


Евразийский национальный университет имени Л.Н. Гумилева
Национальная инженерная академия РК
Казахский национальный педагогический университет имени Абая, Казахстан
Институт математики и математического моделирования КН МВНО, Казахстан
Институт информационных и вычислительных технологий КН МВНО, Казахстан
Международный математический центр ИМ им. С.Л. Соболева СО РАН, Россия
Российский национальный комитет по индустриальной и прикладной математике, Россия
ОФ «Международный фонд обратных задач», Казахстан
Математическое Общество Тюркского Мира.

ЕУРАЗИЯЛЫҚ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ
ЕВРАЗИЙСКАЯ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«ҒЫЛЫМДАҒЫ, ТЕХНИКА МЕН ИНДУСТРИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ КЕРІ ЕСЕПТЕР»

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБРАТНЫЕЗАДАЧИ В НАУКЕ, ТЕХНИКЕ И ИНДУСТРИИ»

«ARTIFICIAL INTELLIGENCE AND INVERSE PROBLEMS IN SCIENCE, TECHNOLOGY AND INDUSTRY»

ЕҢБЕКТЕРІ ТРУДЫ PROCEEDINGS

Астана
14-16 апреля 2025 г.

УДК 004.896:001(082)

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian internationalscientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

ISBN 978-601-385-052-8

Еуразиялық халықаралық ғылыми конференция «Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер» баяндамалар жинағы. 14-16 сәуір 2025 жыл.

Сб. докл. Евразийской международной научной конференций «Искусственный интеллект и обратные задачи в науке, технике и индустрии» 14-16 апрель 2025 год.

Collection of reports the Eurasian internationalscientific conference «Artificial intelligence and inverse problems in science, technology and industry»

– Астана: Л.Н. Гумилев атын. Еуразия ұлттық университеті, 2025. – 451 б. – қазақша, орысша, ағылшынша.

1 СЕКЦИЯ . «КЕРІ ЕСЕПТЕРДІ ШЕШУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ»

СЕКЦИЯ 1. «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ОБРАТНЫХ ЗАДАЧ»

SECTION 1. «ARTIFICIAL INTELLIGENCE IN SOLVING INVERSE PROBLEMS»

2 СЕКЦИЯ «КЕРІ ЖӘНЕ ДҰРЫС ҚОЙЫЛМАҒАН ЕСЕПТЕРДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ЕСЕПТЕУ АСПЕКТІЛЕРІ»

СЕКЦИЯ 2 «ТЕОРЕТИЧЕСКИЕ И ВЫЧИСЛИТЕЛЬНЫЕ АСПЕКТЫ ОБРАТНЫХ И НЕКОРРЕКТНЫХ ЗАДАЧ»

SECTION 2 «THEORETICAL AND COMPUTATIONAL ASPECTS OF INVERSE AND ILL-POSITIONED PROBLEMS»

3 СЕКЦИЯ «АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖӘНЕ ЕСЕПТЕУ ИНТЕЛЛЕКТІСІ

3 СЕКЦИЯ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ»

SECTION 3 «INFORMATION TECHNOLOGY AND COMPUTATIONAL INTELLIGENCE»

4 СЕКЦИЯ «КРИПТОГРАФИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕК ЖӘНЕ КИБЕРҚАУІПСІЗДІК»

4 СЕКЦИЯ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ»

SECTION 4 "ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY AND CYBERSECURITY"

қуатты құралы болып табылады. Бұл оқытудың қызықты тәсілі ғана емес, сонымен қатар қатысушыларға киберқауіптермен күресуге жалпы біліктілік пен дайындықты арттыра отырып, нақты жағдайларда өз қабілеттерін дамытуға, сынауға және жетілдіруге мүмкіндік беретін тиімді әдіс. Жыл сайын CTF ойындарының танымалдығы артып келеді және көптеген ұйымдар бұл әдісті өз қызметкерлерін даярлау үшін, сондай-ақ жалпы хабардарлық пен қауіпсіздік деңгейін арттыру үшін қолдана бастайды.

Қолданылған әдебиеттер тізімі

1. Leune K., Petrilli Jr S. J. Using capture-the-flag to enhance the effectiveness of cybersecurity education //Proceedings of the 18th annual conference on information technology education. – 2017. – С. 47-52.
2. Hanafi A. H. A. et al. A CTF-based approach in cyber security education for secondary school students //electronic Journal of Computer Science and Information Technology. – 2021. – Т. 7. – №. 1.
3. Al-Karaki J. N. et al. Advancing cybersecurity education and training: Practical case study of running capture the flag (ctf) on the metaverse vs. physical settings //2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA). – IEEE, 2023. – С. 1-7.

Тұрсыналы А. Б. студент III курса
образовательной программы 6B06306
«Системы информационной безопасности»,
Евразийский национальный университет
им. Л.Н. Гумилева
Научный руководитель Аймичева Г.И.

МЕТОДЫ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В современном мире информация является одним из самых ценных ресурсов. Конфиденциальные данные компаний, государственных структур и частных лиц находятся под постоянной угрозой компрометации. В условиях глобальной цифровизации, удаленной работы и активного использования облачных сервисов традиционные механизмы защиты часто оказываются недостаточными. Утечки конфиденциальной информации могут иметь катастрофические последствия: от финансовых потерь и потери доверия клиентов до уголовной ответственности и угрозы национальной безопасности. Они могут происходить как в результате преднамеренных действий (кибератаки, шпионаж, инсайдерские угрозы), так и по неосторожности сотрудников или технических сбоев.

Чтобы выявлять источники утечек, определять масштабы ущерба и предотвращать повторные инциденты, специалисты в области информационной безопасности используют криминалистический анализ данных[1]. Это комплекс методов, направленный на детальное изучение цифровых следов, анализ логов, восстановление удаленных данных и сбор доказательств для дальнейшего разбирательства. В данной статье рассмотрены основные

методы криминалистического анализа утечек информации, их принципы работы и роль в расследовании киберинцидентов.

Перед тем как углубляться в методы криминалистического анализа, необходимо разобраться с основными способами утечки данных. Они могут происходить по разным причинам, но в целом делятся на три основные категории:

1. Преднамеренные (злонамеренные) утечки

Этот тип утечек связан с умышленными действиями злоумышленников, направленными на получение, копирование или передачу конфиденциальной информации. Среди них:

✓ Инсайдерские угрозы – передача данных конкурентам, шантаж, финансовая выгода сотрудников.

✓ Кибератаки – целевые атаки со стороны хакеров, направленные на кражу данных.

✓ Использование вредоносного ПО – кейлоггеры, трояны, бэкдоры, предназначенные для сбора информации.

2. Непреднамеренные утечки

В этом случае данные становятся доступными для посторонних из-за случайных ошибок или небрежности пользователей:

✓ Ошибка сотрудников – отправка конфиденциальных файлов не тому адресату.

✓ Публикация данных в открытых источниках – случайное размещение закрытой информации в интернет-ресурсах.

✓ Потеря или кража носителей информации – забытые или украденные USB-накопители, ноутбуки, мобильные устройства.

3. Технические утечки

Этот вид утечек связан с уязвимостями и ошибками в информационных системах:

✓ Эксплуатация уязвимостей ПО – использование ошибок в защите баз данных, серверов или приложений.

✓ Перехват данных в сетях – атаки типа Man-in-the-Middle (MITM), подмена DNS, незащищенные соединения.

✓ Использование закладок и бэкдоров – скрытые механизмы удаленного доступа, встроенные злоумышленниками.

Каждый из этих типов утечек требует индивидуального подхода к расследованию и внедрения превентивных мер защиты. Криминалистический анализ утечек информации включает несколько основных направлений:

1. Анализ цифровых следов и логов. Любая цифровая деятельность оставляет следы в операционной системе, сетевых устройствах и приложениях[2]. Анализ этих следов позволяет выявить источник утечки и восстановить цепочку событий.

1.1. Анализ лог-файлов

Лог-файлы фиксируют все ключевые события в системе: входы пользователей, изменения в файлах, сетевые подключения.

1.2. Анализ сетевого трафика

Если данные передавались через интернет или корпоративную сеть, анализ сетевого трафика может помочь выявить их утечку. Пример инструментов:

- Wireshark – анализатор сетевого трафика.
- Zeek (Bro) – система сетевой безопасности.

2. Расследование утечки данных: анализ веб-активности. Одним из ключевых методов выявления утечки данных является анализ веб-активности подозреваемого[3]. Это позволяет определить, какие ресурсы использовались для возможной утечки данных.

Методы выявления:

- Изучение истории браузеров – анализ временных меток посещений, URL-адресов, загруженных файлов (рис.1).

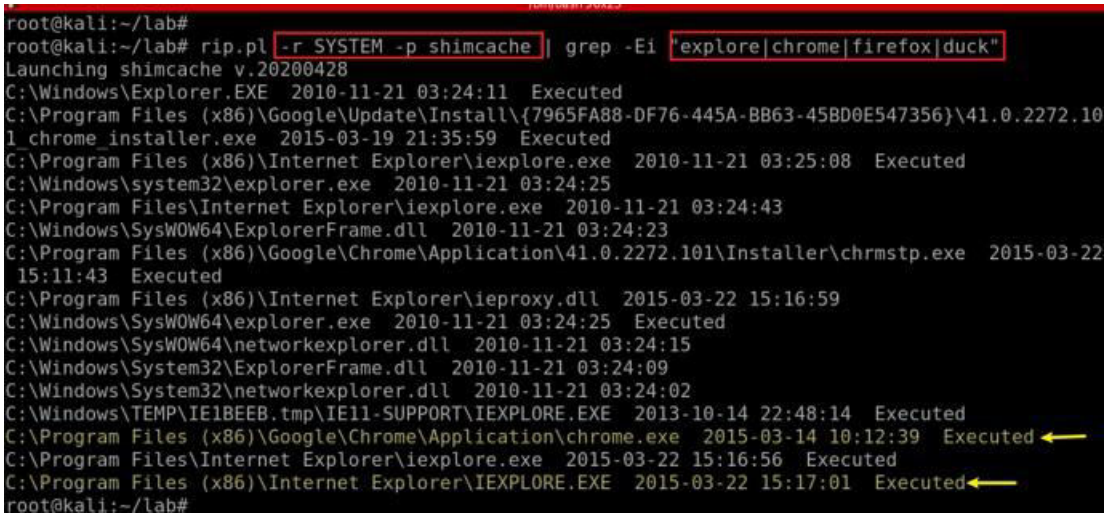

Рисунок 1. Через реестр находим все возможные браузеры (версии), которыми пользовались подозреваемые.

- Форензика кэша браузера – проверка временных файлов, cookie, сохранённых данных автозаполнения.
- Мониторинг сетевого трафика – перехват подозрительных соединений и утечек данных через файлообменные сервисы или мессенджеры.
- Анализ DNS-запросов – выявление посещения подозрительных веб-ресурсов, связанных с утечкой данных.

Пример инструментов для анализа:

- Browser History Examiner – анализ истории браузеров.
- Hindsight – форензика браузеров Google Chrome.
- X1 Social Discovery – исследование активности в социальных сетях.

Просмотр истории Google Chrome через SQLite позволяет получить подробные данные о веб-активности пользователя. Chrome хранит историю посещений в базе данных SQLite в файле `History`. Для анализа необходимо закрыть браузер и скопировать файл `C:\Users\Аружан\AppData\Local\Google\Chrome\User Data\Default\History`. Затем

этот файл открывается в SQLite Browser или через командную строку. Запрос `SELECT datetime(last_visit_time/1000000-11644473600, 'unixepoch') AS visit_time, url FROM urls ORDER BY last_visit_time DESC;` выводит список посещенных сайтов с
временными метками. Также можно проанализировать загруженные файлы, выполнив запрос `SELECT datetime(start_time/1000000-11644473600, 'unixepoch') AS download_time, target_path FROM downloads;`. Эти методы позволяют детально исследовать веб-активность подозреваемого, выявить подозрительные действия и установить возможные источники утечек информации(рис 2.).

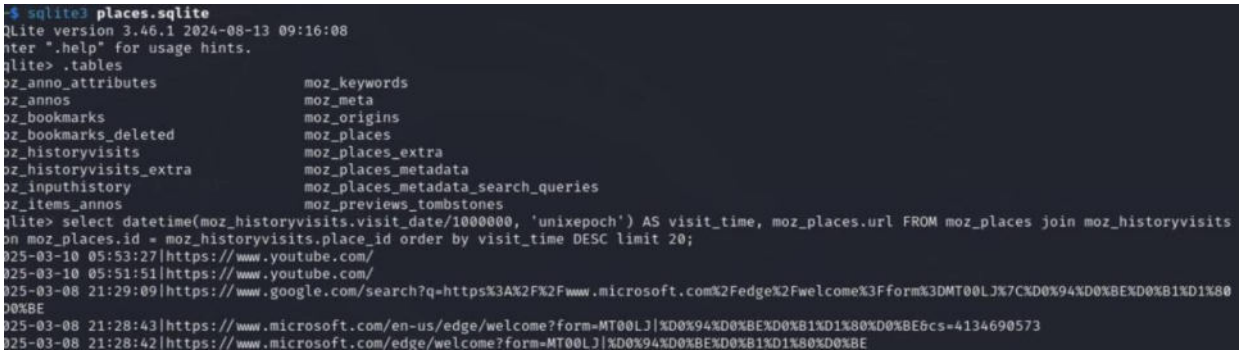

Рисунок 2. Просмотр истории Chrome SQLite

В завершении стоит отметить, что процесс криминалистического анализа утечек
данных требует не только технических знаний, но и внимательности, системного подхода и умения работать с доказательствами. Сочетание передовых технологий анализа, строгих процедур безопасности и постоянного мониторинга позволяет значительно снизить риски утечек и минимизировать их последствия. Кроме того, профилактические меры, такие как контроль доступа, шифрование данных и обучение персонала, играют ключевую роль в защите информации и предотвращении возможных инцидентов.

Список использованных источников:

1. *Zhang, Q., & Wang, L. (2022). Enhancing Online Testing Security: A Review of Proctoring Solutions. Journal of Information Technology in Education, 37(4), 321-335.*

2. *EC-Council. (2021). Digital Forensics Essentials. EC-Council official curricula.*

3. *Xu, W., Deng, L., & Xu, D. (2022). Towards Designing Shared Digital Forensics Instructional Materials. In Proceedings of the 46th Annual International Computer Software and Applications Conference (COMPSAC 2022), 117-122.*