Куликова А.В., Богословский Ф.И. Анализ цифровых следов и средств расследования в области киберпреступности // Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 4(42) с. 56–62

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

АНАЛИЗ ЦИФРОВЫХ СЛЕДОВ И СРЕДСТВ РАССЛЕДОВАНИЯ В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ

[1]Куликова А.В. , **[2]Богословский Ф.И.**
ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: [1]kagamine_2000@mail.ru, [2]f3dorasta@gmail.com

Настоящая научная статья посвящена анализу цифровых следов и средств расследования в области киберпреступности. В современном информационном обществе киберпреступность становится все более распространенной и серьезной угрозой. Цифровые следы, оставленные преступниками в сети, представляют собой ценный источник информации для правоохранительных органов и специалистов по кибербезопасности.

Статья рассматривает методы анализа цифровых следов, включая техники сбора и обработки данных, а также инструменты для выявления и атрибуции киберпреступных действий. Особое внимание уделяется использованию машинного обучения и искусственного интеллекта в процессе анализа цифровых следов, что позволяет повысить эффективность и точность расследования.

Исследование также охватывает актуальные проблемы и вызовы, с которыми сталкиваются специалисты по кибербезопасности при работе с цифровыми следами. В заключение, статья делает выводы о значимости дальнейших исследований в области анализа цифровых следов и развитии средств расследования для борьбы с киберпреступностью.

Ключевые слова: Цифровые следы, киберпреступность, расследование, машинное обучение, искусственный интеллект, кибербезопасность.

ANALYSIS OF DIGITAL TRACES AND INVESTIGATIVE TOOLS IN THE FIELD OF CYBERCRIME

[1]Kulikova A.V., [2]Bogoslovsky F.I.
BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia (105005, Moscow, 2nd Baumanskaya str., 5/1), e-mail: [1]kagamine_2000@mail.ru, [2]f3dorasta@gmail.com

This scientific article is devoted to the analysis of digital traces and investigative tools in the field of cybercrime. In today's information society, cybercrime is becoming an increasingly common and serious threat. Digital traces left by criminals online provide a valuable source of information for law enforcement and cybersecurity professionals.

The article examines methods for analyzing digital traces, including techniques for collecting and processing data, as well as tools for identifying and attributing cybercriminal actions. Particular attention is paid to the use of machine learning and artificial intelligence in the process of analyzing digital traces, which makes it possible to increase the efficiency and accuracy of the investigation.

The study also covers current issues and challenges faced by cybersecurity professionals when dealing with digital footprints. In conclusion, the article draws conclusions about the significance of further research in the field of digital trace analysis and the development of investigative tools to combat cybercrime.

Keywords: Digital footprints, cybercrime, investigation, machine learning, artificial intelligence, cybersecurity.

Введение

В современном информационном обществе киберпреступность становится все более острой и актуальной проблемой, представляя серьезную угрозу для безопасности как государственных структур, так и обычных граждан. Киберпреступники все чаще используют цифровые технологии для осуществления атак на информационные системы, кражи конфиденциальных данных и финансовых средств, а также для совершения других противоправных действий в сети.

Одним из ключевых аспектов борьбы с киберпреступностью является анализ цифровых следов, оставленных преступниками в процессе совершения противоправных действий. Цифровые следы могут содержать ценную информацию о методах атаки, идентификации преступников, их мотивах и связях. Правильный анализ этих следов позволяет выявить уязвимости в системе безопасности, предотвратить новые атаки и привлечь к ответственности злоумышленников.

Целью данного исследования является рассмотрение современных методов анализа цифровых следов и средств расследования в области киберпреступности. Мы стремимся изучить техники сбора и обработки данных, применяемые при анализе цифровых следов, а также рассмотреть возможности использования машинного обучения и искусственного интеллекта для улучшения эффективности расследования. Кроме того, мы намерены выявить актуальные проблемы и вызовы, с которыми сталкиваются специалисты по кибербезопасности при работе с цифровыми следами, и предложить пути их решения.

Теоретические основы анализа цифровых следов

Цифровые следы **[1]** представляют собой информацию, оставленную в цифровой форме в процессе взаимодействия человека с компьютерными системами, мобильными устройствами, интернет-сервисами и другими электронными средствами. Эти следы могут включать в себя данные о действиях пользователя, его посещениях в сети, использованных программных средствах и многое другое. Анализ цифровых следов направлен на извлечение ценной информации из этих данных для целей

Методы сбора и анализа данных

*Сбор данных***.** [2] Для успешного анализа цифровых следов необходимо правильно собирать данные. Это может включать в себя использование специализированных инструментов для извлечения информации с компьютеров, мобильных устройств, сетевых устройств и других источников. Также важно сохранить целостность данных и обеспечить их безопасность во время сбора.

*Обработка данных***.** После сбора данных необходимо провести их обработку для выделения ключевой информации. Это может включать в себя фильтрацию, структурирование, классификацию и агрегацию данных. Техники обработки данных могут зависеть от конкретных задач расследования.

Анализ данных. [3] После обработки данные подвергаются анализу с целью выявления закономерностей, связей и паттернов, которые могут помочь в раскрытии киберпреступлений.

В этом этапе могут применяться методы статистического анализа, машинного обучения, искусственного интеллекта и другие техники.

Визуализация данных. [4] Для наглядного представления результатов анализа цифровых следов часто используется визуализация данных. Это позволяет лучше понять структуру информации, выделить ключевые элементы и обнаружить скрытые закономерности.

Методы анализа цифровых следов

Цифровые следы, оставленные пользователями в сети, представляют собой богатый источник информации для расследования киберпреступлений [5]. Для анализа цифровых следов используются различные методы и техники, позволяющие извлечь ценные данные и выявить закономерности. Ниже приведены основные методы анализа цифровых следов с примерами использования.

1. *Анализ IP-адресов.* Анализ IP-адресов позволяет идентифицировать и отслеживать действия конкретного пользователя в сети. Путем анализа IP-адресов можно определить местоположение пользователя, его интернет-провайдера, использованные устройства и другую важную информацию.

Пример использования: при расследовании киберпреступлений анализ IP-адресов может помочь выявить источник атаки, идентифицировать злоумышленника и связать его с конкретными действиями в сети.

2. *Анализ метаданных*. Метаданные содержат информацию о данных, например, дату создания, автора, местоположение и другие атрибуты. Анализ метаданных позволяет получить дополнительные сведения о файле или сообщении.

Пример использования: при расследовании утечек информации анализ метаданных файлов может помочь определить источник утечки, автора документа или дату его создания.

3. *Анализ социальных сетей*. Анализ социальных сетей позволяет изучить взаимосвязи между пользователями, их активность в сети, интересы и другие данные. Этот метод широко используется для выявления связей между участниками киберпреступных группировок.

Пример использования: при расследовании организованных преступных группировок анализ социальных сетей может помочь выявить лидеров, участников и структуру группы.

4. *Анализ шаблонов поведения*. Анализ шаблонов поведения пользователей в сети позволяет выявить аномалии или необычные действия, которые могут указывать на потенциальные киберпреступления.

Пример использования: при мониторинге корпоративных сетей анализ шаблонов поведения может помочь обнаружить несанкционированный доступ к данным или другие безопасностные инциденты.

Успешные примеры расследований с использованием анализа цифровых следов

В современном цифровом мире, где киберпреступности становятся все более изощренными и сложными, анализ цифровых следов играет ключевую роль в расследованиях преступлений и обеспечении кибербезопасности. Эффективное использование технологий и методов анализа данных позволяет специалистам по кибербезопасности выявлять источники угроз, идентифицировать уязвимости и предотвращать потенциальные атаки. Далее

представлены успешные примеры расследований, в которых анализ цифровых следов сыграл ключевую роль в раскрытии преступлений и защите информационной безопасности.

1. *Расследование хакерской атаки на крупную финансовую организацию*. Специалисты по кибербезопасности провели анализ цифровых следов после того, как крупная финансовая компания стала жертвой масштабной хакерской атаки. Путем анализа IP-адресов, метаданных и шаблонов поведения удалось выявить источник атаки, идентифицировать использованные вредоносные программы и определить механизмы взлома. Эти данные помогли компании укрепить свою кибербезопасность и предотвратить будущие атаки.

2. *Расследование киберпреступления с использованием анализа социальных сетей.* Специалисты по киберпреступности провели расследование организованной преступной группировки, занимавшейся финансовыми мошенничествами через интернет. Путем анализа социальных сетей удалось выявить связи между участниками группировки, определить роли каждого участника и выявить способы общения и координации действий. Эта информация послужила основой для успешного задержания и судебного преследования участников группировки.

3. *Расследование утечки конфиденциальной информации в корпоративной среде*. Компания столкнулась с утечкой конфиденциальных данных, что привело к серьезным финансовым потерям. Специалисты по кибербезопасности провели анализ метаданных файлов, перехваченных сотрудниками компании, и выявили источник утечки. Также был проведен анализ шаблонов поведения сотрудников, что позволило выявить необычные действия, приведшие к утечке данных. Благодаря этим данным компания смогла усилить свои меры безопасности и предотвратить дальнейшие утечки.

Программное обеспечение для анализа цифровых следов

В настоящее время существует широкий спектр программных инструментов и технологий **[6]**, специально разработанных для анализа цифровых следов и проведения расследований в области киберпреступности. Эти инструменты позволяют идентифицировать угрозы, анализировать данные, восстанавливать информацию и выявлять уязвимости в информационных системах. Ниже представлен обзор некоторых из наиболее популярных программных средств, используемых в данной области:

1. EnCase Forensic. Это одно из ведущих программных решений для цифрового расследования, которое предоставляет возможности по сбору, анализу и представлению цифровых данных. EnCase Forensic **[7]** позволяет проводить глубокий анализ файловой системы, реестра Windows, интернет-активности и других источников данных.

2. Autopsy. Это бесплатное и открытое программное обеспечение для цифрового расследования, основанное на платформе Sleuth Kit. Autopsy **[8]** предоставляет широкий спектр функций, включая анализ жестких дисков, извлечение метаданных файлов, восстановление удаленных файлов и многое другое.

3. X-Ways Forensics. Это мощное программное обеспечение для цифрового расследования, которое обладает широкими возможностями по анализу данных. X-Ways Forensics **[9]** позволяет проводить детальный анализ файловой системы, реестра Windows, структуры файлов и многое другое.

4. *Cellebrite UFED.* Это инструмент для извлечения данных с мобильных устройств, который широко используется в цифровых расследованиях. Cellebrite UFED **[10]** позволяет получать данные смартфонов, планшетов и других мобильных устройств, а также проводить анализ извлеченных данных.

Эти программные инструменты представляют лишь небольшую часть доступных на рынке средств для анализа цифровых следов в области киберпреступности. При выборе инструментов для проведения расследований необходимо учитывать особенности конкретной задачи, требования к безопасности данных и доступные ресурсы. Важно также следить за развитием технологий и выбирать инструменты, соответствующие последним трендам в области кибербезопасности.

Этические аспекты

Использование анализа цифровых следов для расследования киберпреступности поднимает ряд этических вопросов, которые необходимо учитывать при проведении исследований в данной области. Некоторые из ключевых этических аспектов, связанных с использованием анализа цифровых следов для расследования киберпреступности, включают следующее:

1. *Приватность и конфиденциальность данных*. При проведении анализа цифровых следов необходимо учитывать права и интересы частных лиц, чьи данные могут быть собраны и использованы в рамках расследования. Важно обеспечить защиту конфиденциальности информации и соблюдать законодательство о защите данных.
2. *Соблюдение процедур и стандартов***.** При использовании средств анализа цифровых следов необходимо соблюдать установленные процедуры и стандарты, чтобы обеспечить точность и надежность результатов расследования. Нарушение процедур может привести к неправомерному использованию данных и ошибочным выводам.
3. *Принцип пропорциональности***.** При сборе и анализе цифровых следов необходимо соблюдать принцип пропорциональности, то есть использовать только необходимую информацию для достижения целей расследования. Избегание излишнего сбора и использования данных поможет минимизировать нарушение приватности.
4. *Ответственность и честность***.** Использование анализа цифровых следов для расследования киберпреступности требует от исследователей высокой степени ответственности и честности. Важно представлять результаты анализа точно и объективно, а также соблюдать этические нормы при работе с данными и участием в процессе расследования.

Эти этические аспекты играют важную роль в обеспечении справедливости, законности и эффективности процесса расследования киберпреступности с использованием анализа цифровых следов. Понимание и учет этических проблем помогут исследователям и специалистам в области кибербезопасности проводить свою работу в соответствии с принципами этики и законности.

Заключение

В ходе исследования была обсуждена значимость анализа цифровых следов и средств расследования в области киберпреступности. Было выявлено, что использование анализа

цифровых следов позволяет эффективно выявлять, анализировать и пресекать киберпреступные деяния, что является критически важным в современном цифровом мире.

Также были обсуждены несколько ключевых этических аспектов, связанных с использованием анализа цифровых следов для расследования киберпреступности, и подчеркнута важность соблюдения принципов приватности, конфиденциальности данных, процедур и стандартов, пропорциональности, ответственности и честности при работе в этой области.

Для дальнейших исследований в области анализа цифровых следов и средств расследования киберпреступности рекомендуется углубленное изучение методов и технологий анализа данных, разработка новых инструментов для выявления и предотвращения киберпреступности, а также проведение дополнительных исследований по этическим аспектам использования цифровых следов в расследованиях.

Список литературы

1. Семикаленова А. И. Цифровые следы: назначение и производство экспертиз //Вестник университета имени ОЕ Кутафина. – 2019. – №. 5 (57). – С. 115-120.
2. Цветков В. Я. Сбор данных и информации //Международный журнал прикладных и фундаментальных исследований. – 2016. – №. 4-3. – С. 646-647.
3. Мхитарян В. С. и др. Анализ данных //Учебник. М: Бакалавр. Академический курс (1-е изд.), Сер. – 2016. – Т. 58.
4. Нефедьева К. В. Инфографика визуализация данных в аналитической деятельности //Труды Санкт-Петербургского государственного института культуры. – 2013. – Т. 197. – С. 89-93.
5. Шевченко Е. С. Актуальные проблемы расследования киберпреступлений //Эксперт-криминалист. – 2015. – №. 3. – С. 29-30.
6. Тихобаев А. Г. Интерактивные компьютерные технологии обучения //Вестник Томского государственного педагогического университета. – 2012. – №. 8 (123). – С. 81-84.
7. Bunting S., Wei W. EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide. – John Wiley & Sons, 2006.
8. Burton J. L., Underwood J. Clinical, educational, and epidemiological value of autopsy //The Lancet. – 2007. – Т. 369. – №. 9571. – С. 1471-1480.
9. Rosalina V., Suhendarsah A., Natsir M. Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic //PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer. – 2016. – Т. 3. – №. 1.
10. Jain P., Mishra A. Extraction of Data using Cellebrite UFED 4PC //International Journal of Medical Toxicology & Legal Medicine. – 2023. – Т. 26. – №. 3and4. – С. 222-232.

References

1. Semikalenova A. I. Digital traces: purpose and production of examinations // Bulletin of the University named after OE Kutafin. – 2019. – No. 5 (57). – pp. 115-120.
2. Tsvetkov V. Ya. Collection of data and information // International Journal of Applied and Fundamental Research. – 2016. – No. 4-3. – pp. 646-647.

3. Mkhitaryan V.S. et al. Data analysis // Textbook. M: Bachelor. Academic Course (1st ed.), Ser. – 2016. – T. 58.
4. Nefedeva K.V. Infographics, data visualization in analytical activities // Proceedings of the St. Petersburg State Institute of Culture. – 2013. – T. 197. – pp. 89-93.
5. Shevchenko E. S. Current problems in the investigation of cybercrimes // Expert criminologist. – 2015. – No. 3. – pp. 29-30.
6. Tihobaev A. G. Interactive computer teaching technologies // Bulletin of Tomsk State Pedagogical University. – 2012. – No. 8 (123). – pp. 81-84.
7. Bunting S., Wei W. EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide. – John Wiley & Sons, 2006.
8. Burton J. L., Underwood J. Clinical, educational, and epidemiological significance of autopsy // The Lancet. – 2007. – T. 369. – No. 9571. – pp. 1471-1480.
9. Rosalina V., Suhendarsah A., Natsir M. Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic //PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer. – 2016. – T. 3. – No. 1.
10. Jain P., Mishra A. Extraction of Data using Cellebrite UFED 4PC //International Journal of Medical Toxicology & Legal Medicine. – 2023. – T. 26. – No. 3and4. – pp. 222-232.