапе активного сбора информация собирается непосредственно с помощью программы или скрипта на объекте. Активный тип имеет характерную особенность: после него остаются журналы, поскольку он напрямую обращается к цели. На этапе пассивного сбора информация собирается с помощью Google, Netcraft, Whois, Recon-NG, Shodan. Его особенность в том, что не остается отдельного журнала фиксации действий, поскольку информация собирается с помощью сторонних приложений.

Этап 3. Обработка и повторное изучение информации, полученной на предыдущем этапе. Поскольку на этапе 2 имеется большое количество информации, задача ее отбора является особенно важной. Кроме того, необходимо учитывать взаимосвязь между информацией, что требует выполнения задач высокой сложности, а это, в свою очередь, – большого опыта и видения перспективы нахождения взаимосвязи в предобработанных данных.

Этап 4. Анализ данных в соответствии с целью разведывательных действий. Например, имеются доказательные данные A, B и C, полученные путем сбора и обработки разнообразной информации для поддержки гипотезы. Гипотеза считается подтвержденной, если доказано, что данные A, B и C верны. Если на этапе анализа требуется дополнительная информация, этапы сбора и обработки данных повторяются для получения новой информации.

Этап 5. Отчетность. Обобщение результатов до этапа 4 включительно и их оформление в виде доказательного и аналитического отчета в зависимости от организации (разведсообщества), которая их использует. Они включают все исходные данные, которые подтверждают точность и достоверность данных для аргументации и доказательства. В результате большая часть общих данных перерабатывается в данные, которые соответствуют критериям, установленным разведсообществом, что обеспечивает получение верных выводов об интересующем объекте или событии [18; 20; 21].

OSINT имеет свои преимущества и недостатки [22; 23].

Преимущества использования OSINT

1. Сбор информации приближен к реальному времени. Информация может быть получена через открытые источники с опорой на различные OSINF. Быстрый доступ к данным.

2. Легитимное получение большого количества данных. Сбор данных дополняется с помощью других дисциплин. Например, при применении HUMINT полученных данных, как правило, не хватает, однако преимущество OSINT состоит в том, что много данных можно получить из открытых источников. Значимые данные могут быть получены, если значительное количество данных будет обработано и проанализировано с помощью OSINT. Кроме того, поскольку OSINT доступен любому человеку, имеется преимущество низкого риска с точки зрения вопросов безопасности и законности.

3. Ясность источников. В HUMINT достоверность данных сомнительна, поскольку источник информации, которую получает исследователь, не всегда ясен, и требуется трудоемкое и иногда сопряженное с риском независимое подтверждение от альтернативного

источника. Данные, собранные OSINT, обеспечивают надежность, поскольку ясность открытых источников гарантируется процессом проверки.

4. Удобство и простота доступа. К некоторым важным и высококачественным данным могут получить доступ только авторизованные пользователи. К информации, собранной OSINT, может легко получить доступ любой человек и использовать ее в соответствии с требованиями разведсообщества.

5. Низкая стоимость. Преимуществом OSINT является получение данных по низкой цене по сравнению со стоимостью обучения агентов и стимулирования источников при применении HUMINT или со стоимостью сбора данных с использованием новейшего оборудования (спутники и беспилотные летательные аппараты (БПЛА) в TECHINT).

Недостатки использования OSINT

1. Слишком большой объем информации. Чем больше информации у исследователя, тем сложнее определить достоверность данных с помощью OSINT. Если среди доказательных данных имеется нескольких факторов, поддерживающих гипотезу, это может снизить их достоверность и привести к появлению ложной информации. Поскольку в настоящее время многие данные можно найти в открытых источниках, требуется время и дополнительные усилия для выявления ложной информации и отбора надежных данных.

2. Организационное восприятие и предрассудки разведсообщества в отношении OSINT. В организационной культуре разведывательных агентств ценность данных, собранных OSINT, недооценивается, а важность данных иногда не учитывается, поскольку любой может получить к ним доступ и использовать их.

3. Вопросы безопасности и технические ограничения при использовании OSINT с помощью Интернета. В результате аналитики разведывательные агентства проявляют пассивное отношение к использованию данных OSINT. Эксперты по компьютерной безопасности стремятся применять методы свободного использования OSD при решении проблем кибербезопасности.

4. Данные, собранные OSINT, могут стать основой для совершения киберпреступлений, поэтому необходимо соблюдение требований и мер безопасности и применение технологий, которые помогут минимизировать ущерб от киберпреступлений, даже если исследователи используют данные OSINT в злонамеренных целях.

Важность OSINT для кибербезопасности

Что касается кибербезопасности, то вопрос использования данных, собранных OSINT, можно рассматривать в двух аспектах. С одной стороны, методы OSINT, стоящие на вооружении у злоумышленников, существенно повышают вероятность успешности атак; с другой – в применении данных методов есть плюсы для построения эффективной системы защиты [23]. Так, если данные собранные с помощью OSINT, будут использоваться в положительном аспекте, то можно получить значительный объем дополнительной информации о тенденциях в области уязвимостей и расстановки сил в хакерских группировках [24; 25]. Кроме того, если данные, собранные OSINT, правильно использовать в аспекте информационной безопасности, можно заранее предотвратить киберпреступления, такие как кибертерроризм. В настоящее время постоянно проводятся исследования по реагированию на кибератаки с использованием OSINT [26] Согласно отчету Министерства внутренней безопасности США использование данных, собранных OSINT, включает общую разведку, заблаговременное предупреждение, борьбу с терроризмом внутри страны, защиту важных критических инфраструктур (включая киберпространство), защиту от кибертерроризма

и предотвращение чрезвычайных ситуаций в области важных миссий [27]. Поэтому управление данными, собранными с помощью OSINT, имеет решающее значение для кибербезопасности. Кроме того, для национальной безопасности было бы важно собирать и анализировать значительное количество данных из различных источников, включая записи о террористических инцидентах и угрозах кибербезопасности, получать из них ценные данные с помощью OSINT [28]. В Таблице 2 представлены методы OSINT, применяемые в решении задач кибербезопасности.

Таблица 2

Методы OSINT для решения задач кибербезопасности

Метод	Область действия метода	Описание метода
Data Mining (добыча данных)	Отслеживание хакерских сообществ	Предлагается структура, состоящая из трех модулей: 1) анализатор кликов, 2) анализатор тем, 3) визуализатор информации. Это унифицированная структура методов добычи данных и обработки естественного языка для сбора данных из журналов чатов для получения интуитивно понятных и интерпретируемых доказательств, которые облегчают процесс расследования преступлений [29]. Источник открытых данных: форумы; даркнет
	Детекция аномального роста активности	Формирование типичного сценария нечеткого обнаружения вторжения с помощью приложения по добыче данных в реальном времени, которые используются для исследования уязвимостей компьютерных сетей [30]. Источник открытых данных: данные интернет-провайдеров
	Обнаружение активностей вредоносного ПО Fast-Flux сетей (FFSN), обнаружение DGA-доменов	Исследование ресурсов по обнаружению Fast-Flux доменов с помощью методов Data Mining (линейная регрессия) для обнаружения FFSN и анализа признаков активностей вредоносных ПО [31]. Для обнаружения вредоносных доменов, сгенерированных с помощью DGA, в последнее время применяют алгоритмы машинного обучения, которые используют общедоступные базы данных и результаты работы DGA в своем обучении [32]. Источник открытых данных: веб-ресурсы белых и черных списков доменов, например, Alexa Top Sites; алгоритмы генерации доменов
	Противодействие кибертерроризму	Обеспечение вспомогательных данных с помощью факторного концептуального анализа для выявления и устранения информационных пробелов в веб-поиске и веб-разведке в целях противодействия кибертерроризму [33]. Источник открытых данных: малые наборы данных по инцидентам кибертерроризма
Интеллектуальный анализ текстов (майнинг текстов)	Противодействие кибертерроризму	Используя UIR-методы (интеллектуальный анализ текста, который фокусируется на обнаружении возможных связей между понятиями в нескольких текстовых документах путем создания следов доказательств, объясняющих связь), возможно разработать схему интерпретации важной для принятия решения информации. Применяя данный метод, важно выбрать термины для запроса на анализ данных [34]. Источник открытых данных: обвинительные заключения доктрины государств, совершающих враждебные действия в киберпространстве

Продолжение таблицы 2

	Обнаружение сетей кибер-террористов, террористов, совершающих атаки на критическую информацион-ную инфраструктуру	Алгоритм на основе графов, который генерирует связи для выявления скрытых узлов в сети с текущей информацией, доступной исследователю. Предлагается новый метод анализа важности связей и выявления ключевых субъектов в террористических (тайных) сетях с использованием программы класса Crime Fighter Assistant или другие методы анализатора связей социальных сетей и сообществ [35]. Источник открытых данных: открытая информация по совершенным терактам и составу террористических групп
Анализ соцсетей	Обнаружение сетевых атак	Использование автоматических семантических сетей с двумя слоями. Первая сеть идентифицирует релевантные атаки на основе признаков сходства, вторая модифицируется на основе первой и корректируется путем добавления опыта в данной области анализа [36; 37]. Источник открытых данных: например, доступные из набора данных KDD Cup 1999 года
	Предотвращение DDoS-атак	Модель представляет собой одномоментную некооперативную игру с нулевой суммой, в которой целью атакующего является поиск оптимальных параметров конфигурации для атаки, чтобы вызвать максимальное нарушение обслуживания с минимальными затратами. Эта модель пытается исследовать взаимодействие между атакующим и защищающимся во время сценария DDoS-атаки [38]. Источник открытых данных: серия экспериментов на основе сетевого симулятора (ns-2) с использованием топологии гантелеобразной сети
Методы оптимизации	Управление доверием и DoS-атаки	Предлагается метод защиты с использованием двух систем управления доверием (Key Note и Trust Builder), а также кэширования учетных данных. В предложенной модели игры с нулевой суммой двух игроков, атакующий пытается лишить защищающегося как можно большего количества ресурсов, а защитник пытается идентифицировать атакующего как можно быстрее [39]. Источник открытых данных: KeyNote (библиотека с открытым исходным кодом для системы управления доверием KeyNote) в качестве примера, демонстрирующего, что DoS-атака может легко парализовать сервер доверительного управления
	Компьютерный взлом	Концептуальная аналитическая схема, основанная на факторах и мотивах, которые побуждают и стимулируют поведение киберпреступников [40]. Источник открытых данных: общедоступные описания особенностей наций тех или иных киберпреступников; описание мотивов в зависимости от типов атак по их источникам и конечным целям; общедоступные базы данных известных угроз и уязвимостей; бюллетени безопасности производителей

Окончание таблицы 2

	Предотвращение преступлений «белых воротничков»	Разработка систем управления знаниями в сфере борьбы с финансовыми преступлениями, содержащей данные для этапов расследования и предотвращения финансовых преступлений [41]. Источник открытых данных: публикации на тему финансовых преступлений
Концептуальные методы	Обнаружение киберпреступлений в финансовом секторе	Многоуровневый подход, направленный на визуализацию взаимодействия как взаимозависимых, так и дифференцированных факторов с акцентом на теорию системной динамики в финансовом секторе. Факторы в совокупности могут способствовать или препятствовать киберпреступности, одновременно увеличивая и/или уменьшая ее экономические и социальные издержки [42]. Источник открытых данных: публикации на тему финансового анализа; новости финансовой сферы; публикации социально-экономических показателей
	Сбор и анализ информации о военно-политической обстановке для предотвращения кризисов в киберпространстве	Механизм раннего предупреждения на основе анализа информации о военно-политической обстановки с четырьмя модулями: модулем сбора; модулем предобработки; модулем анализа; модулем выработки превентивных действий [43]. Для содействия сбору, отслеживанию, мониторингу, анализу и выработке сигналов о вероятном кризисе в киберпространстве разрабатываются специальные информационно-аналитические системы. Источник открытых данных: новостные каналы социальных сетей и мессенджеров; СМИ; личные аккаунты государственных деятелей и лидеров общественного мнения; онлайн-системы государственных закупок; интернет-ресурсы государственных ведомств; интернет-ресурсы логистических, транспортных компаний; интернет-ресурсы НИИ и оборонных предприятий; общедоступные системы геопространственных данных; общедоступные системы отслеживания перелетов и движения морских судов; публикации геополитической и военно-политической направленности

Заключение

Вооруженные конфликты последних лет подтверждают значительный рост важности применения разведки по открытым источникам. Киберпространство уже давно стало полем сражения между преступными сообществами – как независимыми, так и поддерживаемыми государственными структурами, между целыми странами и военно-политическими альянсами. Экспоненциальный рост общедоступных ресурсов, агрегирующих различные данные, существенно повышает эффективность методов OSINT. Доступность вычислительных мощностей и систем хранения, наряду с развитием методов машинного обучения, выводит данные методы на качественно новый уровень. Это позволяет начать их широкое применение для решения задач кибербезопасности, таких как обогащение данных различных аналитических систем, систем предотвращения вторжений, анализ уязвимостей и др.

Литература / References

1. *U.S. National Intelligence: An overview 2013*. Intelligence Community Information Sharing Executive, 2013. 103 p. URL: https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf (accessed 20.03.2023).
2. Minkina M. (2014) *Sztuka wywiadu w państwie współczesnym*. Warszawa : Bellona.
3. We are the Intelligence Community. *Intelligence.gov.* URL: http://www.intelligence.gov (accessed 20.02.2023).
4. Lowenthal M.M. (2022) *Intelligence: From secrets to policy*. Intelligence & Security Academy, LLC. 624 p.
5. Goldman J. (2011) *Words of intelligence: An intelligence professional's lexicon for domestic and foreign threats*. 2nd edition. Scarecrow Press. 310 p.
6. Evangelista J.R.G., Sassi R.J., Romero M., Napolitano D. (2021) Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*. Vol. 16. No. 3. Pp. 345–369. DOI: 10.1080/19361610.2020.1761737
7. Wirtz J.J. (2010) The Sources and Methods of Intelligence Studies. In: *The Oxford Handbook of National Security Intelligence*. Ed. by L.K. Johnson. Oxford University Press. Pp. 59–69. DOI: 10.1093/oxfordhb/9780195375886.003.0004
8. *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*: Report to the President of the United States, 2005. 366 p. URL: http://fas.org/irp/offdocs/wmd_report.pdf (accessed: 20.03.2023).
9. *United States Code*, Title 10, §467. URL: http://uscode.house.gov (accessed: 20.03.2023).
10. Jensen III C.J., McElreath D.H., Graves M. (2022) *Introduction to intelligence studies*. Taylor & Francis. DOI: 10.4324/9781003149569
11. *NATO Glossary of Terms and Definitions (AAP-6)*. North Atlantic Treaty Organisation, NATO Standardization Agency 2010. 451 p. URL: https://www.cimic-coe.org/resources/external-publications/app-6-c.pdf (accessed 20.03.2023).
12. Sands A. (2005) Integrating open sources into transnational threat assessments. In: Jennifer E.S., Gerber B. *Transforming US Intelligence*. Washington, DC : Georgetown University Press. Pp. 63–78.
13. Best J.R.A., Cumming A. (2007) *Open source intelligence (OSINT): Issues for Congress.* December 5. Congressional Research Service. URL: https://sgp.fas.org/crs/intel/RL34270.pdf (accessed 20.03.2023).
14. Bean H. (2007) The DNI's Open Source Center: An Organizational Communication Perspective. *International Journal of Intelligence and Counter Intelligence*. No. 20 (2). Pp. 240–257. DOI: 10.1080/08850600600889100
15. Hulnick A.S. (2010) *The dilemma of open sources intelligence: Is OSINT really intelligence?* In: *The Oxford Handbook of National Security Intelligence*. Ed. by L.K. Johnson. Oxford University Press. Pp. 229–241. DOI: 10.1093/oxfordhb/9780195375886.003.0014
16. Harris S. (2014) *War: The rise of the military-internet complex*. Boston : Houghton Mifflin Harcourt. 263 p.
17. *NATO Open Source Intelligence Handbook*. November 2001. URL: https://bib.opensourceintelligence.biz/STORAGE/2001.%20OPEN%20SOURCE%20INTELLIGENCE%20HANDBOOK.pdf (accessed 20.03.2023).
18. Lee W.H., Yun M.W., Park J.S. (2013) Intelligence in the Internet Era: Understanding OSINT and Case Analysis. *Korean Security Journal*. No. 34. Pp. 259–278.

19. Chauhan S., Panda N.K. (2015) Open source intelligence and advanced social media search. *Hacking Web Intelligence Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Waltham, MA : Elsevier, Inc. Pp. 15–32. DOI: 10.1016/b978-0-12-801867-5.00002-1
20. Danda M. (2019) Open source intelligence and cybersecurity. Unpublished Master's Thesis. Webster University, Webster Groves, MO, USA.
21. Kanta A., Coisel I., Scanlon M. (2020) A survey exploring Open Source Intelligence for smarter password cracking. *Forensic Science International: Digital Investigation*. Vol. 35. Article no. 301075. DOI: 10.1016/j.fsidi.2020.301075
22. Yong-Woon Hwang, Im-Yeong Lee, Hwankuk Kim, Hyejung Lee, Donghyun Kim (2022) Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*. Vol. 2022, Article no. 1290129. DOI: 10.1155/2022/1290129
23. Dokman T., Ivanjko T. (2020) Open source intelligence (OSINT) issues and trends. In: *The Future of Information Sciences: 7th International Conference INFuture2019: Knowledge in the Digital Age*. DOI: 10.17234/infuture.2019.23
24. Lee W.H., Yun M.W., Park J.S. (2013) Intelligence in the internet Era: Understanding OSINT and case analysis. *Korean Security Journal.* No. 34. Pp. 259–278.
25. Shin Kyuyong, Yoo Jincheol, Han Changhee, Kim Kyoung Min, Kang Sungrok, Moon Minam, Lee Jongkwan (2019). A study on building a cyber attack database using Open Source Intelligence (OSINT). *Journal of Information and Security*. Vol. 19. No. 2. Pp. 113–121. DOI: 10.33778/kcsa.2019.19.2.113
26. Wells D. (2016) Taking Stock of Subjective Narratives Surrounding Modern OSINT. In: Akhgar B., Bayerl P., Sampson F. (Eds) *Open Source Intelligence Investigation*. Advanced Sciences and Technologies for Security Applications. Springer, Cham. Pp. 57–65. DOI: 10.1007/978-3-319-47671-1_5
27. Tabatabaei F., Wells D. (2016) OSINT in the Context of Cyber-Security In: Akhgar B., Bayerl P., Sampson F. (Eds) *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications.* Springer, Cham. Pp. 213–231. DOI: 10.1007/978-3-319-47671-1_14
28. Chen H., Chiang R.H.L., Storey V.C. (2012) Business intelligence and analytics: From big data to big impact. MIS quarterly. Vol. 36. No. 4. Pp. 1165–1188. DOI: 10.2307/41703503
29. Iqbal F., Fung B.C.M., Debbabi M. (2012) Mining criminal networks from chat log. *2012 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology.* IEEE, Macau, China, 2012. Vol. 1. Pp. 332–337. DOI: 10.1109/wi-iat.2012.68
30. Ansari A.Q., Patki T., Patki A.B., Kumar V. (2007) Integrating fuzzy logic and data mining: Impact on cyber security. *Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007).* Haikou, China. IEEE. Vol. 4. Pp. 498–502. DOI: 10.1109/fskd.2007.365
31. Wu Jiayan, Zhang Liwei, Liang Jian, Qu Sheng, Ni Zhiqiang (2010). A comparative study for fast-flux service networks detection. *The 6th International Conference on Networked Computing and Advanced Information Management*. Seoul, IEEE. Pp. 346–350. URL: https://ieeexplore.ieee.org/document/5572048?arnumber=5572048 (accessed 20.03.2023).
32. Berman D.S., Buczak A.L., Chavis J.S., Corbett C.L. (2019) A survey of deep learning methods for cyber security. *Information.* Vol. 10. No. 4. Pp. 122. DOI: 10.3390/info10040122
33. Koester B., Schmidt S.E. (2009) Information superiority via formal concept analysis. In: Argamon S., Howard N. (Eds) *Computational Methods for Counterterrorism.* Springer, Berlin, Heidelberg. Pp. 143–171. DOI: 10.1007/978-3-642-01141-2_9
34. Srihari R.K. (2009) Unapparent information revelation: Text mining for counterterrorism. In: Argamon S., Howard N. (Eds) *Computational methods for counterterrorism.* Springer, Berlin, Heidelberg. Pp. 67–87. DOI: 10.1007/978-3-642-01141-2_5

35. Chen A., Gao S., Karampelas P., Alhajj R., Rokne J. (2011). Finding Hidden Links in Terrorist Networks by Checking Indirect Links of Different Sub-Networks. In: Wiil U.K. (Ed) *Counterterrorism and Open Source Intelligence*. Series: Lecture Notes in Social Networks. Springer Vienna. Pp. 143–158. DOI: 10.1007/978-3-7091-0388-3_8
36. Wiil U.K., Gniadek J., Memon N. (2011). Retraction Note to: A Novel Method to Analyze the Importance of Links in Terrorist Networks. In: Wiil U.K. (Ed) *Counterterrorism and Open Source Intelligence*. Series: Lecture Notes in Social Networks. DOI: 10.1007/978-3-7091-0388-3_22
37. He P., Karabatis G. (2012) Using semantic networks to counter cyber threats. *2012 IEEE International Conference on Intelligence and Security Informatics.* IEEE. Pp. 184–184. DOI: 10.1109/ISI.2012.6284294
38. Spyridopoulos T., Karanikas G., Tryfonas T., Oikonomou G. (2013). A game theoretic defence framework against DoS/DDoS cyber attacks. *Computers & Security.* Vol. 38. Pp. 39–50. DOI: 10.1016/j.cose.2013.03.014
39. Li B., Batten L. (2009) Using mobile agents to recover from node and database compromise in path-based DoS attacks in wireless sensor networks. *Journal of Network and Computer Applications.* Vol. 32. No. 2. Pp. 377–387. DOI: 10.1016/j.jnca.2008.02.017
40. Kshetri N. (2005) Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management.* Vol. 11. No. 4. Pp. 541–562. DOI: 10.1016/j.intman.2005.09.009
41. Gottschalk P., Filstad C., Glomseth R., Solli-Sæther H. (2011) Information management for investigation and prevention of white-collar crime. *International journal of information management.* Vol. 31. No. 3. Pp. 226–233. DOI: 10.1016/j.ijinfomgt.2010.07.002
42. Lagazio M., Sherif N., Cushman M. (2014) A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security.* Vol. 45. Pp. 58–74. DOI: 10.1016/j.cose.2014.05.006
43. Song J. (2011) The analysis of military intelligence early warning based on open source intelligence. *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics.* IEEE. Pp. 226–226. DOI: 10.1109/isi.2011.5984775