МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ криминалистически значимой информации

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Назарова Кирилла Дмитриевича

Научный руководитель
Старший преподаватель _____ А. А. Лобов
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Современное состояние информационной безопасности характеризуется непрерывным ростом как количества, так и сложности киберинцидентов. По данным исследований 2024 года, организации сталкиваются с критическими вызовами при выявлении и анализе инцидентов безопасности. Так, 44% организаций требуют более 30 минут для выявления критических проблем в своей инфраструктуре, что в условиях современных атак, когда среднее время от начального доступа до кражи данных составляет всего 72,98 часа, является неприемлемо долгим. Внедрение современных платформ мониторинга и анализа позволило 65% организациям сократить время обнаружения инцидентов до менее чем 5 минут.

Ключевой метрикой в области реагирования на инциденты является время выявления компрометации (Dwell Time) — период, в течение которого злоумышленник находится в системе до момента его обнаружения. В 2024 году этот показатель сократился до 7 дней, что на 46% лучше по сравнению с 13 днями в 2023 году и 26,5 днями в 2021 году. Однако эта позитивная динамика во многом достигнута благодаря совершенствованию методов анализа криминалистической информации и развитию инструментов для быстрого извлечения и обработки артефактов.

Артефакты ОС — это цифровые следы действий пользователя на компьютере, а также зарегистрированные события, связанные с функционированием системы. Они включают в себя временные файлы, журналы, данные приложений и многие другие данные, которые сохраняются в процессе работы устройства.

В то же время, для успешного расследования инцидентов и выявления признаков компрометации необходимо глубокое понимание того, какие данные оставляют операционные системы в результате своей работы, как эти данные организованы и как их эффективно анализировать. Операционные системы семейства Windows и Linux, занимающие доминирующее положение в IT-

инфраструктуре современных организаций (Windows на настольных компьютерах с долей 73,72%, Linux на веб-серверах с долей 59,2%), содержат множество криминалистически значимых артефактов, которые при правильном анализе позволяют реконструировать хронологию событий, выявить несанкционированную активность и определить методы, использованные злоумышленниками.

Существует значительный разрыв между развитостью инструментов автоматического сбора артефактов (таких как KAPE для Windows и UAC для Linux) и методологией комплексного анализа собранной информации. Большинство специалистов по инцидент-менеджменту в своей работе сталкиваются с разнородными, по-разному закодированными данными из различных источников, требующими трудозатратной ручной корреляции и синтеза. Отсутствие унифицированной методики анализа и автоматизированных решений для обработки артефактов обеих операционных систем приводит к снижению скорости и качества расследований.

Целью данной работы является разработка комплексной методологии анализа криминалистически значимой информации и создание модульной платформы для автоматизированной обработки, анализа и суммаризации артефактов, собранных с систем Windows и Linux. Для достижения данной цели поставлены следующие задачи:

- Провести классификацию и детальный анализ криминалистических артефактов операционных систем Windows и Linux, определить их структуру, расположение и информационную ценность для расследования инцидентов;
- Разработать и описать активные методы парсинга и извлечения данных из бинарных артефактов Windows с использованием специализированных инструментов, обосновать преимущества разделения этапов сбора и анализа;

- Определить основные методологические подходы анализа криминалистической информации, включая статистический анализ, выявление аномалий и корреляцию данных из различных источников;
- Спроектировать и реализовать модульную архитектуру платформы Xoctopus, обеспечивающей гибкое расширение функциональности и поддержку различных типов анализа;
- Разработать и описать набор парсеров и анализаторов для обработки артефактов обеих операционных систем, демонстрирующих практическое применение разработанной методологии;
- Провести оценку производительности и эффективности предложенных решений на примерах реальных инцидентов и сценариев расследования.

Новизна работы заключается в комплексном подходе к анализу криминалистической информации обеих основных операционных систем в единой модульной платформе, разработке унифицированной методологии корреляции разнородных данных и создании инструмента, ориентированного на автоматизацию рутинных этапов анализа при сохранении гибкости для специализированных исследований. Работа связана с актуальными исследованиями в области цифровой криминалистики, инцидент-менеджмента и разработки специализированного программного обеспечения для анализа безопасности.

Практическая значимость работы состоит в возможности применения разработанной платформы и описанных методологических подходов при проведении реагирования на инциденты, расследованиях компрометаций и аудитах безопасности IT-инфраструктуры организаций. Инструменты и методики, описанные в работе, позволяют снизить время и трудозатраты на расследование, повысить качество анализа и обеспечить более полное восстановление хронологии событий при инцидентах безопасности.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 12 приложений. Общий объем работы – 77 страниц, из них 42 страниц – основное содержание, включая 15 рисунков, список использованных источников из 30 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

1. Типы криминалистических артефактов операционных систем

Раздел систематизирует артефакты Windows и Linux для расследования инцидентов.

1.1 Артефакты Windows

Windows (73,72% рынка) содержит восемь типов артефактов: системная информация (HKEY_LOCAL_MACHINE), информация о пользователях (SAM-реестр), Prefetch, AmCache, ShimCache, Link Files, RecentDocs/JumpLists, MFT.

Выводы 1.1: Windows оставляет достаточно артефактов для реконструкции событий. Инструмент KAPE обеспечивает эффективное извлечение при триаж-подходе.

2 Криминалистические артефакты ОС Linux

Linux (59,2% веб-серверов) содержит артефакты пользователей (/etc/passwd, /etc/shadow, /etc/sudoers), логи аутентификации (/var/log/auth.log, wtmp, btmp), shell history, системные логи, auditd, systemd-journald, веб-логи.

Выводы 2: Linux содержит достаточно артефактов для реконструкции. Инструмент UAC обеспечивает структурированное извлечение триажа.

3. Методология анализа криминалистически значимой информации

3.1 Активные методы анализа артефактов

Парсинг бинарных артефактов Windows и Linux, хеширование для верификации целостности, разделение сбора и анализа.

Выводы 2.1: разделение этапов обеспечивает независимую верификацию и итеративный анализ множественных устройств.

3.2 Статистический анализ

Подсчёт уникальных источников, частотное распределение процессов, сравнение с базовым поведением для выявления аномалий.

Выводы 3.2: статистический анализ позволяет объективизировать выводы и выявить нетипичные паттерны.

3.3 Корреляция артефактов

Поиск пересечений по временным меткам, идентификаторам (UID, GID, PID), объектам (пути, inode) и сетевым параметрам. Синтез в полный timeline.

Выводы 3.3: корреляция позволяет выявлять сложные сценарии компрометации и timestomping.

4. Описание работы программы Xoctopus

4.1 Архитектура

Главный файл Xoctopus.py запускает три типа модулей: parsers (парсинг), analyzators (анализ), summaryzators (агрегация). Разделение на Linux и Windows версии.

4.2 Модули

Парсеры Linux включают модуль bodytime, осуществляющий преобразование временных меток из формата UNIX_TIMESTAMP в читаемый человеком формат (например, "21.01.2026 14:23:45"), с сохранением результата в файл Xoctopus_bodyfile_convert.txt. Этот модуль критичен для функционирования других модулей, поскольку обеспечивает унифицированный формат временных меток.

Модуль users_dot_files осуществляет сбор dot-файлов (конфигурационных файлов, начинающихся с точки) из домашних директорий всех пользователей: .bashrc, .bash_profile, .zsh_history, .ssh/authorized_keys и других. Результаты конкатенируются с классификацией по типу файла и сортировкой строк по частоте появления (для файлов истории команд). Этот подход позволяет быстро

выявить подозрительные записи в конфигурационных файлах без необходимости просмотра десятков файлов.

Модуль wtmp выполняет парсинг бинарных журналов аутентификации wtmp и btmp с использованием команды last, преобразуя бинарный формат в читаемый текстовый вид. Результаты включают информацию о времени начала и завершения сессии, IP-адреса источников и идентификаторы пользователей.

Модуль zimmerman_extractor (для Windows) использует набор инструментов Zimmerman Tools для парсинга MFT, Prefetch, AmCache и других артефактов. Этот модуль позволяет единовременно обработать все основные артефакты Windows с применением промышленных стандартов парсинга.

Анализаторы включают модуль process-masquerading, выявляющий попытки скрытия истинного исполняемого файла процесса путём сравнения информации из командной строки (cmdline) с внутренней памятью процесса. Некоторое вредоносное ПО подменяет видимое имя процесса на имя системного процесса, в то время как истинный исполняемый файл остаётся в памяти. Модуль сравнивает эти данные и выявляет несоответствия, записывая подозрительные процессы в файл process-masquerading.txt.

Модуль correlate_btmp_wtmp анализирует журналы аутентификации на предмет brute-force атак путём корреляции записей о неудачных попытках (btmp) с успешными входами (wtmp). Модуль может определить, был ли успешный вход совершён после серии неудачных попыток от того же IP-адреса, что указывает на успешный перебор пароля.

Модуль gsocket-finder выявляет использование инструмента gsocket — сложно детектируемой программы для установления скрытого канала управления между злоумышленником и скомпрометированной системой, обходящего правила межсетевого экрана. Модуль использует несколько признаков: обнаружение timestomping через сравнение временных меток (ctime старше mtime, mtime совпадает с наиболее старой mtime в директории), поиск процесса с именем системного сервиса, но удалённого из памяти "deleted", корреляция с сетевыми соединениями. Этот модуль демонстрирует применение

корреляционного анализа для выявления сложных инструментов компрометации.

Суммаризаторы включают модуль bodyfile_sum, объединяющий bodyfile (или bodyfile_convert при наличии парсинга) из всех анализируемых триажей в единый файл "Xoctopus_super_bodyfile" с добавлением идентификатора источника для каждой строки. Этот модуль позволяет аналитику работать с единым скоординированным временным масштабом для всех устройств.

Модуль users_dot_files_sum объединяет результаты работы parsers/users_dot_files из различных устройств в единый документ, облегчая выявление распространённых конфигураций и подозрительных записей на нескольких системах одновременно.

4.3 Примеры использования

Режимы: -t (одна триаж), -c (текущая директория), -m (множество), -a (все модули), -p (конкретный модуль), -s (суммаризация).

Выводы 3: Xoctopus реализует полный цикл парсинг → анализ → суммаризация. Агрегация с модульной расширяемой архитектурой. Позволяет автоматизировать действия и уменьшить время реагирования.

ЗАКЛЮЧЕНИЕ

В современном подходе к реагированию на инциденты информационной безопасности ключевым этапом является триаж – процесс предварительной оценки и приоритизации поступающих данных с целью эффективного распределения ресурсов и ускорения последующего расследования.

В рамках данной работы была разработана программная платформа Xoctopus, предназначенная для автоматизации процесса работы с триажами собранными с помощью внешних программных средств KAPE – для Windows, UAC – для Linux.

Архитектура платформы имеет модульную структуру и включает три типа модулей: парсеры, анализаторы и суммаризаторы, обеспечивающих гибкую работу и простоту интеграции между собой.

В ходе работы были созданы и внедрены модули, реализующие функции парсинга и адаптации бинарных артефактов, анализа артефактов на предмет применения bruteforce атак, поиска процессов с подменным исполняемым файлом, нахождение следов оставленных одним из самых часто применимых вредоносном инструменте gsocket. Также были разработаны модули для суммаризации артефактов с множества устройств в один файл.

Все поставленные цели и задачи исследования выполнены в полном объёме. Полученные результаты демонстрируют, что использование разработанной программной платформы, основанной на автоматизации типовых действий и применении заранее заданных правил корреляции, способствует повышению эффективности работы специалистов по информационной безопасности за счёт снижения трудоёмкости операций и сокращения времени принятия решений при проведении триажа инцидентов.