Обзор искусственного интеллекта (2023 г.) 56: 12407–12438
https://doi.org/10.1007/s10462-023-10454-y

Аналитика с открытым исходным кодом: всесторонний обзор текущего состояния, приложений и будущих перспектив в области кибербезопасности

Ашок Ядав[1] · Атул Кумар[2] · Вриджендра Сингх[1]

Опубликовано онлайн: 15 марта 2023 г.

Абстрактный

Объем данных, генерируемых сегодняшним миром, подключенным к цифровым технологиям, огромен, и значительная их часть общедоступна. Этими источниками данных являются веб-архивы, общедоступные базы данных и социальные сети, такие как Facebook, Twitter, LinkedIn, электронная почта, Telegram и т. д. Разведка с открытым исходным кодом (OSINT) извлекает информацию из коллекции общедоступных и доступных данных. OSINT может обеспечить решение проблем по извлечению и сбору разведданных из различной общедоступной информации и социальных сетей. OSINT в настоящее время расширяется невероятными темпами, предлагая новые подходы на основе искусственного интеллекта для решения проблем национальной безопасности, политических кампаний, кибериндустрии, криминального профилирования и общества, а также киберугроз и преступлений. В этой статье мы описали текущее состояние инструментов/методов OSINT, а также современное состояние различных приложений OSINT в кибербезопасности. Кроме того, мы обсудили проблемы и будущие направления разработки автономных моделей. Эти модели могут обеспечить решения различных проблем, связанных с безопасностью социальных сетей, цифровой криминалистикой и киберпреступностью, с использованием различных машинного обучения (ML), глубокого обучения (DL) и искусственного интеллекта (ИИ) с OSINT.

Ключевые словаИскусственный интеллект · Интеллект с открытым исходным кодом · Кибербезопасность · Публичные данные · Социальные сети · Глубокое обучение

* Ашок Ядав
ashok.smsit@gmail.com

Атул Кумар
atul.kumar@dsci.in

Вриджендра Сингх
vrij@iiita.ac.in

[1] Департамент информационных технологий, Индийский институт информационных технологий, Аллахабад, Праяграддж, Уттар-Прадеш 211015, Индия

[2] Совет по безопасности данных Индии, Нью-Дели 110025, Индия

1. Введение

Открытые источники существуют уже много лет, но бурный рост Интернета и Всемирной паутины (WWW) побуждает некоторых специалистов и исследователей в области кибербезопасности публиковать журналы и статьи о киберугрозах, профилировании киберпреступников и сборе информации (Амаро и др.). .2018 год). Текущее состояние анализа искусственного интеллекта (ИИ)/машинного обучения (МО) в контексте открытого исходного кода является сложным. Чтобы эффективно использовать общедоступные неструктурированные данные в расследовании киберпреступлений, исследователи разрабатывают методы их выявления, сбора и организации. Термин «ОС» OSINT означает «Открытый исходный код»; оно относится к общедоступному источнику, из которого пользователь получает информацию для своих разведывательных целей. Термин «Информация» является важнейшим компонентом OSINT, который представляет собой свободно доступную информацию. Вам не нужно быть хакером, чтобы использовать OSINT в повседневной жизни. Возможно, вы уже использовали OSINT, но не осознавали этого. Все интернет-пользователи так или иначе используют тактику OSINT, например, при онлайн-поиске фирмы, школы, университета или отдельного человека. Не имеет значения, где хранится информация и получена ли она из социальных сетей, фотографий, видео, блогов, газет или твитов, главное, чтобы она была общедоступной, доступной и законной. С помощью надлежащих знаний, полученных с помощью OSINT, мы можем добиться значительных конкурентных преимуществ, таких как профилирование преступников, отслеживание сотрудников компаний и отслеживание организованной преступности. Доступность информации и методы ее сбора постоянно меняются со временем.

Раньше open-source фокусировался на светских мероприятиях, открытых выступлениях и интервью. Однако сегодня информация находится в сети, и методы ее поиска становятся все более сложными, инновационными и открытыми для всех. Полезную информацию можно собирать из общедоступных и несекретных источников благодаря распространению социальных сетей и доступному сегодня обмену информацией в режиме реального времени. Значение OSINT ускорило спор о том, как следует собирать разведывательные данные из нескольких источников между военными, правительством и коммерческим сектором. Некоторые проблемы включают сбор, использование и распространение соответствующих данных для удовлетворения конкретных требований разведки (Nouh et al.2019 год).

В последние годы несколько журналов опубликовали работы о киберпреступности, уязвимостях кибербезопасности и потенциальных угрозах, которые представляют собой отдельные лица, предприятия и страны. Данные из открытых источников создали проблемы в приобретении и поддержании необходимых навыков для использования разнородной информации и доступных электронных средств массовой информации. В открытом доступе имеется несколько инструментов и методов, которые могут помочь следователям расследовать киберугрозы с использованием OSINT (Revell et al.2016 год). Различные характеристики киберпреступников можно легко собрать с помощью инструментов и методов OSINT. Эти характеристики киберпреступников помогают составить профиль преступников (Эдвардс и др.2022 год). OSINT становится все более важной дисциплиной в современных уголовных расследованиях как метод разрешения нескольких типов дел. Правоохранительные органы и следственные органы полагаются в первую очередь на открытые данные для проверки информации, сбора доказательств и сбора информации для различных расследований, включая отмывание денег, обнаружение мошенничества, торговлю людьми и оружием и т. д.

Для облегчения принятия важных решений и мер безопасности, таких как анализ настроений и борьба с беспорядками, реагирование на стихийные бедствия, борьба с экстремизмом, меры по дезинформации, разведка угроз, реагирование на инциденты, мониторинг блокчейна и даркнета, обнаружение утечек данных и меры социальной инженерии и т. д. различные государственные органы, в том числе

военные организации и спецслужбы, полагаясь на огромные и современные открытые данные.

Оставшаяся часть статьи структурирована следующим образом. Необходимость проверки OSINT описана в разд.1.1. Где мы можем использовать OSINT, описано в разд.1.2. Самые последние приложения OSINT представлены в разделе.2. Мы рассмотрели рабочий процесс OSINT в разд.3. Подробное рассмотрение различных инструментов и методологий OSINT, а также предложения по выбору правильного варианта для конкретной задачи представлены в разд.4. Обсуждение статьи, в которой мы обсуждали нынешнюю практику, описано в разд.5бумаги. Работа завершается в разд.6, в котором рассматриваются проблемы и будущие направления исследований. Вклад статьи графически суммирован, как показано на рис.1.

1.1 Необходимость OSINT-проверки

Объем информации, доступной в Интернете, может быть полезен как частным лицам, так и предприятиям. Недостаток осведомленности и знаний может привести к потенциальному вреду из-за развития ложных представлений о недостоверной информации, что поднимает проблемы обеспечения информационной безопасности. Из-за доступа к Интернету и уязвимостей безопасности количество опубликованных исследований обычно быстро увеличивается до того, как они будут оценены. Некоторые исследования могут давать неясные, запутанные или противоречивые результаты или быть доступны на разных языках. Таким образом, на основе приведенной выше информации обнаружены следующие пробелы в исследованиях: отсутствие ясности для обобщения системной безопасности других стран, отсутствие решения проблем кибербезопасности и киберзащиты с использованием OSINT, отсутствие способов использования OSINT в надежных и автоматизированных моделях, отсутствие знаний о правильном выборе инструментов, методов и процессов в зависимости от наличия данных и целей. Автоматическая и самоходная модель расследования киберпреступлений и киберугроз в соответствии с требованиями. Поэтому необходим систематический обзор приложений OSINT с точки зрения кибербезопасности, который обеспечивает правильную и объективную информацию.

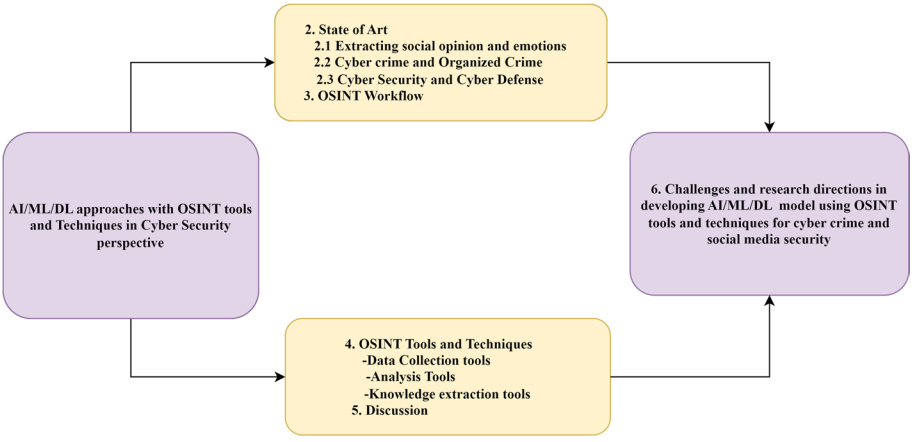

рисунок 1Графический обзор статьи

1.2 Где можно использовать разведку из открытых источников?

Этические хакеры, тестеры на проникновение и эксперты по безопасности выявляют потенциальные недостатки в системе, используя инструменты и методы с открытым исходным кодом. Обычно обнаруживаемые дефекты включают веб-жизнь, открытые порты или несвязанные веб-гаджеты, неисправленное программное обеспечение (например, веб-сайты, на которых используются старые настройки основных элементов CMS), утечку ресурсов или незащищенные непреднамеренные контейнеры для вставки всего кода для конфиденциальных данных, таких как ресурсы. . Некоторые из важных областей, где используется OSINT, — это правоохранительные органы (LEA), государственные органы, а также корпоративная и кибербезопасность.

1.2.1 ПОО

Мы наблюдаем сокращение HUMINT (человеческого интеллекта), например, инспекторы маршируют по улицам и стучатся в двери людей. Использование OSINT значительно возросло из-за того, что люди проводят большую часть своей жизни в Интернете. Это особенно полезно при расследовании уголовных преступлений, таких как торговля людьми и отмывание денег.

1.2.2 Государственные органы

Военные группы используют открытые данные для проведения эффективных расследований и контрразведки. Органы национальной безопасности используют методы OSINT для обнаружения групп угроз, таких как террористические ячейки, обеспечения эффективного реагирования на беспорядки и стихийные бедствия, анализа настроений, опровержения слухов и выполнения многих других гражданских обязанностей.

1.2.3 Корпоративная и кибербезопасность

Компании уделяют больше внимания информационной безопасности из-за значительных финансовых потерь, вызванных единственной атакой программы-вымогателя или компрометацией корпоративных данных. OSINT-фреймворки играют решающую роль в разведке угроз, включая тестирование на проникновение и реагирование на инциденты, но также могут использоваться для противодействия постоянным проблемам, таким как атаки на основе социальной инженерии или даже просто безответственные способы обработки данных. Хотя стратегии OSINT варьируются от случая к случаю, существуют фундаментальные методы получения ценной разведывательной информации на этапах сбора и обработки данных. OSINT помогает экспертам по безопасности бороться с киберугрозами, например определять, какие уязвимости можно эффективно использовать, блокировать угрозы неизбежных атак и т. д. Обычно в работе по кибер-расследованию следователям необходимо различать и связывать множество фокусных точек информации для выявления киберугроз. Например, один компрометирующий твит может не вызывать беспокойства, но если он связан с опасным кластером, который, как известно, динамичен в конкретной отрасли, связанный с ним твит может рассматриваться с подозрительной точки зрения. Одна из самых важных вещей, которые следует знать об OSINT, — это его использование в сочетании с другими подтипами разведки. Извлечение информации из закрытых источников, таких как внутренняя телеметрия, сети даркнета и общие внешние разведывательные сети, обычно используется для проверки и подтверждения OSINT. Различные применения OSINT показаны на рис.2.

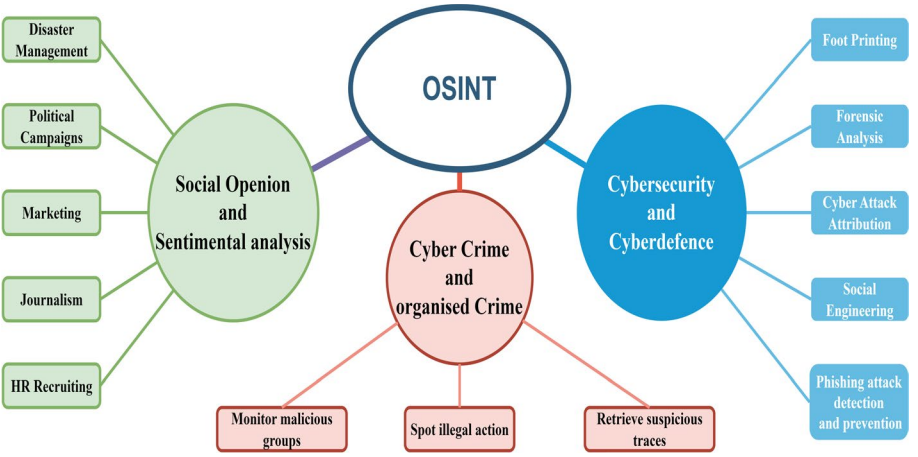

Рис. 2Приложения OSINT (Хера2021 год)

2 Современное состояние

В этой статье была предпринята попытка объединить результаты предыдущих исследований, связанных с инструментами и методами OSINT (разведка с открытым исходным кодом). Чтобы лучше понять и ускорить прогресс в исследованиях OSINT, мы сформулировали пять исследовательских вопросов (RQ), основанных на всестороннем обзоре инструментов, методов OSINT и их применения. Основная цель этих вопросов — улучшить наше понимание OSINT и его использования.

1. **RQ1**Каковы различные категории OSINT и как мы можем их использовать? В предыдущих исследованиях OSINT использовался только для целей перевода, использования, анализа и распространения, но с появлением технологий его можно использовать в различных приложениях. OSINT классифицируется в соответствии с такими приложениями, как геопространственный интеллект, сигнальный интеллект, визуальный интеллект, человеческий интеллект и интеллект социальных сетей. Подробная информация об этих категориях представлена в таблице.1.
2. **RQ2**Каковы основные сильные и слабые стороны различных инструментов и методов OSINT? Фактическая цель этого вопроса состояла в том, чтобы выявить сильные и слабые стороны различных инструментов и методов OSINT с точки зрения нескольких аспектов, таких как общедоступность, применение, время обработки, тип ввода и оценка надежности. Подробно инструменты и методы описаны в таблицах разд.4.
3. **запрос 3**Какие существуют эталонные исследовательские работы, которые интегрируют OSINT с различными областями, чтобы максимизировать использование OSINT? Этот вопрос в основном касался источников опубликованных исследовательских работ и того, насколько они связаны с OSINT, и эти работы регулярно цитируются и отдаются предпочтение в предыдущих исследованиях. Подробности описаны в разд.2.
4. **RQ4**Существует ли какой-либо механизм или рабочий процесс для использования OSINT для использования общедоступных данных? Опубликованы некоторые исследовательские работы, правительственные рекомендации и отчеты, в которых исследуется рабочий процесс OSINT. Этот рабочий процесс весьма полезен для использования инструментов и методов OSINT в соответствии с требованиями. Наша цель — изучить различные соответствующие рабочие процессы на основе их характеристик и приложений. Общий порядок работы показан на рис.5

5.**RQ5**Как мы можем использовать инструменты и методы OSINT для анализа социальных сетей, извлечения мнений, кибербезопасности, борьбы с терроризмом, киберзащиты, расследования киберпреступлений, составления криминальных профилей, наблюдения и т. д. Есть несколько очень хороших исследовательских статей, писем, журналов и блогов. доступны, которые исчерпывающе использовали инструменты и методы OSINT.
Это означает, что применение OSINT в различных областях весьма полезно и подходит для реальных сценариев (таких как отслеживание преступников, борьба с терроризмом, отслеживание кораблей/рейсов и наблюдение). Поэтому основная цель этого вопроса — определить структуру, которая интегрирует OSINT с машинным обучением/глубоким обучением/искусственным интеллектом, которая может дать лучшие результаты. Этот вопрос также фокусируется на результатах модели без OSINT, поэтому мы можем легко сравнить их, включив их в OSINT. Все вышеперечисленные пункты мы рассмотрели в Сектах.2и4.

2.1 Процесс исследования

Мы использовали различные ключевые слова для современного уровня техники, такие как OSINT, инструменты и методы OSINT, обнаружение киберпреступности и организованной преступности с использованием OSINT, борьба с киберпреступниками с использованием OSINT, разведка угроз с использованием OSINT, применение OSINT в киберзащите, разведка безопасности, управление стихийными бедствиями, извлечение общественного мнения, анализ настроений, анализ вредоносного ПО, оценка уязвимости, наблюдение за национальной безопасностью и борьба с дезинформацией. Используя эти ключевые слова, мы выполнили поиск в следующих электронных базах данных, таких как Google Scholar, цифровые библиотеки ACM, Web of Sciences, Science Direct и IEEE Xplore. Мы также искали различные инструменты и методы OSINT, различные журналы, посвященные OSINT, блоги OSINT и информационные бюллетени OSINT. Мы включили те работы, которые связаны с OSINT, приложениями OSINT и возможными областями интеграции OSINT. Другими характеристиками являются рейтинг цитируемости, известные журналы/публикации и сценарии, основанные на реальной жизни. Фигура3показывает анализ ресурсов, к которым осуществляется доступ и которые используются для изучения тенденций OSINT в кибербезопасности с использованием различных методов AI/ML/DL.

2.2 Извлечение общественного мнения и эмоций

Да и Аунг (2020 год) предложил модель, которая использовала прилагательные, отрицания и усилители текста для определения мнения пользователя по данному тексту. Их модель предназначена только для языка Мьянмы. Кандиас и др. (2017 год) автор провел эксперимент на 450 пользователях Facebook, чтобы определить уровень стресса. Яду и Шукла (2020 год) использовать пять разных

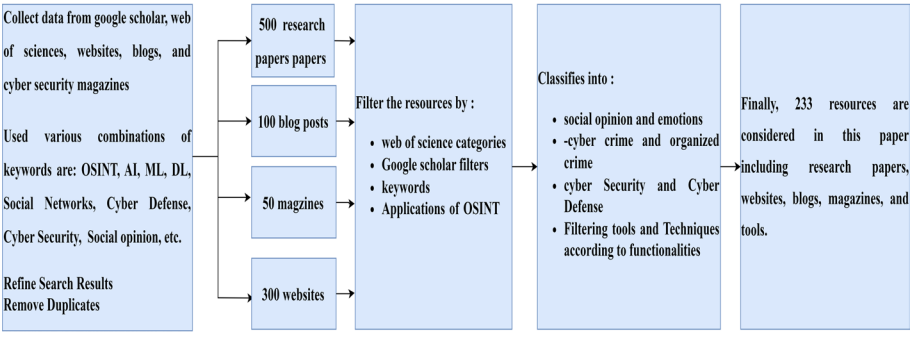

Рис. 3Обзор ресурсов, использованных для анализа

методы классификации для анализа эмоций, содержащихся в твитах индийской службы Air Asia. Прабхакар и др. (2019 год) использовал AdaBoost (Ensemble), который также объединяет другие классификаторы для создания надежного классификатора. Точность модели составляет 84,5%. По словам Вадавадаги и Паги (2020 год) использование глубокой нейронной сети можно распространить на другие задачи анализа настроений. Эти задачи анализа включают категоризацию партнерских отношений, компьютерный перевод, ответ на запрос и распознавание субъектов. Другие задачи, такие как обнаружение полярностей и символы мнений, также включены в анализ настроений. Хашида и др. (2018 год) предложил модель, основанную на распределенном многоканальном представлении, позволяющую гибридную интерпретацию текстовых данных.

Насим и др. (2019 год) предложили модель, основанную на двунаправленной кратковременной памяти (BiLSTM) и гибридном представлении слов, что повышает точность модели. В сентиментальных исследовательских твитах авиакомпаний они рассматривают термины из словаря (OOV), грамматику, многозначность, синтаксис и чувства слов. Сумро и др. (2020 год) предложили модель, в которой они проанализировали более 18 миллионов твитов. Все твиты связаны с новым коронавирусом. Твиты были проанализированы, чтобы увидеть связь между количеством заражений коронавирусом и общественным настроением. В связи с этим количество случаев увеличивается или уменьшается. Автор статьи (Абдул-Магид и Диаб2014 год) предложил модель, в которой анализ настроений использовался главным образом для понимания настроений на арабском языке через комментарии на YouTube и твиты в Твиттере. Гарсия и Бертон (2021 год) предложил модель, использующую данные Twitter для анализа настроений на португальском языке. Их целью было проанализировать последствия пандемии в двух географических точках: США и Бразилии.

Мишра и др. (2019 год) предложил модель, которая анализировала настроения различных обзоров. Используя результаты модели, они создали систему рекомендаций отелей. Используя методы MO, Джайн и Данданнавар (2016 год) изучили различные этапы анализа настроений с использованием данных Twitter. Они собрали данные из Twitter и использовали для предварительной обработки обработку естественного языка (NLP). Затем, чтобы получить характеристики, связанные с настроением, они выполнили извлечение признаков. Для обучения модели они использовали такие классификаторы, как дерево решений (DT), машина опорных векторов (SVM) и наивный байесовский метод (NB). Шуай и др. (2018 год) предложил модель с помощью отзывов китайских отелей. Они также использовали Doc2Vec для организации данных в сбалансированные отрицательные и положительные эмоции. Для обучения модели Doc2Vec данные интегрируются и оцениваются с использованием различных классификаторов, таких как SVM, логистическая регрессия (LR) и NB. Согласно результатам его работы, с показателем F 81,16%, SVM дал лучший результат по сравнению с другими классификаторами. Основываясь на современном уровне техники извлечения общественного мнения и эмоций, мы проанализировали, что извлечение мнений и эмоций важно, поскольку они могут нанести ущерб человеку, сообществу и стране. В большинстве случаев набор данных собирается случайным образом, и стандартный набор данных недоступен. Поэтому, если мы будем использовать инструменты и методы OSINT с AI/ML/DL, это улучшит результаты.

2.3 Киберпреступность и организованная преступность

Цифровая криминалистика и разведка из открытых источников — это два основных типа расследований киберпреступлений. Киберпреступность разделена на следующие категории в соответствии с конвенцией Совета Европы: преступления против ЦРУ (конфиденциальность, целостность и доступность), преступления в отношении контента, компьютерные преступления и другие виды киберпреступлений. Для описания киберпреступности мы рассмотрели такие термины, как компьютерная преступность, технологическая преступность, преступность в сфере высоких технологий, цифровая преступность и электронная преступность. Торговля людьми, порнография, детская порнография, убийства, продажа наркотиков, террористическая деятельность, рынки киберпреступности и обмен криптовалютами входят в число восьми основных киберпреступлений, выделенных Наза и др. (2020 год). Согласно

к информации, выбор инструментов и методов оказывает большее влияние на киберрасследования. Мы обнаружили, что ни один инструмент или процедура не могут собрать все доказательства, необходимые следователям, поэтому они используют различные комбинации инструментов и методов для проведения расследования киберпреступлений. Быстрый и Чу (2018 год) предложил систему, основанную на OSINT, которая повышает точность ареста преступника, и применил OSINT в цифровой криминалистике для улучшения анализа криминальной разведки. Делавальяде и др. (2017 год) предложил модель, полностью основанную на данных социальных сетей. Модель извлекает показатель преступности из разных социальных сетей и прогнозирует будущие преступления.

Шестак и Кощеева (2021 год) точно описал преступления, относящиеся к категории киберпреступлений, как пандемия коронавируса привела к росту уровня киберпреступности и возможные процедуры их смягчения. Была реализована структура для анализа инцидентов с использованием связанных твитов, количества ретвитов, хэштегов и соединений с унифицированным указателем ресурсов (URL). Географическое местоположение, положение текста направления эксперта и время твита были извлечены из фразы с использованием метода n-грамм, точность которого составляет 80 % (Родди и Холт). 2022 год; Мартин и др.2020 год; Синха и др.2022 год; Каккар2020 год). Малхотра и др. (2021 год) предложил модель оценки того, связан ли твит с событиями Crime Hub. Для классификации они использовали описание функций, токенизацию, остановку, трейлинг и извлечение TF-IDF. Было проведено исследование, чтобы отследить частые центры преступности в индийских штатах. Hub Watch можно использовать для сбора информации о потенциальных рисках, мошенничестве и работе общественного транспорта. Для планирования решений использовались три классификатора, а именно сеть Байеса (BN), KNearest Neighbours (kNN) и DT.

Авторы предложили объединенную архитектуру, которая поможет следователям идентифицировать и воссоздать места преступлений. Каждый этап сочетает логические процедуры с абстрактными принципами. Чтобы гарантировать, что правоохранительные органы могут повысить эффективность и результативность расследования, некоторые инструменты с открытым исходным кодом на каждом этапе предлагаемой объединенной архитектуры показаны на рис.4. Преступление

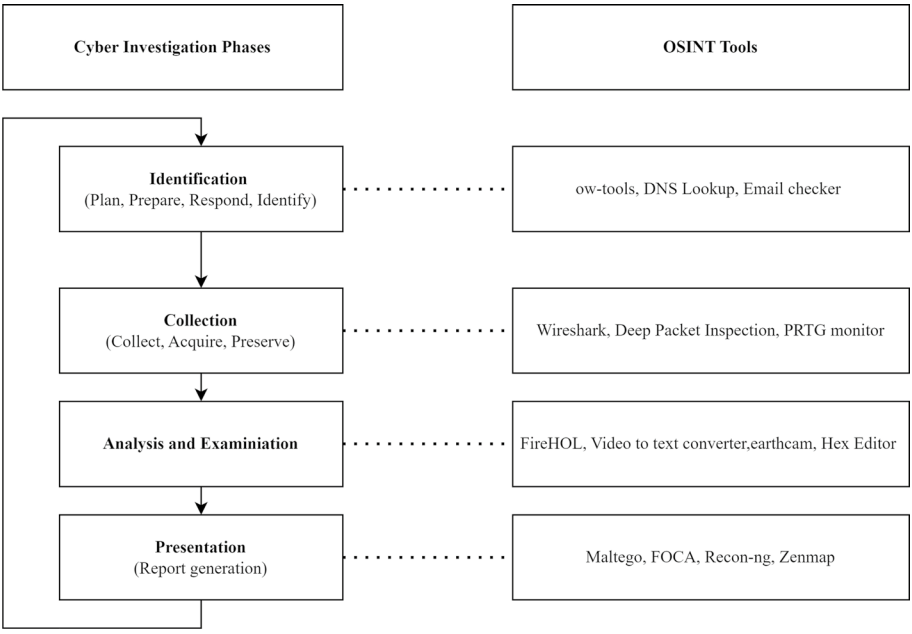

Рис. 4кибер-расследование с использованием инструментов OSINT (Као и др.2018 год)

Данные концентратора подразделяются на точечное и канальное разделение. Этот подход правильно классифицировал 467 твитов по ссылкам и 3168 твитов из Crime Hub по точкам с точностью 94,66% и 76,85% соответственно (Valluripally et al.2019 год). Кадогучи и др. (2020 год) исследования привели к разработке устройства. Это устройство можно использовать для отслеживания в реальном времени различных мест преступности в индийских штатах. Для классификации мошенничества в Crime Hub они использовали различные классификаторы ОД, SVM имеет самую высокую точность среди всех методов классификации - 97,28%. Статистические данные о приближениях к цели злоумышленника были отображены в качестве стратегии, помогающей хакерам избежать хакеров, инцидентов и обслуживания хаба киберпреступности (Родди и Холт2022 год).

Исследователь дал этой системе термин (Интеллектуальная транспортная система). Методы обнаружения и токенизации, основанные на онтологиях, использовались для предварительной обработки данных Твиттера в виде текстовой контекстной информации для выявления преступного центра в реальном времени. Затем значение было определено количественно с помощью извлечения IDF, а затем классифицировано. Согласно результатам, метод SVM обеспечивает максимальную точность. Он имеет точность 91,1% при просмотре текущего состояния задержек в Центре по борьбе с преступностью и 86,3% затормаживаний в Центре по борьбе с преступностью. Просмотр темной сети может быть полезен следователям, поскольку помогает узнать о новых рисках, новых видах лекарств и новых поставщиках (Celestini et al.2017 год). Пять методов интеллектуального анализа данных описаны Эдвардсом и др. (2015 год): обработка естественного языка (NLP), извлечение информации, анализ социальных сетей (SNA), компьютерное зрение (CV) и машинное обучение. Эти методы используют технологии для сбора данных из интернет-источников о связях преступных или террористических групп. Ляо и др. (2016 год) предложил iACE — технологию, которую можно использовать для автоматического сбора информации из многочисленных источников и анализа взаимосвязей данных. ИИ можно научить искать закономерности, сигнализирующие о преступной деятельности, в криминалистических данных, например в сетевом трафике. Фишинг — это атака социальной инженерии, как заявили Кромбхольц и др. (2015 год) и Иватури и Янчевский (2011 г.). И Пиента и др. (2018 год) и Гупта и др. (2017 год) предложил классификацию фишинговых атак, но не предоставил достаточного анализа фишинговых атак по электронной почте.

Опыты Альблади и Вейра (2017 год) и Халеви и др. (2013) предсказали, что личностные качества оказывают прямое влияние на способность пользователя обнаруживать фишинговые атаки по электронной почте, но из-за несогласованности результатов они разработали модель гипотез, в которой утверждалось, что на способность пользователя обнаруживать влияют личностные качества, доверие, компетентность и мотивация. Тандале и Павар (2020 год) предоставил обзор нескольких форм фишинговых атак и методов обнаружения. Кроме того, они представили несколько различных методов защиты от фишинга. Они пришли к выводу, что среди всех существующих методов борьбы с фишингом с использованием ML можно достичь 100% точности обнаружения фишинга. Алабдан (2020 год) предоставил обзор и полную оценку последних стратегий фишинговых атак для ознакомления с методами фишинга и различными типами атак. Растенис и др. (2020 год) представил модель классификации фишинговых атак на основе электронной почты, которая устраняет все недостатки предыдущей модели классификации фишинговых атак. Кэтрин и др. (2019 год) обсудили множество фишинговых атак и новейшие методы их предотвращения. Их исследование демонстрирует, как обнаружить и распознать фишинговые атаки с помощью алгоритмов машинного обучения.

Кунджу и др. (2019 год) рассмотрел различные методы обнаружения фишинговых атак. Их исследование продемонстрировало различные идеи и методы обнаружения атак. Они также заявляют, что некоторые из предлагаемых методологий неэффективны для обеспечения эффективных решений атак. Алеруд и Чжоу (2017 год) представил таксономию фишинговых стратегий, а также их векторы и меры противодействия. В документе освещены часто используемые уязвимости, а в таксономии представлены рекомендации по разработке различных успешных и эффективных методов защиты от фишинга. Куи и др. (2017 год) предложил метод расчета количества HTML-тегов, используемых в атаках DOM. Они использовали кластеризацию для создания кластеров атак, происходящих в пределах заданного диапазона расстояний, и заявили, что эти кластеры можно агрегировать и

используется для обнаружения фишинговых атак. Их результаты показали, что его стратегия может обнаружить значительное количество новых фишинговых атак.

Ван и др. (2020 год) предложил подход к предотвращению фишинга. На Android-смартфон установили систему оптического распознавания символов. Чтобы проверить эффективность предложенной профилактической методики, они протестировали атаки перехвата. Они заявили, что предложенный ими подход OCR преодолевает недостатки и ограничения существующих решений и достаточно эффективен для обнаружения фишинговых веб-сайтов. Чури и др. (2017 год) предложил прототип модели определения веб-сайта как фишингового. В своем исследовании они заявили, что существующие системы защиты от фишинга неэффективны для обнаружения фишинговых сайтов. Они использовали комбинацию визуальной криптографии и методов генерации кода. Предложенная ими методология создает изображение, делит его на две части с помощью визуальной криптографии, а затем объединяет эти две части для создания капчи изображения. Чтобы отличить подлинный сайт от фишинговых, пользователю предлагается сопоставить сайт с изображением капчи. Стаффорд (2020 год) исследовали последствия и причины фишинговых атак, а также то, как атаки влияют на пользователей. Люди подвержены фишингу из-за своих особенностей и поведения, таких как нарциссизм, восприимчивость и частое использование электронной почты. Результаты показывают, что целенаправленный фишинг является наиболее целенаправленным методом фишинга.

2.4 Кибербезопасность и киберзащита

Сенекаль и Коце (2019 год) использовал НЛП для анализа чатов WhatsApp для замечательного расследования, в котором оценивается масштабный вандализм в Южной Африке. Некоторые исследователи наблюдали использование OSINT в уголовных расследованиях, связанных с скоординированным неправомерным поведением и киберпреступностью (Као и др.2018 год). В настоящее время доступность онлайн-сервисов увеличивается, что приводит к росту большого объема цифровой информации (Эррера-Кубидес и др. 2020 год). Аль-Килани и Кусеф (2021 год) для дополнительной безопасности предложена интеграция некоторых методик OSINT с соответствующими пунктами стандарта ISO 27001. В контексте их интеграции с глобальным стандартом ISO 27001 они представили набор инструментов/методов OSINT, которые предназначены для проверки при приеме на работу, проверки анкетных данных и оценки рисков поставщиков.

Радж и Мил (2022 год) предложил модель обнаружения фейковых новостей. В своей модели они использовали два реальных набора данных Medival202 (Погорелов и др.2020 год) и CovidHeRA (Dharawat et al.2020 год). Они делят твиты на два класса: настоящие и фейковые. Чтобы определить фейковые и настоящие новости, они использовали следующие характеристики: пол, использование СМИ, полярность настроений, количество подписчиков, количество друзей, количество статусов, количество ретвитов и количество избранных. Эдвардс и др. (2017 год) предложили классификационную модель, в которой классифицируют личность организации на сотрудника и несотрудника, с помощью которой мы можем найти уязвимости, а также предотвратить атаки на организацию методом социальной инженерии. Классификатор, используемый для классификации, — DT. Они использовали такие подклассификаторы, как «Субклассификатор имени», «Субклассификатор активности», «Субклассификатор письма отпечатков пальцев», «Субклассификатор анализа ссылок», «Подклассификатор друзей» и «Географический подклассификатор». Юань и др. (2021 год) предложил модель под названием Domain Adversial и Graph Attention-Neural Network для обнаружения фейковых новостей. Где два реальных набора данных: «Набор данных Twitter MediaEval 2015 года (Boididou et al.2015 год) и набор данных Weibo» (Hu et al.2020 год) использовались в целях обучения и тестирования. В представленной модели интегрированы дискриминатор предметной области, экстрактор мультимодальных признаков данных и классификатор фейковых новостей на основе графа внимания. Для извлечения текстовых признаков, Bi-LSTM и изображений использовалась предварительно обученная модель VGG-19.

Синелли и др. (2022 год) исследовал скоординированный и нескоординированный аккаунт в Твиттере, рассматривая политические выборы в Великобритании в 2019 году. Для сбора данных они использовали API Twitter, учитывая хэштеги, связанные с выборами, влиятельные политические аккаунты, официальные аккаунты партий и аккаунты политических лидеров. Ислам и др. (2022 год) предложил инструмент проверки, использующий информацию о киберугрозах для автоматизации проверки предупреждений безопасности и инцидентов на базе оперативных центров безопасности. Они собрали «Индикаторы компрометации», используя OSINT с общедоступных веб-сайтов и MISP (MISP F).2021 год). Ч и др. (2020 год) предложил модель для анализа уровня киберпреступлений в масштабах штата. Они используют различные методы ОД для классификации киберпреступлений. NB и K-средние используются для классификации и кластеризации соответственно. Для классификации они использовали различные атрибуты, такие как жертва, инцидент, правонарушитель, возраст правонарушителя, вред, год, местонахождение и киберпреступность.

Ганесан и Майилваханан (2017 год) предложил методологию, которая помогает выявить непредсказуемые закономерности. Они собрали данные с различных веб-страниц и баз данных, которые помогают классифицировать киберпреступления. Классы киберпреступлений включают киберзапугивание, кражу личных данных, мошенничество, преследование, грабеж, преследование и клевету. Многофункциональная интеллектуальная система для борьбы с киберпреступностью была предложена Ноу и др. (2016 год). Основная цель этой системы заключалась в сокращении использования когнитивных предубеждений на протяжении всего процесса расследования. Этот метод предусматривает шесть основных этапов: выявление проблемы, разработка гипотезы, сбор данных, оценка гипотезы, выбор связанной гипотезы и постоянный мониторинг инцидентов. Аслан и др. (2018 год), предложил методологию обнаружения учетных записей социальных сетей (например, учетных записей Twitter), связанных с кибербезопасностью. Они использовали различные методы машинного обучения, такие как Random Forest, DT, SVM и т. д., для автоматического обнаружения подозрительных учетных записей. Они также использовали некоторые поведенческие характеристики, извлеченные из собранных твитов, для выявления подозрительных аккаунтов.

Аббасс и др. (2020 год) предложили методологию, которая помогает прогнозировать различные киберпреступления, связанные с социальными сетями, такие как киберзапугивание, киберпреследование, киберпреследование, кибервзлом и кибермошенничество и т. д. Они использовали данные, собранные с различных веб-сайтов социальных сетей. Они использовали Multinomial Naive Bayes (MNB), KNN и SVM для классификации киберпреступлений по различным классам. Кумар и др. (2020 год) предложили методологию, в которой они использовали тип данных о преступности, время и место для прогнозирования преступности в определенных регионах Индии. Они использовали KNN для прогнозирования и преступлений, которые прогнозируются с помощью этих методов: грабеж, несчастный случай, насилие, азартные игры, убийства и похищения людей. Демографическая и географическая информация об инцидентах прошлых лет использовалась для прогнозирования террористической деятельности в Индии. Они использовали ИИ для прогнозирования террористических актов (Верма и др.2019 год). Карлони (2014 год) предложил методологию, основанную на различных методах ML, для обнаружения и прогнозирования кибератак. Они использовали предыдущие данные о киберпреступлениях для обучения и тестирования модели.

3 Рабочий процесс OSINT

Рабочий процесс OSINT включает в себя следующие этапы, такие как сбор, обработка, анализ, извлечение знаний, распространение и планирование, как показано на рис.5.

Сбор — это этап, на котором мы собираем данные из открытых источников в соответствии с поставленной целью (Herrera-Cubides et al.2020 год). На этом этапе мы собираем данные из социальных сетей, веб-сайтов, форумов, отчетов (НПО, правительства, суда и правоохранительных органов), статей (научных исследований, журналистов), средств массовой информации (новости, интервью, видео- и аудиозаписи), буклетов. , книги и т. д. На этапе обработки собранные данные обрабатываются в соответствии с

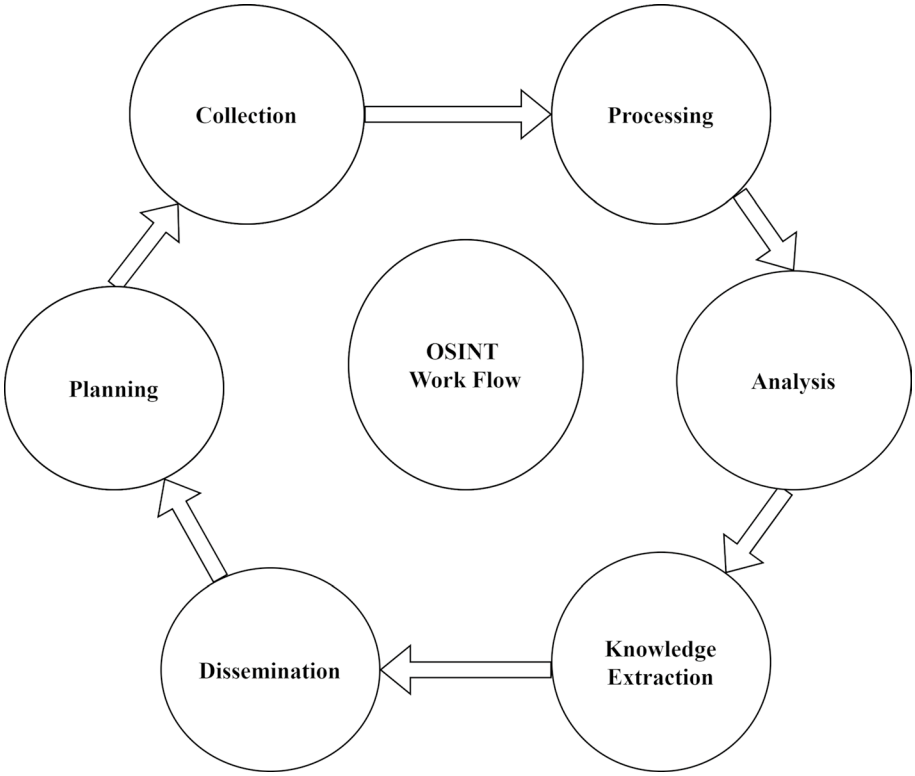

Рис. 5Рабочий процесс OSINT (Ахгар и др.2017 год)

объективны и синтезированы таким образом, чтобы их можно было легко понять. Данные будут разделены на релевантные и нерелевантные. Кроме того, он проверяет надежность источников, из которых собираются данные. На этом этапе мы также выполняем перевод, если это необходимо, например, если мы получаем данные в другом формате/языке, мы переводим их в необходимый формат/язык.

На этапе анализа мы оцениваем обработанные или соответствующие данные. Мы проводим лексический анализ (Гази и др.2018 год), CHC (Штиглиц и др.2018 год) и геопространственный анализ (VoPham et al. 2018 год) и т. д. Лексический анализ предполагает агрегирование и анализ текстовых данных, собранных из открытых источников. Мы также анализируем наиболее часто используемые термины, аккаунты людей в социальных сетях и их демографические характеристики. В SNA мы изучаем учетные записи в социальных сетях, связи, области интересов и т. д. В ходе этого анализа также анализируются подключенные сети конкретных пользователей/сообществ и их цели. В рамках геопространственного анализа мы находим местоположение целей или групп целей, используя различные инструменты с открытым исходным кодом, и анализируем координаты местоположения. На этапе извлечения знаний мы извлекаем соответствующую информацию из собранных данных для достижения цели задачи.

Распространение – это процесс, который помогает политикам, студентам, исследователям, правоохранительным органам, правительствам, организациям и т. д. Распространение осуществляется с образовательной и исследовательской точки зрения. В образовательных целях мы информируем человека о конфиденциальности и безопасности его данных, чтобы защитить свои данные от киберпреступлений или других проблем безопасности. В исследовательских случаях распространение информации помогает совершенствовать методы, тактику и приемы предотвращения

данные для цифровой криминалистики. Кроме того, это помогает использовать данные из открытых источников для расследования. План подготавливается для конкретной задачи путем анализа и обработки других этапов рабочего процесса OSINT на этапе планирования.

4 инструмента и метода OSINT

OSINT имеет несколько общих категорий, таких как геопространственный интеллект (GEOINT), человеческий интеллект (HUMINT), сигнальный интеллект (SIGINT), визуальный интеллект (IMINT) и интеллект социальных сетей (SOCMINT). Преимущества, недостатки и применение этих категорий перечислены в таблице.1(Оманд и др.2012 год; Уильямс и Блюм2018 год).

Данные также можно собрать физически, но это отнимает много времени и их легче использовать на более позднем этапе. Этот инструмент облегчает этап выбора, позволяя собирать информацию о нескольких объектах за считанные минуты. Ваша задача — определить, доступно ли имя пользователя, и предположить, что оно есть на всех сайтах социальных сетей. Один из способов — войти на все интернет-сайты, посвященные жизни (возможно, вы не имеете о них ни малейшего представления!) и проверить свое имя пользователя на этих сайтах. Другой вариант — использовать устройство с открытым исходным кодом, которое ссылается на различные веб-сайты, которые вы можете легко запомнить, и без задержек проверяет имена пользователей на каждом веб-сайте, и это занимает минимальное время. Управляйте несколькими устройствами, чтобы собрать все данные, относящиеся к цели, а затем объединить и проанализировать их. Общая поверхность атаки с использованием различных инструментов и методов OSINT показана на рис.6.

Исторические данные обычно используются для проверки или расследования конкретного инцидента. Доступно несколько архивов исторических данных, таких как коллекции газет, карт, книг, рукописей, научной информации, записей о рождении, свидетельств о браке и записей о смерти и т. д. Некоторые веб-сайты с историческими данными перечислены в таблице.2.

С помощью исторических данных расследование и проверка становятся проще. Инструменты и методы OSINT могут автоматизировать извлечение исторических данных и проверку информации.

Официальные хранилища утечек данных предоставляют нам утекшие данные, такие как данные шпионажа и исправлений, информацию о компаниях и официальные материалы с ограниченным доступом. Эти данные можно собрать с помощью официальных репозиториев утечек. Некоторые из них перечислены в таблице3.

Эти данные помогают в проверке и расследовании преступлений, а также в обучении моделей на основе DL. Для доступа к различным онлайн-сервисам люди используют уникальное имя пользователя. Используя имя пользователя, мы можем легко собрать данные, относящиеся к конкретному пользователю. Стол4исследует некоторые инструменты и методы работы с именами пользователей. Эти инструменты помогают найти учетную запись в социальных сетях. Например, lullar — это OSINT-инструмент, который автоматически генерирует URL-адреса пользовательских профилей различных социальных сетей.

Настоящее имя также используется для сбора данных о цели. Некоторые инструменты и приемы, основанные на реальных именах, перечислены в таблице.5. Используя эти инструменты, на основе настоящего имени мы можем собирать другую информацию, такую как адрес электронной почты, местоположение, учетные записи в социальных сетях, изображения, номера телефонов и возраст.

При расследовании электронной почты проверяется заголовок и тело электронного письма на наличие информации об отправителе и получателе. При анализе заголовка мы можем получить такую информацию, как «Получено», «X-получено», «Путь возврата», «Получено-SPF», «Аутентификация» и т. д. Полученная информация содержит IP-адрес сервера, SMTP-идентификатор, а также дату и время отправки электронного письма. полученный. X-Received — это параметр, не определенный в официальном стандарте протокола Интернета. Они создаются агентом передачи почты и содержат то же, что и параметр «Получено». Обратный путь включает IP-адрес сервера, адрес электронной почты получателя.

Таблица 1Преимущества, недостатки и применение общих категорий OSINT

Категории преимуществ OSINT		Недостатки	Приложения
ГЕОИНТ	Ситуационная осведомленность, Своевременность и точность информация, Интеграция из нескольких источников, Поддержка широкого спектра действий, Выявление закономерностей, Поддержка услуг на основе местоположения	Ограниченная доступность, стоимость, разное качество данных. ация, Отсутствие стандартизации, Ограниченная масштабируемость, Ограниченная точность, Ограниченное разрешение, Ограниченная визуализация данных	Вооруженные силы и оборона, Национальная безопасность, Катастрофы тер реагирование, Экологический мониторинг, Правоохранительные органы, морская охрана и безопасность
ДУМИНТ	Выявить и оценить потенциальные угрозы, в том числе террористические группы, преступные организации и иностранные правительства, используемые для разработки и реализации эффективных стратегий контрразведки и борьбы с терроризмом, используемые для выявления и отслеживания перемещения оружия, денег	Ненадежны и склонны к предвзятости, не поддаются проверке, требует много времени и ресурсов, подвержен культурным, языковым и социальным барьерам, уязвим для контрразведки, вероятность человеческой ошибки, зависит от правовых и этических соображений	Контрразведывательные операции, борьба с терроризмом. Изм, военные операции, сбор разведывательной информации о киберугрозах, правоохранительные органы, используются для сбора разведывательной информации о потенциальных угрозах общественной безопасности, помогая выявить закономерности, тенденции и потенциальные угрозы.
СИГНАЛ	Разведка в реальном времени, наблюдение на большом расстоянии, Ненавязчивый, гибкий, Кибервойна, Выявление уязвимостей, Поддержка военных операций, Экономически эффективный	Ограниченная точность, проблемы конфиденциальности, зависимость влияние на технологии, Сложность, Ограниченный географический охват, Этические соображения, Риски кибербезопасности	Военные операции, Борьба с терроризмом, Кибер оборона, Правоохранительные органы
ИМИНТ	Информация в режиме реального времени, экономичность, поддержка другие типы разведки (такие как SIGINT, HUMINT), Ненавязчивость, возможность предоставления исторических данных и долгосрочного анализа, легкое получение изображений с высоким разрешением	Зависит от погоды, Ограниченное проникновение (плотная леса или подземные сооружения), Дорого, Проблемы конфиденциальности и этики, Зависимость от технологий, Ограниченные сроки, уязвимость к мерам электронного противодействия (помехи или спуфинг), уязвимость к взлому, вредоносному ПО и другим формам киберугроз	Используется для поддержки военных операций (таких как разведка, определение целей и оценка боевого ущерба), может использоваться для обнаружения и отслеживания потенциальных угроз, таких как контрабанда, нелегальная иммиграция и терроризм (пограничная и прибрежная безопасность), наблюдение и разведка
СОЦМИНТ	Информация в режиме реального времени, экономичность, большой размер наборы данных, Нефильтрованная информация, Целевая информация, Широкий охват, Общественное мнение, Выявление тенденций и закономерностей, Выявление потенциальных кризисов, Выявление влиятельных лиц, Поддержка расследований	Проблемы конфиденциальности, качество данных, информация перегрузка, Зависимость от технологий, Ограничение онлайн-данных, Юридические и этические соображения, Отсутствие стандартизации, Трудность в определении достоверности источников, Ограничение на определенные языки	Собирайте разведданные и выявляйте преступную деятельность на платформах социальных сетей, политические кампании, потенциальное мошенничество, такое как фишинг или кража личных данных, киберугрозы, уязвимости и эксплуатации, правительственная разведка, уголовные расследования, обнаружение мошенничества, обнаружение киберзапугивания

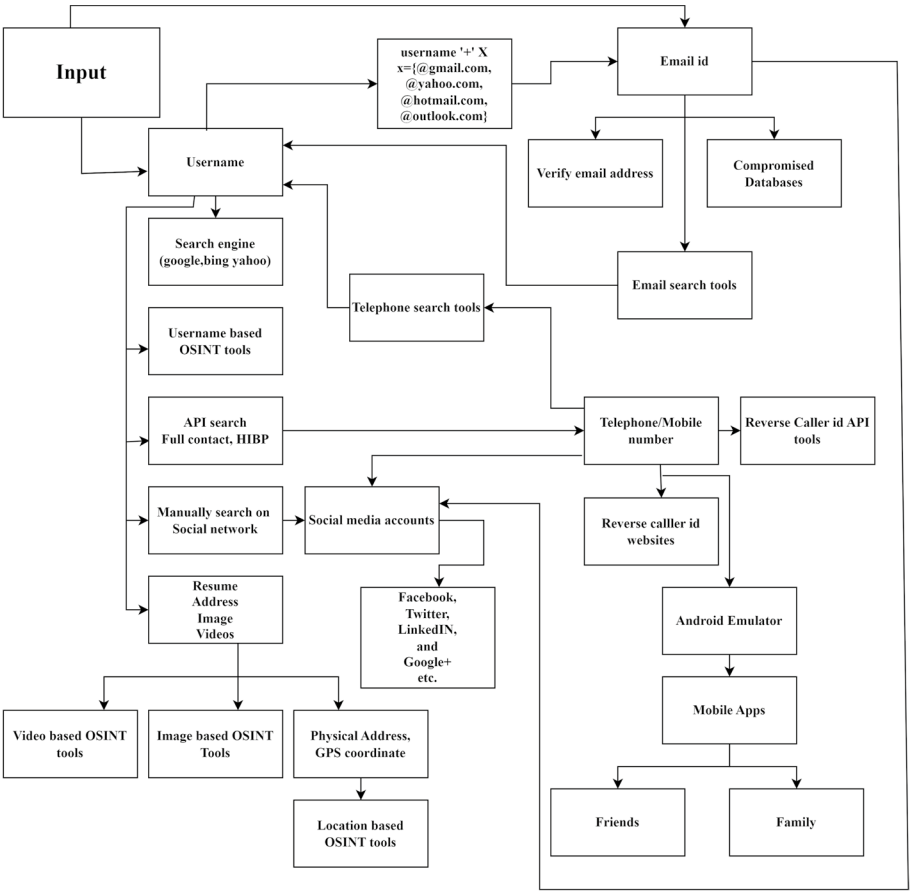

Рис. 6Общая поверхность атаки (Баззелл2016 год)

Таблица 2Веб-сайты для извлечения исторических данных

Имя	Функции
Библиотека Конгресса (Хайден2022 год)	Огромная коллекция газетных архивов, карт, фотографий. графики, книги и рукописи
Жизненная запись (Записи2022 год)	Запись о рождении, свидетельство о браке и запись о смерти
Science.gov (Правительство США2022 год)	США. Научная информация (более 200 миллионов страниц).
Алекса (2022 год)	Подробная информация на веб-сайтах.
Каталог журналов открытого доступа (Олиджук2022 год)	Обеспечивает доступ к рецензируемым, высококачественным и открытым доступ к журналам
Страницы онлайн-книг (Ockerbloom2022 год)	Более 10 миллионов книг

Таблица 3Официальный репозиторий утечек данных

Имя	Функции
WikiLeaks (Ассанж)2022 год)	Публикация больших наборов данных о цензурированных или иным образом ограниченных должностных лицах. материалы, связанные с войной, шпионажем и коррупцией
Криптом (2022 год) OffshoreLeaks (Деспрат2022 год)	Публикация секретных документов, запрещенных правительствами во всем мире Предоставляет информацию о владельцах компаний, доверенных лицах и посредниках. в секретных юрисдикциях

Таблица 4Инструменты проверки имени пользователя

Имя	Функции
Проверьте имя пользователя (Wise2008 год) Намечек (2009 год) Проверка имени (2022 год) Команда поиска пользователей (2022 год)	Помогает найти доступность пользователя в социальных сетях. Помогает найти учетную запись пользователя в социальной сети. Найти учетную запись в социальной сети. Найдите кого-нибудь по имени пользователя или адресу электронной почты в социальной сети. работы, Сайты знакомств, Форумы, Криптофорумы, Сайты чатов и Блоги

Таблица 5 Инструменты и методы поиска настоящего имени

Имя	Функции
Искатель истины (2015 год) Труба (Свинец2004 г.)	Публичные поисковые системы Америки Помогают найти настоящего человека
Спокео (Тан2006 г.)	Выполняйте поиск по имени, телефону, адресу или электронной почте для конфиденциального поиска. информация о людях
TruePeopleSearch (2022 год)	Помогает найти реального человека
Поиск в США (Быстрый поиск людей2022 год)	Прозрачный и информативный источник для поиска адресов, телефонов номера и адреса электронной почты
Разработчики PeekYou (2006 г.) Белая страница (Макмиллан1997 год)	Помогает находить друзей, родственников и коллег в Интернете. Находить людей, контактную информацию и проверять биографические данные.
Проверено (Вирджиния)2007 год) Поиск адреса (2022 год) Луллар (2022 год) Ясни (2022 год)	Поиск людей, транспортных средств, собственности и контактной информации. Поиск чьей-либо электронной почты или выяснение того, кто пишет вам по электронной почте. Поиск по профилю по электронной почте. Имя, фамилия или имя пользователя. Поиск людей.
ProfileEngine (2022 год)	Предоставьте полную информацию о сайте
Быстрый поиск людей (2022 год) Это они (2014 год)	Люди выполняют поиск по имени, адресу или обратному поиску телефона. Найти людей по имени, узнать, кто живет по адресу, найти людей, использующих номер телефона, электронная почта и т. д.
Вебмии (2022 год)	Поисковая система людей
Howmanyofme (OOO)2009 год)	Поисковая система людей
Генеалогия (2022 год)	Поиск семейной истории

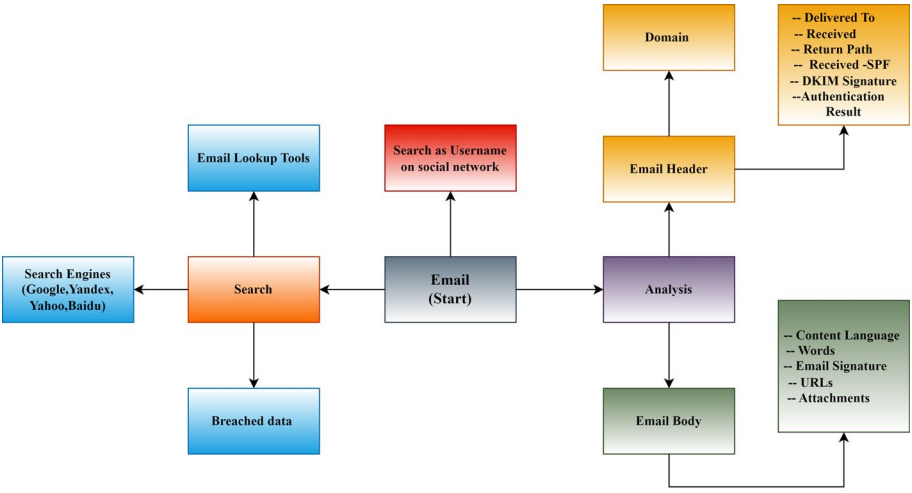

Рис. 7Поверхность атаки по электронной почте для расследования

Таблица 6Инструменты расследования электронной почты

Имя	Функции
Электронное досье (Технологии1997 год)	Проверить адрес электронной почты.
Emailhippo (Пол2010 год) Охотник (Финк2015 год)	Подтвердить адрес электронной почты.
Проверка электронной почты (2022 год)	Проверка электронной почты.
	Проверка электронной почты
Валидатор электронной почты байтовой установки (GmbH2003 г.)	Валидатор электронной почты
Формат электронной почты (2018 год) Мошенничество (Марк2004 г.)	Проверьте формат электронной почты Архив мошеннических писем
Анализ заголовков электронных писем (ipTRACKERonline2010 год)	Инструмент анализа заголовка электронной почты

адрес, информация о шифровании и т. д. Полученный-SPF включает IP-адрес отправителя вместе с именем хоста.

Есть некоторые параметры, такие как pass, что означает, что источник электронной почты действителен; softfail, что означает, что возможен поддельный источник; нейтральный, что означает, что достоверность источника трудно понять как надежную и неизвестную, что означает, что запись SPF не найдена. При анализе тела электронного письма мы проверяем язык содержимого, подписи, вложений и т. д. А также мы искали идентификаторы электронной почты в различных поисковых системах, инструментах поиска электронной почты, украденные данные, связанные с этим электронным письмом, и в нескольких социальных сетях для сбора. информацию, как показано на рис.7. Инструменты с открытым исходным кодом для расследования электронной почты перечислены в таблице.6.

Номер телефона также является ключевым объектом, который собирает информацию о цели. Некоторые инструменты и методы, основанные на телефонных номерах, перечислены в таблице.7. Мы можем быстро получить данные владельца номера телефона и информацию об устройстве, используя номер телефона.

Адрес интернет-протокола (IP) помогает собирать такую информацию, как географическое местоположение устройства, часовой пояс, код города, интернет-провайдер и т. д. Некоторые инструменты сбора географического местоположения на основе IP-адреса перечислены в таблице.8.

Таблица 7Поиск номера телефона

Имя	Функции
Зпросмотр (2022 год) Обратный поиск телефона (2022 год) Интер800 (Дианко 1995 год) Твилио (Лоусон2008 год) Fonefinder (Брубейкер1997 год) Призыватель истины (Заррингалам2009 год) FreeCarrierLookup (2022 год) Поиск телефона (2022 год)	Проверка владельца мобильного номера Информация о владельце мобильного номера Найдите продукты или услуги по бесплатному номеру. Мгновенно предоставляет вам имя вызывающего абонента и тип человека. Информация о владельце мобильного номера. Информация о владельце мобильного номера Имя оператора связи и тип номера: беспроводной или стационарный. Информация о владельце мобильного номера.

Таблица 8Информационные инструменты геолокации IP

Имя	Функции
IPверс (2022 год) IP2Location (Hexasoft2001 г.) IP-отпечатки пальцев (MaxMind2002 г.)	Предоставьте список IP-адресов Предоставить информацию о геолокации IP Географическое расположение IP-адреса вместе с некоторая другая полезная информация, включая интернет-провайдера, часовой пояс, код города, штат и т. д.
БД-ИП (2010 год)	API и база данных геолокации IP.
IP-местоположение (медиа2006 г.)	Предоставление информации о геолокации IP.
Утрейс (2022 год)	Предоставление информации о геолокации IP.

Таблица 9 IP-адрес в черном списке

Имя	Функции
Черный список (Мартин2007 год) FireHOL (Коста2022 год)	Сообщайте об атаках на ваш сервер Анализирует все доступные IP-каналы безопасности, в основном связанные с онлайн-атаками. злоупотребление линейными услугами, вредоносное ПО, ботнеты, серверы управления и контроля и другие виды киберпреступной деятельности.
Каталог вредоносных IP (Принц2004 г.)	Точный момент сбора адреса и собранный IP-адрес. это

Мы можем легко собрать список IP-адресов, занесенных в черный список, с помощью инструментов. Эти IP-адреса, занесенные в черный список, постоянно обновляются, что может помочь обучить модель DL обнаружению кибератак. Некоторые каталоги IP-адресов, занесенных в черный список, перечислены в таблице.9.

Изображение также является одним из ключевых объектов, с помощью которого мы собираем информацию о конкретном изображении. Инструменты поиска изображений помогают собирать изображения, связанные с различными инцидентами, такими как преступность, образование, последние новости, исторический имидж, политика и выборы. Эти инструменты помогают расследовать киберинциденты, такие как поиск изображений Google (2022 год), поиск изображений Bing (2022 год), изображения Yahoo (2022 год), Поиск картинок Яндекса (2022 год) и Байду (2022 год). Некоторые другие инструменты и методы поиска изображений перечислены в таблице.10.

В настоящее время обратный поиск изображений — это популярный метод, который помогает собрать информацию о конкретном изображении. Инструменты обратного поиска изображений помогают собирать такую информацию, как

Таблица 10Инструменты поиска изображений

Имя	Функции
Имгур (я2022 год)	Сайт для обмена изображениями и хостинг изображений Сайт
Фотоведро (2022 год)	для обмена изображениями и видеохостинг Сайт для обмена
СамодовольнаяКружка (2022	фотографиями
год) Flickrmap (Норби2022 год)	Сайт для обмена фото и видео
GettyImages (2022 год)	Сбор, создание и сохранение контента для повышения популярности визуальные коммуникации
Мгновенный поиск логотипа (MaxCDN2016 год)	Поиск логотипа
Фотографии Рейтер (1993 год)	Предоставить архив изображений, видео, аудио, графики и новости
Новости Прессы (Obits2022 год)	Предоставляет актуальные новости о различных типах преступлений, таких как образование, политика и выборы
Портал изображений Associated Press (Меир2013)	Коллекции исторических и современных фото-графики
Изображения PA (Маршалл2018 год)	Поиск изображений в Великобритании
Европейское пресс-фотоагентство (VisualRightsGroup 2003 г.)	Фото- и видеорепортаж о последних новостях
Архив изображений канадской прессы (2019 год)	Архив пресс-изображений Канады

Таблица 11Обратный поиск изображений

Имя	Функции
Обратный поиск Google (RGoogle2022 год)	Все связанные изображения, связанные с именем, в Google.
Кармадекай (Reddit2022 год) TinyEye	Источник изображения в основном ищется на Reddit.
(Тиней2008 год)	Чтобы узнать интересы или различные интересы человека, ему необходимо подключено только по изображению
Обратный поиск изображений (2011 г.)	Легко получить доступ к сайтам, содержащим загруженное изображение. в нем как открывается новая вкладка и отображаются все ссылки в ней
Камера находит приложение (2019 год)	Все места в сети, где присутствует изображение. Ограничено, поскольку это мобильное приложение.
Проект идентификации изображения (Wolfram1987 год)	Содержание изображения основано на результатах AI. ИИ, который определяет содержимое внутри изображения, что полезно при анализе объемных изображений.

устройство, использованное для захвата, местоположение и источник изображения и т. д. Некоторые инструменты и методы обратного поиска изображений перечислены в таблице.11.

Инструменты проверки манипуляций с изображениями помогают анализировать изображения. Эти инструменты также помогают собирать такую информацию, как метаданные изображения, местоположение захваченного изображения, скрытые пиксели и т. д. Некоторые инструменты и методы проверки манипуляций с изображениями перечислены в таблице.12.

Инструменты поиска видео помогают найти такую информацию, как источник видео, тип контента в видео и метаданные видео. Эти инструменты также помогают собирать разведданные о преступлениях и информацию о жертвах, а также помогают расследовать преступления, например, поиск видео Google (Google2022c), поиск видео Yahoo (Yahoo2022 год) и Bing Video (Microsoft20226). Некоторые другие инструменты поиска видео перечислены в таблице.13.

Инструменты геопространственного поиска помогают собирать информацию о местоположении и анализировать происшествия в любом конкретном месте, вид на улицу и другую информацию, связанную с целевыми местоположениями. Google

Таблица 12Проверка манипуляций с изображением

Имя	Функции
Судебно-медицинская экспертиза (Фридрих 2015 год) фотокриминалистика (Кравец2012 год) Гиро (Гиренсикс2017 год)	Лупы, анализаторы строк, обнаружение клонов ELA, скрытые пиксели, метаданные, строки и т. д. Извлечение метаданных, GPS-локализация, анализ уровня ошибок и т. д.
ExifTool (Харви2022 год)	полностью автоматизированный инструмент, предназначенный для проведения криминалистического анализа огромного количества изображений с помощью простого и удобного веб-приложения. Инструмент редактирования метаданных
GeoSetter (Смит2019 год)	Измените географические данные, связанные с файлом image.exe, чтобы они были отключены. загружено, но может быть полезно для изменения информации
Давайте улучшим (2022 год)	Изображение с более высоким разрешением. Устранение размытия размытого изображения полезности.

Таблица 13Поиск видео

Имя	Функция
AOL (Ланзоне)2022 год)	Видео основаны на различных классификациях. Очень Меньше поскольку точно определить информацию о жертве сложно
Стартовая страница поиска видео (2006 г.)	Общий поиск в Интернете, НО помогает не оставлять следов позади
Поиск видео в Facebook (2022 год)	Просматривайте видео на Facebook
Интернет-архив фильма с открытым исходным кодом (Kahle1996 год)	Все соответствующие медиа-файлы в Интернете. Соберите огромные количество информации только из названия
Мета трубка (2007 год)	Результаты распространились по Facebook. Требуется информация от Фейсбук
Земляная камера (1996 год)	Анализируйте окрестности жертвы. Прямая
Инсекам (2022 год) EzGif	трансляция с ближайшей камеры видеонаблюдения.
(Мадарс2022 год)	Редактируйте и проверяйте скрытые данные в видео.
Конвертер видео в текст (360Converter2021 год)	Анализируйте метаданные видео.

карты (20226), Карты Bing (Microsoft2022a), и карта Яндекса (2022 год) являются распространенными геопространственными инструментами. Некоторые геопространственные инструменты и методы перечислены в таблице.14.

Инструменты и методы OSINT для отслеживания движения воздуха помогают определить траекторию полета и текущее местоположение, а также отслеживать текущее местоположение цели в движении. Это также помогает контролировать воздушное движение в любом месте в любой момент времени. Некоторые OSINT-инструменты отслеживания движения воздуха перечислены в таблице.15

Основным этапом проведения морских исследований является обнаружение АИС (автоматической идентификационной системы) судна. Вы можете увидеть название судна, позицию, пункт назначения, тип судна и другую информацию с помощью AIS. Инструменты и технологии OSINT могут использоваться для отслеживания судов, которые нарушают закон, занимаются контрабандой наркотиков, людьми, незаконным рыболовством и практикуют военно-морские маневры (Smitrae2021 год). Некоторые OSINT-инструменты и методы слежения за судами приведены в таблице.16.

Используя сиамскую сеть с сетью региональных предложений, Шан и др. (2020 год) предложил систему слежения за морскими судами. Они внесли изменения в CNN в сиамской подсети, чтобы повысить эффективность абстракции признаков, и представили метод адаптивного извлечения области поиска, чтобы уменьшить воздействие тряски. Однако

Таблица 14Инструменты геопространственного поиска

Имя	Функции
Цифровой глобус (ESRI2022 год)	Карта локации, Исследуйте окрестности жертвы если место известно
Даум (2022 год)	Карта местоположения, ограниченная, как и все на корейском языке.
H2йо (2022 год)	Прямая трансляция со спутника для получения соответствующих
покачиваться (2001 г.)	данных. Сетевые карты местоположения.
BB Байк (Schneider)2022 год) Газетная	Различные карты размещены рядом для удобства сравнения.
карта (OpenStreetMap2022 год)	Intel важнее общих интересов в этой области, бренды News Papers используется в основном в этой области
Геологическая служба США (2022 год)	США наконец предоставили карту, отвечающую установленным требованиям. erties, Полезно для сужения цели
Просмотр улиц на карте Google (	Просмотр улиц в этом месте или вокруг него. Публично
2022a) KartaView (Крис2020 год)	доступные наборы данных для просмотра улиц. Прямая
ZoomEarth (2022 год) Мапиллярный (	трансляция со спутника с погодой и всеми видами
2013)	улиц, если таковые имеются.
Поиск адреса (Агарвал2004 г.)	Адрес кликера т.е. процесс превращения жертвы нажмите кнопку и получите его адрес
Виамихелин (2022 год) Проект	Путь между локациями
Корона (Уилсон1960 год)	Карта, сделанная секретным спутником США в 1970-х годах, использовалась для знать старое название места
ТрипГео (2022 год)	Анимированный путь между предоставленными локациями
Мапквест (2022 год)	Карта с указанием ближайших общественных мест, например ресторанов и т. д. поблизости, Легко исследовать обширную территорию
Мапхаб (2022 год)	Совместные карты
Коллекция карт библиотеки Перри-Кастанеды (2022 год)	Карта выбранного периода. Возьмите несколько действительно старых карт и новые карты тоже WayBack Machine of Maps
Круглый выстрел (Зейтц2022 год)	Живая камера активна поблизости. Исследуйте природу и поймите страна
Живая карта Земли (GlobalIncidentMap2006 г.)	Отметки на местах недавнего стихийного бедствия произошло, понять различные проблемы, с которыми сталкиваются разные страны в связи со стихийными бедствиями.

Таблица 15Отслеживание движения воздуха

Имя	Функции
Flightware (Сулак)2005 г.)	Путь и текущее местоположение полета, отслеживание текущего местоположения цели в движении
Полетный радар 24 (2006 г.)	Мониторинг воздушного движения в любом месте в любой момент времени
Отслеживание грузовых авиаперевозок (Track Trace1998 год)	Отслеживать груз, загруженный на рейс, позволяют ограниченные рейсы. эта функция, поэтому функциональность тоже ограничена
Радарный блок 24 (Брандао)2001 г.)	Отслеживайте воздушное движение в любом месте в любой момент
База данных World Aircraft (PlaneMapper2022 год)	времени. Данные, относящиеся к рейсу, словарь всех доступных рейсов.

предлагаемый трекер работает для ограниченных судов и погодных условий. Ян и др. (2022 год) предложил сеть отслеживания прибрежных судов, которая объединяет сегментацию и визуальное отслеживание объектов в целом, которая может одновременно отслеживать и сегментировать суда. Они использовали ERM

Таблица 16 Инструменты отслеживания морских перемещений

Имя	Функции
Морское сообщение (2007 год)	Карта всех морских перевозок по всему миру. Знайте морские перевозки. вокруг нужного места
Поиск судна (2011 г.)	Карта всех морских перевозок по всему миру. Знайте морские перевозки. вокруг нужного места
Круизный картограф (2022 год) Поиск	Знайте морское движение вокруг нужного места
кораблей (розовый корень2012 год)	Все корабли (названия) на локации, Знайте, где майор знаменитый корабли находятся вживую
Список префиксов контейнера (Лоренц1990 год)	Все о разных контейнерах. Активный, мертвый, на скамье подсудимых и т. д.
Идентификационный код контейнера владелец (БИК1970 год)	Точное местоположение и детали, связанные с кодом, Узнайте подробнее о владельце контейнера
Волза (Волза2022 год)	Знайте коды всех портов мира, чтобы облегчить поиск.

с более продвинутым подходом объединения пирамид функций. Этот подход расширяет карту функций сети во время извлечения и объединения функций, что поможет повысить точность отслеживания. Они использовали Большой морской набор данных, который содержит скоростные катера, грузовые суда, пассажирские суда, рыболовные суда и беспилотные суда. Ван и др. (2021 год) предложили модель обнаружения судов с использованием различных классификаторов ML, таких как Random Forest, SVM, LR, KNN и LDA и т. д. Для обучения модели они использовали спутниковые изображения. При предварительной обработке они использовали фильтр SDT для удаления шума с изображений. Для проверки они использовали данные Google Earth. Спадон и др. (2022 год) предложил модель, которая учитывает поведение сообщений AIS с использованием различных алгоритмов ML, а также DL в условиях нерегулярных и зашумленных данных. Чжан и др. (2021 год) предложил модель RoDAN, которая объединяет три измерения, такие как масштаб, движение и регион, для отслеживания информации. Они использовали модуль ASPP для масштабирования размеров, что помогает получать более точную информацию для отслеживания кораблей. Они использовали общедоступные наборы морских данных под названием SMD (Prasad et al.2017 год) и набор данных HSD, подходящий для отслеживания судов, например MarDCT (Gundogdu et al.2016 год). Инструменты отслеживания пакетов помогают отслеживать посылку и получать обновленную информацию о посылке. Эти инструменты помогают отслеживать посылки с контрабандой наркотиков, оружия и нелегальные посылки. Некоторые OSINT-инструменты и методы отслеживания посылок перечислены в таблице.17.

Таблица 17Инструменты отслеживания посылок

Имя	Функции
После корабля (Чан2022 год)	Живой трек после падения
Отслеживаниеех (2022 год) 17 Трек	Отслеживание посылки в реальном времени с точки зрения компании. Отслеживание в
(Растин2010 год) Отслеживание	реальном времени после получения.
посылок (USP2008 год) Почта Канады	Отслеживание посылки в реальном времени с точки зрения компании
(Эттингер2019 год) Королевская почта	Местоположение и информация о пакетах, ограничено только для Канады. Местоположение
(Томпсон2022 год)	и информация о пакетах ограничено, ограничено только Великобританией.

5 Обсуждение

Задачами OSINT-расследований являются: автоматизация процесса сбора, анализа и извлечения знаний, интеграция нескольких открытых источников данных, фильтрация дезинформации и нерелевантных данных, глобализация инструментов и методов OSINT, осведомленность о конфиденциальности, этические и юридические соображения, а также предотвращение злоупотребление инструментами и методами OSINT.

С этической точки зрения инструменты и методы OSINT должны использоваться искренне и законно для законных целей. Общедоступные данные не означают, что они не являются конфиденциальными данными. Потому что, если чьи-то политические взгляды, медицинские данные, религиозные убеждения, а также информация о семье и друзьях станут общедоступными, эти данные могут быть использованы для угроз или шантажа. Например, религиозные убеждения могут привести к убеждению правительства и общественности в терроризме. В связи с этим мы должны гарантировать, что мы соблюдаем этические нормы, правила и нормы конфиденциальности данных, такие как Общий регламент по защите данных (GDPR), Закон Калифорнии о конфиденциальности потребителей (CCPA) и другие применимые законы, соответствующие их местонахождению.

GDPR (EC2016 год) был введен Европейским Союзом для регулирования обработки персональных данных граждан Европы. OSINT также предполагает обработку персональных данных. Таким образом, некоторые аспекты GDPR, связанные с OSINT, — это подотчетность (все используемые данные и способы их сбора должны быть документированы), правовая основа (вам необходимо получить согласие (статья 6.1.a)), юридические обязательства и законный интерес, принципы(статья 5) и права субъектов данных (статья 14). Принципы включают в себя законность, которая гласит, что метод сбора, который будет использоваться для сбора, должен быть юридически проверен (не нарушайте протокол аутентификации для сбора любого типа данных). Прозрачность означает, что используемый обработчик данных, тип обрабатываемых данных и цель обработки собранных данных должны быть прозрачными, Минимизация данных (вы должны стараться обрабатывать как можно больше минимальных личных данных), Ограничение хранения (не хранить данные дольше). чем это необходимо), Целостность и конфиденциальность (к данным должны быть доступны только вы и ваш клиент, вы должны хранить данные в зашифрованном виде). Права субъектов данных включают право на уведомление, право доступа, право на исправление, право на удаление данных и право на ограничение обработки данных.

В случае наблюдения (Miller et al.2022 год), мы собрали огромное количество информации из разных источников, которая помогает отслеживать и контролировать отдельного человека, группу и организацию. Эта информация может поднять вопрос о гражданских свободах и свободе выражения мнений, поэтому мы должны гарантировать, что не нарушаем никаких прав личности. Существуют различные вопросы, такие как конфиденциальность данных, защита данных, вопросы гражданских свобод, свобода выражения мнений и т. д. Согласно GDPR, вы можете обрабатывать и хранить данные до тех пор, пока они не потребуются. В противном случае вы должны навсегда удалить всю информацию, касающуюся конкретного расследования. Собранные данные должны храниться в зашифрованном виде и доступны только вам и вашему клиенту. OSINT полезен правительству, правоохранительным органам и специалистам по кибербезопасности, но для законной работы его следует использовать этично. Вы должны убедиться, что сбор данных осуществляется в соответствии с правилами и положениями и не нарушает протоколы аутентификации. Кроме того, организации/частные лица должны иметь четкое представление о законах и правилах, регулирующих сбор, хранение и использование OSINT. Это включает в себя понимание прав отдельных лиц и организаций в отношении их личной информации и понимание санкций за несоблюдение.

OSINT необходимо использовать в соответствии с законом и с учетом политики конфиденциальности и защиты данных (Раджамаки и Симола).2019 год). OSINT является законным по определению, но необходимо обеспечить, чтобы данные, собранные исследователями, следователями, государственными органами и правоохранительными органами,

не публиковался, даже если данные общедоступны. Мы не должны нарушать протокол аутентификации для сбора данных. Другими словами, мы можем сказать, что OSINT необходимо использовать ограниченно для законной и неопасной деятельности. Нам необходимо найти баланс между тем, что мы собираем, и тем, что мы храним или упоминаем в отчете после расследования. В любом запросе мы собираем все возможные данные, но нам необходимо убедиться, что в окончательном отчете информация подпадает под действие GDPR, а данные должны быть в зашифрованном виде и доступны только вам и вашему клиенту.

Учитывая дезинформацию, на ранних стадиях пандемии COVID-19 государства отчаянно нуждались в любых средствах борьбы с экономическими, медицинскими и человеческими последствиями этой болезни. Серьезность кризиса побудила государства использовать или рассматривать возможность использования любых доступных инструментов, даже тех, которые ранее ограничивались целями национальной безопасности. Использование инструментов разведки и наблюдения, традиционно используемых для обеспечения безопасности, разведки и правоохранительной деятельности для наблюдения за пандемией, подчеркивает решительные меры, которые многие государства приняли для сдерживания распространения и минимизации воздействия COVID-19.

Технологии, которые используются для наблюдения за национальной безопасностью (например, мониторинг местоположения, распознавание лиц и разведка в социальных сетях), используются для борьбы с пандемией Covid-19. Например, Соединенные Штаты разработали технологию, использующую данные социальных сетей (таких как блоги, новости, социальные сети и правительственные источники) для противодействия распространению пандемии Covid-19 (Берман и др.2020 год). Некоторые другие страны (например, Израиль, Пакистан, Южная Корея, Гонконг, Китай и т. д.) также использовали свои разведывательные данные национальной безопасности (например, мониторинг местоположения, видеонаблюдение, распознавание лиц, отслеживание отдельных лиц / групп, GPS и отслеживание мобильных телефонов, и т. д.) для контроля распространения и противодействия Covid. Из-за ковида умирают миллионы людей, и это влияет на экономические условия во всем мире. В связи с этим использование разведывательной системы национальной безопасности, а также инструментов и методов OSINT для противодействия пандемии оправдано. Но инструменты и методы OSINT должны использоваться с учетом киберзаконов и правил, конфиденциальности данных, защиты данных, свободы выражения мнений, гражданских свобод и т. д.

Для сбора данных используются веб-сканеры, веб-скраперы и инструменты на основе API. При анализе и извлечении знаний мы обычно проводим семантический анализ, анализ моделей угроз, корреляцию с другими событиями, а также возникновение данных, чтобы найти связь между различными отдельными частями информации и получить соответствующую информацию. А также использовал методы интеллектуального анализа данных, методы НЛП и СНС для извлечения соответствующей информации из собранных данных. При интеграции множества данных с открытым исходным кодом мы интегрируем агрегированные данные из различных социальных сетей, Интернета, а также из даркнета. В случае обнаружения фейковой информации, фильтрации нерелевантных данных и дезинформации обычно предлагаются модели ML и DL. Когда мы используем инструменты и методы OSINT, нам необходимо сосредоточиться на конфиденциальности пользователей, конфиденциальности членов семьи пользователей, конфиденциальности друзей пользователей и конфиденциальности их коллег. И следуйте правилам и нормам защиты GDPR. OSINT является законным, поскольку источники данных общедоступны. Нам также необходимо помнить, что общедоступные данные подвержены злоупотреблениям (Кастель 2018 год), киберагрессия (Кумар и др. 2018 год), киберзапугивание (Хосейнмарди и др.2015 год; Вакс и др. 2019 год), кибер-сплетни (Гарсиа-Фернандес и др.2022 год) и киберпреследование (Abarna et al.2022 год).

Неправильное использование инструментов и методов OSINT приводит к одиночеству, депрессии, страданиям, а в худшем случае жертвы могут покончить жизнь самоубийством. Мы можем успешно использовать OSINT для набора кадров, противодействия киберпреступникам, предотвращения распространения дезинформации, обнаружения фейковой информации, профилирования киберпреступников, проведения цифровой криминалистики и т. д. Профилирование киберпреступников на рынке даркнета является одним из вариантов использования OSINT. инструменты и техники. Проблема, однако, заключается в том, что профилирование человека, который на самом деле не представляет собой

угроза приводит к дискриминационному и несправедливому отношению, а затем может затронуть жертв. OSINT помогает профилировать кибератаки и совершенствует сложные кибератаки (Akinrolabu et al.2018 год). Это выгодно в частном секторе, а также служит ресурсом общественного интереса для правительств (Ланде и Шнурко-Табакова).2019 год). Это также помогает в секретных расследованиях и секретных операциях (Ларсен и др.2017 год). Помогает в расследовании и стратегическом планировании борьбы с преступлениями (Ахгар2016 год).

6 Заключение и будущая работа

В этом документе обсуждается текущее состояние разведки с открытым исходным кодом (OSINT). Выяснилось, что существующие методы неадекватны из-за их недостаточной эффективности в реальных сценариях. В этом документе основное внимание уделяется важности интеграции OSINT в киберзащиту, социальные сети, цифровую судебную экспертизу и другие возможные области для выявления профиля преступников, киберпреступлений, борьбы с терроризмом и киберинцидентов. В документе также изложены основные методы OSINT-поиска и описаны расширенные инструменты OSINT. Правильный выбор инструментов на основе имеющихся данных и целей имеет решающее значение, но использование комбинации инструментов — лучший способ добиться точных результатов.

В этой статье мы также описали данные из открытых источников, социальные сети, различные типы киберпреступлений, а также инструменты и методы OSINT с использованием NLP/AI/ML/DL, и это может быть полезно следователям для улучшения исследований и приложений OSINT. Как правило, IOC извлекаются из традиционных черных списков, таких как cleanMX и Phishtank, которые включают только URL-адреса, домены, IP-адреса и подписи MD5, но не включают преступные группы и другую контекстную информацию. Таким образом, используя OSINT, мы можем добавить психологические и поведенческие особенности. Мы пришли к выводу, что OSINT может помочь улучшить проблемы кибербезопасности в различных областях, таких как обнаружение фишинга, сбор информации об угрозах, обнаружение разжигания ненависти, обнаружение фейковых новостей, торговля людьми, торговля детьми, криминальное профилирование и т. д. OSINT также помогает отслеживать группы APT, фальшивые изображения. /video анализ, отслеживание вредоносных действий и отслеживание насильственных действий. В случае обнаружения фишинга мы используем различные доступные наборы данных для обучения модели. Но если мы будем использовать функции автоматического обновления, шаблоны атак и IOC, то модель может стать более надежной и эффективной.

Задачи, которые необходимо решить, заключаются в следующем: извлечение индикаторов компрометации и их взаимосвязей из неструктурированных отчетов об угрозах и использование полученных знаний для поиска угроз, создание консорциума преступников для их отслеживания, разработка структуры всех возможных инструментов и методов OSINT, автоматизация сбора информации и извлечения аналитических данных из данных из открытых источников с использованием искусственного интеллекта, создание модели в реальном времени с использованием методов OSINT и DL для автоматического мониторинга групп Advanced Persistent Threat (APT), создание многоплатформенных и многоязычных социальных сетей на основе эталонный набор данных для обнаружения киберпреступлений с помощью инструментов и методов OSINT. Также необходимо изучить возможность автоматического обнаружения торговли людьми и детей с помощью методов OSINT и DL.

Рекомендации

360Converter (2021 г.) 360converter предоставляет различные виды конвертеров, в первую очередь ориентированных на видео, аудио, речь и голос в текст.http://www.360converter.com/

Абарна С., Шиба Дж., Джаясрилакшми С. и др. (2022 г.) Выявление киберпреследований и намерений их жертв пользователей на платформах социальных сетей. Eng Appl Artif Intell 115(105):283

Аббасс З., Али З., Али М и др. (2020 г.) Система прогнозирования социальной преступности с помощью твитов в Твиттере с использованием машинное обучение. В: 2020 IEEE 14-я международная конференция по семантическим вычислениям (ICSC), IEEE. стр. 363–368

Абдул-Магид М, Диаб М (2014) Сана: крупномасштабный многожанровый и многодиалектный лексикон для арабского суб- анализ объективности и настроений. В: Материалы девятой международной конференции по языковым ресурсам и оценке (LREC'14).

Поиск адреса (2022 г.) Бесплатный поиск адреса электронной почты и почтового адреса.https://www.адреспоиск.ком/. Доступ июль 2022 г.

Агарвал А. (2004) Где я? Знайте свое местоположение и почтовый адрес на картах Google.https://ctrlq.org/карты/адрес

Ахгар Б (2016) Осинт как неотъемлемая часть аппарата национальной безопасности. В: Ахгар Б (ред.) С открытым исходным кодом. разведывательное расследование. Спрингер, Нью-Йорк, стр. 3–9.

Ахгар Б., Байерл П.С., Сэмпсон Ф. (2017) Разведывательное расследование с открытыми источниками: от стратегии к реализации. ция. Спрингер, Нью-Йорк

Акинролабу О, Аграфиотис И, Эрола А (2018) Проблема обнаружения сложных атак: идеи из Аналитики SOC. В: Материалы 13-й международной конференции по доступности, надежности и безопасности. стр. 1–9

Алабдан Р. (2020) Исследование фишинговых атак: типы, векторы и технические подходы. Будущий Интернет 12(10):168

Алблади С.М., Вейр Г.Р. (2017)Личностные качества и виктимизация от кибератак: анализ множественного посредничества. В: 2017 Бизнес-модели, пользователи и сети Интернета вещей, IEEE. стр. 1–6

Алеруд А., Чжоу Л. (2017) Среда, методы и меры противодействия фишингу: опрос. Вычислить Безопасность 68: 160–196

Alexa (2022 г.) Уведомление о прекращении обслуживания.https://www.alexa.com/. Доступ июль 2022 г.

АлКилани Х., Кусеф А. (2021) Интеграция методов Osint с оценкой рисков ISO/IEC 27001. В: Interna- Международная конференция по науке о данных, электронному обучению и информационным системам 2021. стр. 82–86.

Амаро Л., Де Лос Сантос Т., Джозеф Н. и др. (2018) Применение процесса отзывчивой идентификации о модели социальных сетей (призма) в контексте онлайн-платформы для мам

Аслан ЧБ, Саглам РБ, Ли С (2018) Автоматическое обнаружение учетных записей, связанных с кибербезопасностью, в социальных сетях. сети: Twitter в качестве примера. В: Материалы 9-й международной конференции по социальным сетям и обществу. стр. 236–240

Ассанж Дж. (2022) Wikileaks — это гигантская библиотека.https://wikileaks.org/. Доступ июль 2022 г.

Да Ю.М., Аунг С.С. (2020) Анализ настроений на основе контекстной лексики в текстовых обзорах Мьянмы. В: 2020 г. 23-я конференция восточного Международного комитета COCOSDA по координации и стандартизации речевых баз данных и методов оценки (O-COCOSDA), IEEE. стр. 160–165

Baidu (2022) Изображение Baidu.http://image.baidu.com/. Доступ июль 2022 г.

Баззелл М. (2016) Методы разведки с открытым исходным кодом: ресурсы для поиска и анализа онлайн-информации. Мация. Независимая издательская платформа CreateSpace, Скоттс-Вэлли,

Берман Э., Фаулер Л.Р., Робертс Дж.Л. (2020) Наблюдение за Covid-19

BIC (1970) Международный реестр кодов владельцев контейнеров.https://www.bic-code.org/bic-codes/

Изображение Bing (2022 г.).http://www.bing.com/images. Доступ июль 2022 г.

Боидиду С., Андреаду К., Пападопулос С. и др. (2015) Проверка использования мультимедиа в средневековье, 2015 г. Медиа- aEval 3(3):7

Брандао А. (2001) Глобальная информация об отслеживании рейсов: отслеживание рейсов в реальном времени и статус аэропорта.https://www.радар box.com/

Брубейкер В. (1997) находит географическое местоположение любого телефонного номера.http://www.fonefinder.net/ CamFind

(2019) Мобильная визуальная поисковая система.http://camfindapp.com/

Canadian Press (2019) Ведущая коллекция фотографий и видео Канады Canadian Press.http://www.cpimages.com/fotoweb/index.fwx

Карлони Дж. (2014) Интегрированное обучение по содержанию и языку: смешанная модель в высшем образовании. Инт Дж Technol Knowl Soc Annu Rev 9:4

Кастель М. (2018) Лингвистические идеологии классификации глубоко оскорбительных языков. В: Труды 2-й онлайн-семинар по ненормативной лексике (ALW2). стр. 160–170

Селестини А., Ме Г., Миньон М. (2017) Исследовательский анализ данных торговых площадок Tor: случай с наркотиками. В: Интер- национальная конференция по глобальной безопасности, безопасности и устойчивому развитию. Спрингер, стр. 218–229.

Ч.Р., Гадекаллу Т.Р., Абиди М.Х. и др. (2020) Вычислительная система для классификации киберпреступлений с использованием машинное обучение. Устойчивое развитие 12(10):4087

Чан Т (2022) Отслеживание доставки.https://www.aftership.com/couriers. По состоянию на июль 2022 г., Крис

(2020 г.), просмотр карты.https://kartaview.org/landing

Чури Т., Савардекар П., Пардеши А. и др. (2017) Надежная методология защиты от фишинга. В: 2017 г. международная конференция по инновациям в информационных, встроенных и коммуникационных системах (ICIIECS), IEEE. стр. 1–4

Синелли М., Креши С., Кваттрочиокки В. и др. (2022) Скоординированное недостоверное поведение и информация распространение в твиттере. Системы поддержки принятия решений. p 113819

Коста Т (2022 г.) Черные списки IP: каналы репутации IP.http://iplists.firehol.org/. По состоянию на июль 2022 г. CruiseMapper (2022 г.) Cruisemapper.http://www.cruisemapper.com/. Доступ июль 2022 г.

Криптом (2022) Несанкционированное разглашение государственной тайны.https://cryptome.org/. По состоянию на июль 2022 г. Cui J et al (2017) Отслеживание фишинговых атак с течением времени. стр. 667–676

Даум (2022) Инструмент геопространственного поиска.http://map.daum.net/. По состоянию на июль 2022 г. DBIP (2010 г.). API и база данных геолокации IP.https://db-ip.com/

Делаваллад Т., Бертран П., Тувено В. (2017) Извлечение показателей будущей преступности из социальных сетей. В: Ларсен Х.Л. и др. (ред.) Использование открытых данных для обнаружения угроз организованной преступности. Спрингер, Нью-Йорк, стр. 167–198.

Desprat C (2022) База данных утечек на море.https://offshoreleaks.icij.org/. Доступ: июль 2022 г. Дхарават А., Лоренцу I, Моралес А. и др. (2020 г.) Пить отбеливатель или что делать дальше? covid-hera: набор данных для принятия решений в области здравоохранения с учетом рисков в условиях дезинформации о covid19. Препринт на http://arxiv.org/abs/2010.08743

Dianco (1995) Каталог Internet 800 - каталог бесплатных звонков (бесплатный), список 800, 866, 877 и 888. Объединение предприятий по компаниям, количеству и типам отраслей, независимо от оператора дальней связи. http://inter800.com/index.html

EarthCam (1996 г.) Глобальная сеть принадлежащих и управляемых веб-камер прямой трансляции.http://www.earthcam.com/

Эдвардс М., Рашид А., Рэйсон П. (2015) Систематический обзор технологий онлайн-анализа данных, предназначенных для правоохранительных органов. ACM Comput Surv (CSUR) 48 (1): 1–54

Эдвардс М., Ларсон Р., Грин Б. и др. (2017) Поиск золота: автоматический анализ социальных сетей в Интернете инженерные поверхности атаки. Компьютерная безопасность 69: 18–34

Эдвардс М., Уильямс Э., Пирсман С. и др. (2022) Характеристика киберпреступников: обзор. Препринт на http://arxiv.org/abs/2202.07419

Проверка электронной почты (2022 г.).https://email-checker.net/. Доступ июль 2022 г.

Формат электронной почты (2018 г.) Формат адреса электронной почты для миллионов компаний.https://email-format.com/

Enhance (2022) увеличивает разрешение изображения без потери качества.https://letsenhance.io/. Доступ в июле 2022 год

ESRI (2022) Цифровые карты глобуса.https://discover.digitalglobe.com/. Доступ июль 2022 г.

Эттингер Д. (2019) Инструменты онлайн-доставки и маркетинга.https://www.canadapost-postescanada.ca/cpc/en/инструменты.страница

EC E (2016) Lex-02016r0679-20160504-en-eur-lex.https://eur-lex.europa.eu/eli/reg/2016/679/04.05.2016

Facebook (2022) Видео из Facebook.https://www.facebook.com/pg/facebook/videos. По состоянию на июль 2022 г. Fast People Finder (2022 г.) Поиск быстрых людей.https://fastpeoplefinder.com/. По состоянию на июль 2022 г. Fink A (2015 г.) Проверка электронной почты: подтвердите адрес электронной почты с помощью бесплатной программы проверки электронной почты.https://hunter.io/email-верификатор

Flightradar24 (2006 г.) Глобальный сервис отслеживания рейсов, который предоставляет вам информацию в режиме реального времени о тысяч самолетов по всему миру.https://www.flightradar24.com/

FreeCarrierLookup (2022) Инструмент поиска номеров телефонов.http://freecarrierlookup.com/. По состоянию на июль 2022 г.

Фридрих Дж. (2015 г.) Инструменты для обнаружения клонов, анализа уровня ошибок, извлечения метаданных.https://29a.ch/фотокриминалистика/

Ганесан М., Майилваханан П. (2017)Анализ киберпреступности в социальных сетях с использованием метода интеллектуального анализа данных. Int J Pure Appl Math 116(22):413–424

Гарсия К., Бертон Л. (2021) Выявление тем и анализ настроений в контенте Твиттера, связанном с Covid-19. из Бразилии и США. Приложение Soft Comput 101(107):057

Гарсиа-Фернандес СМ, Морено-Мойя М, Ортега-Руис Р. и др. (2022) Участие подростков в кибер-сплетни: влияние на социальную адаптацию, издевательства и киберзапугивание. Span J Psychol 25:e6 Генеалогия (2022 г.) Исследовательский ресурс с более чем 14 000 онлайн-форумов, посвященных генеалогии.https://www.генеалогия.com/. Доступ июль 2022 г.

GettyImages (2022 г.) Бесплатные стоковые фотографии, иллюстрации, векторная графика и видеоклипы.http://www.gettyimages.com/. Доступ июль 2022 г.

Гази Й., Анвар З., Мумтаз Р. и др. (2018)Подход на основе контролируемого машинного обучения для автоматизации. своевременное извлечение информации об угрозах высокого уровня из неструктурированных источников. В: Международная конференция по передовым технологиям (FIT), IEEE, 2018 г. стр. 129–134

Ghirensics (2017) Автоматизированный инструмент для криминалистики цифровых изображений.http://www.getghiro.org/ GlobalIncidentMap (2006)
Находите и картируйте террористические акты, вспышки заболеваний, землетрясения, лесные пожары,
авиационные происшествия, угрозы церквям, угрозы школам, угрозы журналистам и т. д.http://quakes.globalincidentmap.com/
GmbH B (2003) Проверьте адреса электронной почты с помощью валидатора электронной почты byteplant.https://www.email-валидатор.сеть/
Google (2022a) Откройте для себя просмотр улиц и добавьте свои собственные изображения на карты Google.https://www.google.com/streetview. Доступ июль 2022 г.
Google (2022b) Карты Google.https://www.google.co.in/maps. По состоянию на июль 2022 г. Google (2022c)
Видео Google.https://www.google.com/videohp. По состоянию на июль 2022 г. GoogleImages (2022 г.)
Инструмент для изображений. https://images.google.com/. Доступ июль 2022 г.
Портал правительства США (2022 г.) предлагает бесплатный доступ к результатам исследований и разработок, а также научным данным.
Техническая и техническая информация от научных организаций 13 федеральных агентств.https://www.science.gov/. Доступ июль 2022 г.
Гундогду Э., Солмаз Б., Ючесой В. и др. (2016) Marvel: крупномасштабный набор данных изображений для морских судов.
сел. В: Азиатская конференция по компьютерному зрению. Спрингер, стр. 165–180.
Гупта Б.Б., Тевари А., Джайн А.К. и др. (2017) Борьба с фишинговыми атаками: современное состояние и будущее
вызовы. Приложение нейронных вычислений 28(12):3629–3654
Халеви Т., Льюис Дж., Мемон Н. (2013)Фишинг, личностные качества и Facebook. Препринт наhttp://arxiv.opr/абс/1301.7643
Харви (2022) Нейтринная обсерватория Садбери.https://sno.phy.queensu.ca/?phil%2Fexiftool%2F. Доступ июль 2022 г.
Хашида С., Тамура К., Сакаи Т. (2018) Классификация твитов, посвященных достопримечательностям, с использованием сверточной нейронной сети.
работает с многоканальным распределенным представлением. В: Международная конференция IEEE по системам,
человеку и кибернетике (SMC), 2018 г., IEEE. стр. 178–183
Хайден С. (2022 г.) Дом: библиотека Конгресса.https://www.loc.gov/. По состоянию на 16 сентября 2022 г. Эррера-Кубидес Х.Ф., Гаона-Гарсиа
П.А., Санчес-Алонсо С. (2020) Образовательные исследования в области разведки с открытым исходным кодом.
ресурсы: визуальный перспективный анализ. Прикладная наука 10(21):7617
Hexasoft (2001) IP-адрес для определения местоположения и информации о прокси-сервере.https://www.ip2location.com/
Хоссейнмарди Х., Мэттсон С.А., Ибн Рафик Р. и др. (2015). Анализ инцидентов, обозначенных как киберзапугивание, на
социальная сеть инстаграм. В: Международная конференция по социальной информатике. Springer, стр. 49–66 Ху Ю,
Хуан Х, Чен А и др. (2020) Weibo-cov: крупномасштабный набор данных социальных сетей о Covid-19 от Weibo.
Препринт наhttp://arxiv.org/abs/2005.09174
Imgur (2022) База данных трендовых изображений.https://imgur.com/. По состоянию на июль 2022 г. Каталог камер прямой трансляции
Insecam (2022 г.).http://www.insecam.org/. По состоянию на июль 2022 г. IpTRACKERonline (2010 г.). Полный анализ заголовка электронного
письма. Анализировать, отслеживать ip здесь.https://www.iptra
ckeronline.com/email-header-anaанализ.php
Ipverse (2022) Списки заблокированных адресов Ipv4/ipv6 по коду страны.https://xranks.com/ipverse.net. Доступ
июль 2022 г.
Ислам С., Бабар М.А., Крофт Р. и др. (2022) Smartvalidator: система автоматической идентификации и
классификация данных о киберугрозах. J Netw Comput Appl 202(103):370
Иватури К., Янчевски Л. (2011) Таксономия атак социальной инженерии
Джайн А.П., Данданнавар П. (2016)Применение методов машинного обучения для анализа настроений. В:
2016 2-я международная конференция по прикладным и теоретическим вычислительным и коммуникационным
технологиям (iCATccT), IEEE. стр. 628–632
Кадогути М., Кобаяши Х., Хаяши С. и др. (2020) Глубокая самоконтролируемая кластеризация даркнета
для разведки киберугроз. В: Международная конференция IEEE по разведке и информатике
безопасности (ISI), 2020 г., IEEE. стр. 1–6
Кале Б (1996) Цифровая библиотека интернет-сайтов и других культурных артефактов.https://archive.org/details/
Каккар А. (2020) Исследование методов безопасной связи в беспроводных гетерогенных сетях 5G.
Инфо-слияние 62: 89–109
Кандиас М., Грицалис Д., Ставру В. и др. (2017) Выявление уровня стресса с помощью модели использования OSN и хронического
ity анализ: модуль анализа угроз osint. Компьютерная безопасность 69:3–17
Као Д.Ю., Чао Ю.Т., Цай Ф и др. (2018)Аналитика цифровых доказательств, применяемая в расследованиях киберпреступлений. В:
Конференция IEEE 2018 по безопасности приложений, информации и сетей (AINS), IEEE. стр. 111–116 Катрин
Г.Дж.В., Прайз П.М., Роуз А.А. и др. (2019) Варианты фишинговых атак и технологии их обнаружения.
ники. В: 2019 3-я международная конференция по тенденциям в электронике и информатике (ICOEI), IEEE.
стр. 255–259
Кера Д.В. (2021) Введение в разведку с открытым исходным кодом (osint).https://журнал о киберзащите.com/an-introduction-to-open-source-intelligence-osint

Кравец Н. (2012) Фотокриминалистика предоставляет начинающим исследователям и профессиональным следователям доступ к передовые инструменты для криминалистики цифровых фотографий.http://fotoforensics.com/

Кромбхольц К., Хобель Х., Хубер М. и др. (2015) Продвинутые атаки социальной инженерии. Приложение J Inf Secur 22: 113–122

Кумар С., Гамильтон В.Л., Лесковец Дж. и др. (2018) Взаимодействие сообщества и конфликты в сети. В: Про-Итоги Всемирной веб-конференции 2018 года. стр. 933–943

Кумар А., Верма А., Шинде Г. и др. (2020)Прогнозирование преступности с использованием алгоритма k-ближайших соседей. В: 2020 Международная конференция по новым тенденциям в области информационных технологий и техники (IC-ETITE), IEEE. стр. 1–4

Кунджу М.В., Дайнел Э., Энтони Х.К. и др. (2019) Оценка методов фишинга на основе машинного обучения. инж. В: Международная конференция по интеллектуальным вычислениям и системам управления (ICCS), IEEE, 2019 г. стр. 963–968

Ланде Д.В., Шнурко-Табакова Е.В. (2019) Осинт как часть системы киберзащиты. Игорь Сикорский Киевский Политехнический институт, Киев

Lanzone J (2022) Видео Aol, предлагающее лучший видеоконтент из AOL и со всего Интернета.https://www.aol.ком/видео. Доступ июль 2022 г.

Ларсен Х.Л., Бланко Дж.М., Пастор Р.П. и др. (2017) Использование открытых данных для обнаружения угроз организованной преступности: факторы вождение будущей преступности. Спрингер, Нью-Йорк

Лоусон Дж. (2008) API поиска.https://www.twilio.com/lookup

Lead T (2004) Pipl собирает, перекрестно ссылается и связывает идентификационную информацию в Интернете.https://pipl.com/ Ляо Х, Юань К., Ван Х и др. (2016) Успех в игре ioc: на пути к автоматическому обнаружению и анализу информация о киберугрозах с открытым исходным кодом. В: Материалы конференции ACM SIGSAC 2016 г. по компьютерной и коммуникационной безопасности. стр. 755–766

ООО «АТ» (2009 г.) Исследует распространенность или необычность имен.http://howmanyofme.com/search/ Лоренц (1990) Крупнейшая в мире контейнерная площадка.https://www.prefixlist.com/

Lullar (2022) Lullar — поиск в профилях людей по адресу электронной почты или имени пользователя.http://com.lullar.com/. Доступ в июле 2022 год

Madars (2022) Ezgif — это бесплатный и простой в использовании набор инструментов, предназначенный в первую очередь для создания и редактирования.https://ezgif.com/обратное-видео. Доступ июль 2022 г.

Малхотра П., Сингх Й., Ананд П. и др. (2021 г.) Интернет вещей: эволюция, проблемы и проблемы безопасности. Датчики 21:1809

MapHub (2022 г.) Maphub создает интерактивные карты.https://maphub.net/. По состоянию на июль 2022 г.

Mapillary (2013 г.) Доступны изображения улиц и картографические данные.https://www.mapillary.com/

Mapquest (2022 г.) Геопространственные решения Mapquest с поддержкой определения местоположения.https://www.mapquest.com/. Доступ июль 2022 г.

MarineTraffic (2007) Глобальная разведка по отслеживанию судов: морское движение AIS.https://www.marinetraffic.com/ Марк С. (2004). Отчеты о мошенничестве, мошенничество по электронной почте, интернет-мошенничество, кража личных данных и бесплатный репозиторий фишинговых ресурсов. http://www.scamdex.com/

Marshall C (2018) Ведущий британский поставщик новостей, спортивных и развлекательных изображений.https://www.paimages.co.Великобритания/

Martin S (2007) Сервис Fail2ban-отчетов (отправляли отчеты об атаках на postfix, ssh, apache-атаки, спам-боты, irc-боты, reg-боты, ddos и многое другое) из Fail2ban через x-arf.http://www.blocklist.de/en/index.html

Мартин Дж., Мункгаард Р., Кумбер Р. и др. (2020) Продажа наркотиков на крипторынках дарквеба: дифференциация пути, риски и выгоды. Br J Criminol 60(3):559–578 MaxCDN (2016)

Мгновенный поиск по логотипу.http://instantlogosearch.com/

MaxMind (2002) Поиск географического местоположения по IP-адресу.http://www.ipfingerprints.com/ Макмиллан Л. (1997) Найдите людей, контактную информацию и проверку биографических данных.https://www.whitepages.com/

Media B (2006). Геолокация на основе IP — это отображение IP-адреса.https://www.iplocation.net/

Меир Н. (2013) Доступ к крупнейшим в мире коллекциям исторических и современных фотографий.http://www.apimages.com/

Metatube (2007) позволяет обмениваться видео и фотографиями и загружать их.http://www.metatube.com/ Карты Microsoft (2022a) Bing.https://www.bing.com/maps. Доступ к видео

Microsoft (2022b) Bing в июле 2022 г.https://www.bing.com/videos. Доступ июль 2022 г.

Миллер С., Риган М., Уолш П.Ф. (2022) Разведка и этика национальной безопасности. Тейлор и Фрэнсис, Кембридж, Мишра Р.К., Уролагин С. и др. (2019) Рекомендации отелям на основе анализа настроений с использованием подхода tf-idf. В: 2019 Международная конференция по вычислительному интеллекту и экономике знаний (ICCIKE), IEEE. стр. 811–815

MISP F (2021) Платформа анализа угроз с открытым исходным кодом Misp и открытые стандарты для информации об угрозах делиться

n2yo (2022) Спутниковое слежение в реальном времени.http://www.n2yo.com/. Доступ июль 2022 г.

NameCheckr (2022 г.) Namecheckr: поиск доступности социальных сетей и доменных имен для профессионалов бренда. https://www.namecheckr.com/. Доступ июль 2022 г.

NameChk (2009) Проверка имени пользователя и доменного имени — выполните поиск по всем доменным именам и именам пользователей, чтобы увидеть если они доступны.https://namechk.com/

Насим У, Хан С.К., Раззак И и др. (2019) Представление гибридных слов для анализа настроений авиакомпаний. В: Австралазийская совместная конференция по искусственному интеллекту. Спрингер, стр. 381–392.

Наза С., Худа С., Абаваджи Дж. и др. (2020) Эволюция анализа и обнаружения угроз даркнета: система атический подход. Доступ IEEE 8: 171796–171819.

Norby (2022) Онлайн-приложение для управления фотографиями и обмена ими.https://www.flickr.com/map. Доступ июль 2022 г.

Ноу М., Медсестра Дж.Р., Голдсмит М. (2016) На пути к созданию многоцелевой системы сбора данных о киберпреступлениях. рамки. В: Европейская конференция по разведке и информатике безопасности (EISIC), 2016 г., IEEE. стр. 60–67

Ноух М., Медсестра Дж.Р., Уэбб Х. и др. (2019) Следователи по киберпреступлениям тоже являются пользователями! понимание социально-технические проблемы, с которыми сталкиваются правоохранительные органы. Препринт наhttp://arxiv.org/abs/1902.06961 Некрологи (2022) Новости Санта-Барбары.https://newspress.com/. Доступ июль 2022 г.

Окерблум Дж. М. (2022) Страница онлайн-книг.https://onlinebooks.library.upenn.edu/. Доступ в июле 2022 год

Олиджук Т. (2022) Справочник журналов открытого доступа.https://doaj.org/. Доступ июль 2022 г.

Оманд Д., Бартлетт Дж., Миллер С. (2012) Знакомство с интеллектом социальных сетей (socmint). Интел Натл Секьюр 27 (6): 801–823

OpenStreetMap (2022) Расположение газет.https://newspapermap.com/. Доступ: июль 2022 г. Пол М. (2010 г.). Бесплатно подтвердите адрес электронной почты с помощью инструмента проверки электронной почты.https://www.verifyemailaddress.org/ PclMaps (2022 г.) Карты Pcl: Техасский университет в Остине.https://legacy.lib.utexas.edu/maps/. Доступ июль 2022 г.

PeekYou Developers (2006) Peekyou — поиск людей стал проще.https://www.peekyou.com/ PhoneLookup (2022) Поиск телефона.https://www.phonelookup.com/. По состоянию на июль 2022 г. Photobucket (2022 г.) Photobucket.http://photobucket.com/. Доступ июль 2022 г.

Пиента Д., Тэтчер Дж.Б., Джонстон А.С. (2018) Таксономия фишинга: типы атак, охватывающие экономику, временные, широтные и целевые границы

Pinkfroot (2012) Поиск судов работает, собирая данные с судов, используемых коммерческими судами и прогулочными судами. ремесло, чтобы передать свое имя, должность, ммси, статус и многое другое.https://shipfinder.co/

PlaneMapper (2022) Мировая база данных самолетов.http://www.planemapper.com/aircrafts. Доступ: июль 2022 г.

Погорелов К., Шредер Д.Т., Бурхард Л. и др. (2020 г.) Фейковые новости: вирус короны и задача заговора 5g на Medieval 2020. В: MediaEval.

Прабхакар Э., Сантош М., Кришнан А.Х. и др. (2019) Анализ настроений данных Твиттера американских авиакомпаний с использованием новый подход Aadaboost. Int J Eng Res Technol 7 (1): 1–6

Прасад Д.К., Раджан Д., Рахмавати Л и др. (2017)Обработка видео с электрооптических датчиков для Обнаружение и отслеживание объектов в морской среде: обзор. IEEE Trans Intell Transp Syst 18 (8): 1993–2016 гг.

Prince M (2004) Крупнейшее в Интернете сообщество, отслеживающее онлайн-мошенничество и злоупотребления, проект «Медовый горшок». https://www.projecthoneypot.org/

ProfileEngine (2022 г.) Profileengine.com.http://profileengine.com/. Доступ июль 2022 г.

Quick D, Choo KKR (2018) Цифровая судебная экспертиза: подмножества данных и разведка из открытых источников (dfint+osint): своевременная и связная смесь. Вычислительная система Futur Gener 78: 558–567

Радж С., Мил П. (2022) Люди лгут, а действия — нет! моделирование предикторов распространения инфодемии среди пользователи социальных сетей. Технол Сок 68(101):930

Раджамаки Дж., Симола Дж. (2019) Как обеспечить конфиденциальность в анализе osint и больших данных? В: ECCWS 2019 18-я Европейская конференция по кибервойне и безопасности, научные конференции и ограниченное количество публикаций. стр. 364

Растенис Дж., Раманаускайте С., Янулявичюс Дж. и др. (2020) Таксономия фишинговых атак на основе электронной почты. Приложение Наука 10(7):2363

Записи V (2022 г.) Записи актов гражданского состояния — свидетельства о рождении, записи о смерти, свидетельства о браке и многое другое.http://www.vitalrec.com/. Доступ июль 2022 г.

Reddit (2022 г.) Reddit — это дом для тысяч сообществ, бесконечных разговоров и подлинного человеческого общения. связь.https://www.reddit.com/domain/karmadecay.com/. По состоянию на июль 2022 г.

Reuters T (1993). Фотографии Reuters.http://pictures.reuters.com/

Ревелл К., Смит Т., Стейси Р. (2016)Инструменты для исследований на основе осинтов. Вышли: Ревелл К., Смит Т., Стейси Р. (ред.) Разведывательное расследование из открытых источников. Спрингер, Нью-Йорк, стр. 153–165.

ReverseImage (2011) Найдите изображения в Google и найдите фотографию в Интернете.http://www.reverse-image-search.com/
ReversePhoneLookup (2022) Обратный поиск телефона: поиск номера телефона.https://www.обратный поиск по телефону.ком/. Доступ июль 2022 г.
RGoogle (2022) Обратный поиск изображений.https://www.google.com/imghp. Доступ июль 2022 г.
Родди А.Л., Холт Т.Дж. (2022) Оценка наемных убийц и поставщиков насилия по контракту, действующих в Интернете. Деви-Поведение муравьев 43(2):139–151
Растин (2010) Отслеживание посылок «Все в одном».https://www.17track.net/en
Шнайдер В. (2022) Извлекает области из Planet.osm.https://extract.bbbike.org/. Доступ июль 2022 г.
Зейтц П. (2022) Изображения с камеры Livecam являются настоящим активом цифрового маркетинга, и ими можно делиться не только в Интернете.https://www.roundshot.com/xml_1/internet/en/intro.cfm?userlg=en. Доступ июль 2022 г.
Сенекал Б., Коце Э. (2019) Разведка из открытых источников (OSINT) для мониторинга конфликтов на современном Юге Африка: проблемы и возможности в контексте больших данных. Afr Secur Ред. 28 (1): 19–37
Шан Ю, Чжоу Х, Лю С и др. (2020) Siamfpn: метод глубокого обучения для точного морского судна в режиме реального времени отслеживание. IEEE Trans Circuits Syst Video Technol 31(1):315–325
Шестак В.А., Кощеева Д.А. (2021) Киберпреступность в условиях пандемии COVID-19: ключевые тенденции и пути решения Проблема Уголовной политики Российской Федерации в сфере обеспечения экономической безопасности Круглый стол (20 октября 2021 г.). Институт законодательства и сравнительного правоведения, Москва
Шуай Кью, Хуан Ю, Цзинь Л и др. (2018) Анализ настроений по отзывам китайских отелей с помощью doc2vec и classi-фейры. В: 2018 г. Третья конференция IEEE по передовым информационным технологиям, электронному и автоматическому управлению (IAEAC), IEEE. стр. 1171–1174
Синха Т., Чоудхури Т., Шоу Р.Н. и др. (2022) Анализ и прогнозирование подтвержденных случаев Covid-19 с использованием глубокого модели обучения: сравнительное исследование. В: Передовые вычисления и интеллектуальные технологии. Спрингер, стр. 207–218.
Смит (2019) Geosetter — это бесплатный инструмент для окон для отображения и изменения географических данных и других метаданных. http://www.geosetter.de/en
Смитрэ (2021) Исследование морских судов.https://wondersmithrae.medium.com/6-tips-for-investigating-морские суда-77e9c8bf75
SmugMugInc (2022 г.) Защищайте, делитесь, храните и продавайте свои фотографии.https://www.smugmug.com/. Доступ в июле 2022 год
Соомро З.Т., Ильяс ШВ, Якуб У (2020) Настроения, подсчет и случаи: анализ дискуссий в Твиттере во время COVID-19 пандемия. В: 2020 г. 7-я международная конференция по поведенческим и социальным вычислениям (BESC), IEEE. стр. 1–4
Спадон Г., Феррейра М.Д., Соарес А. и др. (2022) Развертывание поведения передачи AIS для режима движения судна. Работа с зашумленными данными с использованием машинного обучения. Доступ IEEE.https://doi.org/10.1109/ACCESS.2022.3197215
Стаффорд CD (2020 г.) Самое слабое звено: оценка факторов, влияющих на подверженность риску стать жертвой фишинга атаки и методы их смягчения. Кандидатская диссертация, Колледж Ютика
StartPage (2006) Стартовая страница — частная поисковая система. никакого отслеживания. Нет истории поиска.https://www.startpage.com/англ/video.html
Штиглиц С., Мирбабаи М., Росс Б. и др. (2018) Аналитика социальных сетей — проблемы обнаружения тем, сбора данных и подготовка данных. Int J Inf Manage 39: 156–168
Сулак Дж. (2005 г.) Крупнейшая в мире платформа отслеживания рейсов и данных.https://uk.flightaware.com/
Тандейл К.Д., Павар С.Н. (2020) Различные типы фишинговых атак и методы обнаружения: обзор. В: 2020 г. международная конференция по интеллектуальным инновациям в дизайне, окружающей среде, управлении, планировании и вычислениях (ICSIDEMPC), IEEE. стр. 295–299
Тан Х (2006) Поиск людей: белые страницы: обратный поиск по телефону.https://www.spokeo.com/
Technologies H (1997). Инструменты для исследования, изучения и устранения неполадок интернет-ресурсов, таких как домен. имена, IP-адреса, адреса электронной почты и URL-адреса.https://hexillion.com/
Thatsthem (2014) Найдите людей по имени: бесплатный поиск людей: Thatsthem.https://thatshem.com/people-search Томпсон С (2022) Отслеживайте и отслеживайте ваши отправления royal mail group ltd.https://www.royalmail.com/track-ваш предмет. Доступ июль 2022 г.
Tineye (2008) Обратный поиск изображений Tineye.http://www.tineye.com/ Track Trace (1998) Отслеживание авиагрузов.http://www.track-trace.com/aircargo
Trackingex (2022) Комплексное отслеживание посылок.https://www.trackingex.com/. По состоянию на июль 2022 г. TripGeo (2022 г.) Карта маршрутов с анимированным видом улиц.http://www.tripgeo.com/Directionsmap.aspx. Доступ июль 2022 г.
TruePeopleSearch (2022) Поиск настоящих людей.https://truepeoplesearch.io/. По состоянию на июль 2022 г. Truthfinder (2015 г.) Популярные инструменты поиска людей.https://www.truthfinder.com/
Команда поиска пользователей (2022) Найдите кого-то по имени пользователя или адресу электронной почты в социальных сетях, на сайтах знакомств, форумах, в криптовалюте. форумы, чаты и блоги. Поддерживается более 600+ сайтов! крупнейший обратный поиск пользователей в Интернете!https://поиск пользователей. org/lookups.php. Доступ июль 2022 г.
Геологическая служба США (2022) Исследователь Земли.https://eartheexplorer.usgs.gov/. Доступ июль 2022 г.

USP (2008) Лучший сайт для отслеживания посылок.https://www.packagetrackr.com/track/usps Utrace (2022) Найдите IP-адреса и доменные имена.http://en.utrace.de/. Доступ июль 2022 г.

Валлурипалли С., Сухеджа Д., Охри К. и др. (2019) Интеллектуальная система сигнализации для контроля багажа на базе Интернета. В: Международный конференция по Интернету вещей и подключенным технологиям. Спрингер, стр. 294–302.

Верма Д., Ярлагадда Р., Гартнер С. и др. (2019 г.) Понимание моделей терроризма в Индии (2007–2017 гг.) с использованием машинное обучение искусственного интеллекта. Int J Technol Knowl Soc 15(4):23–39 VesselFinder (2011)

Бесплатное средство отслеживания судов с бортовой системой навигации.https://www.vesselfinder.com/

ViaMichelin (2022) Планировщик маршрутов, карты, информация о пробках, отели.https://www.viamichelin.com/. Доступ в июле 2022 год

Вирджиния (2007 г.) Миссия — помочь людям обнаруживать, понимать и использовать общедоступные данные.https://www.beenverified.com/

VisualRightsGroup (2003) Дом.https://www.epa.eu/

Волза (2022 г.) Данные о мировой экспортно-импортной торговле 209 стран.https://www.volza.com/. По состоянию на июль 2022 г. VoPham T, Hart JE, Laden F et al (2018) Новые тенденции в геопространственном искусственном интеллекте (geoai): потенциал приложения для экологической эпидемиологии. Здоровье окружающей среды 17(1):1–6

Вакс С., Райт М.Ф., Вазсони А.Т. (2019) Понимание пересечения между киберзапугиванием и киберненавистью совершение преступлений: смягчение последствий токсичного онлайн-расторможения. Crim Behav Ment Health 29(3):179–188

Вадавадаги Р., Паги В. (2020) Анализ настроений с помощью глубоких нейронных сетей: сравнительное исследование и эффективность. Мансальная оценка. Artif Intell Ред. 53(8):6155–6195

Ван Ю, Лю Ю, Ву Т и др. (2020) Экономически эффективная реализация распознавания текста для предотвращения фишинга на мобильных платформах. В: Международная конференция по кибербезопасности и защите цифровых сервисов (Cyber Security) 2020 года, IEEE. стр. 1–8

Ван Й., Раджеш Г., Мерсилин Рааджини Х и др. (2021 г.) Обнаружение и отслеживание судов на основе машинного обучения с использованием спутниковые снимки для морского наблюдения. J Amb Intell Smart Environ 13:1–11 Webmii (2022 г.)

Открытая информация доступна в Интернете. http://webmii.com/. По состоянию на июль 2022 г. WiGLE (2001 г.)

Отображение беспроводной сети.https://wigle.net/

Уильямс Х.Дж., Блюм I (2018) Определение разведки с открытым исходным кодом второго поколения (OSINT) для оборонных предприятий. приз. Рэнд Корпорейшн, Санта-Моника

Уилсон Дж. (1960) Атлас короны и система ссылок.http://corona.cast.uark.edu/ Wise B (2008)

Проверьте имена пользователей.https://knowem.com/

Wolfram S (1987) Проект идентификации изображений на языке Wolfram.https://www.imageidentify.com/ Яду Р., Шукла Р. (2020)Метод сентиментальной классификации данных Твиттера для анализа услуг Indian Air Asia. Тех. представитель EasyChair

Yahoo (2022) Поиск видео Yahoo.https://video.search.yahoo.com/. По состоянию на июль 2022 г.

YahooImage (2022 г.) Поиск изображений Yahoo.http://images.yahoo.com/. По состоянию на июль 2022 г. Яндекс (2022 г.) Карты Яндекса.http://maps.yandex.com/. Доступ июль 2022 г.

ЯндексКартинки (2022) Поиск изображений в Интернете или поиск по изображению.https://yandex.com/images. Доступ в июле 2022 год

Ян Х, Ван Ю, Ван Н и др. (2022) Расширенная сеть siammask для отслеживания прибрежных судов. IEEE Транс Geosci Remote Sens 60: 1–11.https://doi.org/10.1109/TGRS.2021.3122330

Yasni G (2022) Yasni — бесплатная поисковая система, предназначенная для поиска людей в сети.http://www.yasni.com/. Доступ июль 2022 г.

Юань Х., Чжэн Дж., Йе Кью и др. (2021) Улучшение обнаружения фейковых новостей с помощью доменно-состязательного и графического внимания. нейронная сеть. Система поддержки Decis 151(113):633

Заррингхалам Н. (2009 г.) Лучшее в мире приложение для идентификации вызывающего абонента и блокировки спама.https://www.truecaller.com/ Чжан В., Хе Х, Ли В и др. (2021 г.) Надежная сеть глубокого взаимодействия для отслеживания нескольких судов. IEEE Транс Инструмент Meac 70:1–20.https://doi.org/10.1109/TIM.2021.3077679

Zlookup (2022). Найдите владельца любого мобильного или сотового телефона с помощью zlookup.https://www.zlookup.com/. Доступ июль 2022 г.

ZoomEarth (2022) Карта погоды в реальном времени, отслеживание штормов, радар дождя.https://zoom.earth/. Доступ июль 2022 г.