Научная статья

**OSINT В КИБЕРБЕЗОПАСНОСТИ. АНАЛИЗ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИИ ДЛЯ СБОРА И АНАЛИЗА ИНФОРМАЦИИ ИЗ ОБЩЕДОСТУПНЫХ ИСТОЧНИКОВ.**

OSINT IN CYBERSECURITY. ANALYSIS OF THE POSSIBILITY OF USING AI TO COLLECT AND ANALYZE INFORMATION FROM PUBLICLY AVAILABLE SOURCES.

**Мазлов Николай Евгеньевич,** студент, Казанский национальный исследовательский технологический университет, г. Казань (420015 Россия г. Казань, ул. Карла Маркса 68), pikzzzfckr@gmail.com

**Алексеева Анна Александровна,** доцент, Казанский национальный исследовательский технологический университет, г. Казань (420015 Россия г. Казань, ул. Карла Маркса 68), annank90@mail.ru

**Mazlov Nikolai Evgen’evich,** student, Kazan National Research Technological University, Kazan (420015 Russia Kazan, Karl Marx 68), pikzzzfckr@gmail.com

**Alekseeva Anna Alexandrovna,** docent, Kazan National Research Technological University, Kazan (420015 Russia Kazan, Karl Marx 68), annank90@mail.ru

**Введение**

Open Source Intelligence (OSINT) — это метод сбора информации из общедоступных или других открытых источников, который может быть использован экспертами по безопасности, национальными разведывательными агентствами или киберпреступниками. При использовании киберзащитниками цель состоит в том, чтобы обнаружить общедоступную информацию, относящуюся к их организации, которая может быть использована злоумышленниками, и принять меры для предотвращения таких атак в будущем. Основным источником информации, который нельзя упускать из виду, является огромное количество общедоступной информации (PAI), производимой потребителями, хакерами, ньюсмейкерами и блоггерами каждый день. Во всем мире почти каждый человек и организация взаимодействуют через несколько платформ и сетей, а также виртуально решают личные и корпоративные потребности, такие как покупки, планирование поездок и управление данными. Тем не менее, где бы ни собрались люди, особенно если есть потенциал для получения денежной выгоды, риск подлого поведения возрастает. Это создало повышенную потребность в OSINT-платформах. Вопрос всесторонней помощи обеспечивается поиском и своевременным предоставлением информации. Для этого предназначен OSINT, т.е. разведданные, синтезированные с использованием общедоступных данных. Анализируются цифровые следы, оставленные пользователями на открытых платформах, что может помочь найти геопозицию противника, его численность и прочую информацию. Исходя из этого, актуальность данной темы трудно переоценить в контексте современного информационного общества. Вот несколько подтверждающих аспектов:

Информационная перегрузка: В современном мире объем информации, доступной из общедоступных источников, становится все более огромным. Люди, компании и правительства сталкиваются с проблемой обработки этой информации и извлечения из нее ценных знаний. Использование ИИ для автоматизации этого процесса может значительно упростить и ускорить анализ.

Точность и эффективность: Использование алгоритмов машинного обучения и анализа данных позволяет проводить более точный и эффективный анализ больших объемов информации. ИИ может автоматически обрабатывать и классифицировать данные, выявлять скрытые паттерны и тенденции, что делает процесс анализа более глубоким и информативным.

Борьба с дезинформацией: В условиях распространения фейковых новостей, манипуляций информацией и дезинформации, использование ИИ для анализа общедоступных источников становится важным инструментом для выявления и фильтрации ложной информации. Автоматизированные системы могут помочь идентифицировать поддельные новости и недостоверные источники, что способствует поддержанию информационной безопасности.

Прогнозирование трендов и событий: Использование ИИ для анализа информации из общедоступных источников позволяет предсказывать возможные тренды, события и риски. Это может быть полезно как для бизнеса (прогнозирование спроса на товары и услуги), так и для правительственных структур (предотвращение кризисов и конфликтов). Развитие технологий искусственного интеллекта: С каждым годом технологии машинного обучения и анализа данных становятся все более продвинутыми и доступными. Новые алгоритмы и методы постоянно появляются, что позволяет создавать более эффективные системы сбора и анализа информации из общедоступных источников. Таким образом, анализ возможности использования ИИ для сбора и анализа информации из общедоступных источников является актуальной и перспективной темой, которая имеет широкие применения в различных областях деятельности.

Цель исследования "Анализ возможности использования искусственного интеллекта для сбора и анализа информации из общедоступных источников"

Для реализации цели были рассмотрены популярные инструменты поиска информации и оценена их эффективность и потенциал.

В сферу интересов OSINT входят получение и анализ официальных документов, проектов уставов, отслеживание новых научных разработок, баз данных, коммерческих и правительственных веб-сайтов, сетевых дневников и многое другое. Такая дисциплина дополняет уже существующие, но от этого не становится менее важной.

OSINT отличается от других форм сбора разведывательной информации несколькими особенностями, в том числе следующими: 1. OSINT ориентирован на общедоступную и легально доступную информацию, в то время как другие формы сбора разведданных могут включать конфиденциальные или секретные источники. 2. OSINT использует различные источники, включая социальные сети, новостные статьи, публичные записи и правительственные отчеты. В отличие от этого, другие формы сбора разведывательной информации могут быть сосредоточены на определенном типе источника. 3. OSINT часто включает в себя использование передовых аналитических методов, таких как обработка естественного языка и машинное обучение, для извлечения информации и информации из больших объемов данных. В отличие от этого, другие формы сбора разведывательной информации могут в большей степени полагаться на анализ и интерпретацию человеком. Сбор и анализ OSINT-информации, в конечном счете, будет оцениваться по ее вкладу в общую разведывательную деятельность. Сбор информации из открытых источников, как правило, менее затратен и менее рискован, чем сбор информации из других разведывательных источников. Использование OSINT может привести не только к экономии денежных средств, но и к меньшему риску, чем использование конфиденциальных технических и человеческих ресурсов.

На данный момент ИИ значительно облегчает поиск информации. Приведу пример нескольких таких инструментов ИИ.

Maltego. Maltego фокусируется на поиске конкретных взаимосвязей между активами, людьми, компаниями и доменами веб-сайтов.

Инструмент работает путем автоматизации поиска ваших данных по различным общедоступным источникам информации. Он управляет этими источниками данных с помощью так называемого «преобразования» и имеет довольно много встроенных функций. Некоторые из них — записи DNS, поиск в социальных сетях, проверки WHOIS и некоторые другие.

Usersearch. Usersearch — это обширная сеть поисковых систем, которые сканируют Интернет, чтобы найти точное совпадение по имени пользователя или адресу электронной почты. Он может найти конкретный профиль пользователя на форумах, в социальных сетях, на сайтах знакомств, досках объявлений. На сегодняшний день это одна из самых полных и точных поисковых систем в Интернете по именам пользователей и адресам электронной почты.

Intelligence x. Intelligence x — один из лучших архивных и поисковых сервисов, к которым у нас есть доступ в Интернете. Он не только архивирует исторические версии веб-сайтов в Интернете, но также включает утечку данных, которые в наши дни обычно удаляются довольно быстро.

Chat-GPT. Chat-GPT:

1. Может имитировать человека и поддерживать диалог;
2. Знает огромное количество информации из Интернета (её уже боится Google!);
3. Умеет писать стихи, песни и тексты компьютерных программ;
4. Пишет даже дипломные работы (которые успешно защищаются);
5. Создаёт за людей резюме и проходит тестовые задания;

Вы можете задавать Chat-GPT вопросы о конкретном человеке, компании или теме, и он ответит информацией, которую он собрал из общедоступных источников. Можно запросить у Chat-GPT последние новости по определенной теме, и он предоставит вам ссылки на соответствующие статьи и отчеты. Chat-GPT способен проанализировать данные из общедоступных источников и предоставить информацию, такую как тенденции, закономерности или корреляции. Вы можете попросить Chat-GPT генерировать отчеты по конкретным темам на основе собранной информации. Это может быть полезно для различных целей, таких как комплексная проверка, оценка рисков или аналитика угроз.

Рассмотрим поиск информации через инструмент Chat-GPT. Начнем с того, что цикл разведки можно представить в виде трёхлистника из бесконечной стрелки, показывающей основные этапы процесса: подготовку, сбор и обработку информации.


Следуем данной модели. На первом этапе подготовки нам нужно понять, что искать, где искать, а также составить краткий план действий.

Проще, когда есть четкое задание по поиску. Но что делать, когда вопрос ставится расплывчато? Например, как найти информацию о конкретном человеке в публичном доступе?



Хорошо, нейросеть выдала нам некоторые указания по поиску информации о человеке. Теперь спросим о конкретных источниках, где можно найти эту информацию.



Разумеется, можно и самому выполнить поиск инструментов и источников, но Chat-GPT сильно облегчает работу.

Также спросим у нейросети, сможет она сама найти и предоставить информацию о человеке или нет.



К сожалению, это противоречит принципам Chat-GPT.

Отлично. Следующий этап – сбор. Он включает в себя поиск, мониторинг и индексацию информации.

Попробуем воспользоваться каким-либо сайтом-источником данных и начнем в нем искать.



Что ж, иногда проще использовать браузер, либо конкретные сайты, в поиске информации на открытых источниках Chat-GPT еще не силен.

Перейдем к обработке. Предположим, что мы получили некоторые данные и хотим сделать вывод. Обратимся за помощью к нейросети.



Хорошо. Нейросеть даже выдала нам рекомендации, как действовать в такой ситуации. Итог, Chat-GPT в какой-то степени справляется с поверхностной аналитикой.

В заключение хочу сказать, что ИИ сильно облегчает процесс сбора и анализа информации из огромных объемов данных. Этот метод не только улучшает процесс принятия решений, но и обеспечивает более оперативное реагирование на изменения в окружающей среде. Внедрение таких систем может принести значительные выгоды в различных сферах деятельности, способствуя повышению эффективности и конкурентоспособности организаций

Источники:

1. Sentinel One company. What.(2019, June 17).Is Open Source Intelligence (OSINT).

https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/

1. Richard A., Best Jr., Cumming A..Open Source Intelligence (OSINT): Issues for Congress.СRS: report for

Congress. https://sgp.fas.org/crs/intel/RL34270.pdf

1. Imperva company.(2022, September 20). Open-Source Intelligence (OSINT).

https://www.imperva.com/learn/application-security/open-source-intelligence-osint/

1. Guise Bule.(2020). A Guide To Open Source Intelligence (OSINT).https://itsec.group/blog-post-osint-guidepart-1.html
2. Nihad Hassan.(2018, August 12). An Introduction To Open Source Intelligence (OSINT) Gathering.

https://www.secjuice.com/introduction-to-open-source-intelligence-osint/

1. Hamilton, B. The DNI’s Open Source Center: An Organizational Communication Perspective / B. Hamilton //

International Journal of Intelligence and CounterIntelligence [Electronic resource]. – Access mode:

http://www.oss.net/dynamaster/file\_archive/ 110802/9853247889921643

2d3d76e2f9d4534c/20110802%20Dr.%20Bean%20IJIC%20Open%20Source%20Center.pdf

1. Electronic encyclopedia Wikipedia. [Electronic resource]. – Access mode: http://en.wikipedia.org/wiki/

Foreign\_Broadcast\_Information\_Service

1. Open Source Intelligence, U.S. Army Field Manual Interim FMI 2-22.9, December 2006 [Electronic resource].

– Access mode: www.fas.org/irp/ doddir/ army/ fmi2-22-9.pdf

1. Electronic encyclopedia Wikipedia. [Electronic resource]. – Access mode: http://en.wikipedia.org/wiki/

Director\_of\_National\_Intelligence