РОЛЬ КОМПЬЮТЕРНОЙ ФОРЕНЗИКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Шутко А.П.

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Герасимов А.С.

Аннотация: В статье обоснована необходимость автоматизации процесса удаленного сбора цифровых артефактов. Проанализированы недостатки существующих решений: высокая сложность развертывания, отсутствие гарантированной доставки данных, ограниченная гибкость настройки. В качестве решения предложена модульная архитектура системы, обеспечивающая централизованное хранение данных, локальное сохранение информации и расширяемость функциональности. Внедрение системы позволяет минимизировать потерю данных, сократить время получения информации и обеспечить прозрачность расследования.

Цифровая трансформация всех сфер деятельности общества привела к значительному росту числа компьютерных инцидентов и киберпреступлений. По данным Генеральной прокуратуры Республики Беларусь, в январе-феврале 2026 года количество зарегистрированных киберпреступлений увеличилось на 22 % по сравнению с аналогичным периодом прошлого года и составило более 3,1 тыс. преступлений [3]. В этих условиях особую значимость приобретает компьютерная форензика – область знаний, занимающаяся сбором, анализом и хранением цифровых доказательств, пригодных для использования в судебных процессах и внутренних расследованиях организаций [1].

Ключевыми принципами компьютерной форензики являются:

- неизменность доказательств (исходные данные не должны изменяться в процессе исследования);
- документирование всех операций (обеспечение цепочки хранения);
- воспроизводимость результатов.

Соблюдение данных принципов позволяет обеспечить юридическую значимость собранных цифровых доказательств [2].

Процесс расследования компьютерных инцидентов включает несколько последовательных этапов: идентификация инцидента, сбор цифровых доказательств, их исследование и анализ, документирование результатов, а также извлечение уроков для предотвращения подобных инцидентов в будущем. Схематичное представление данного процесса приведено на рисунке 1.

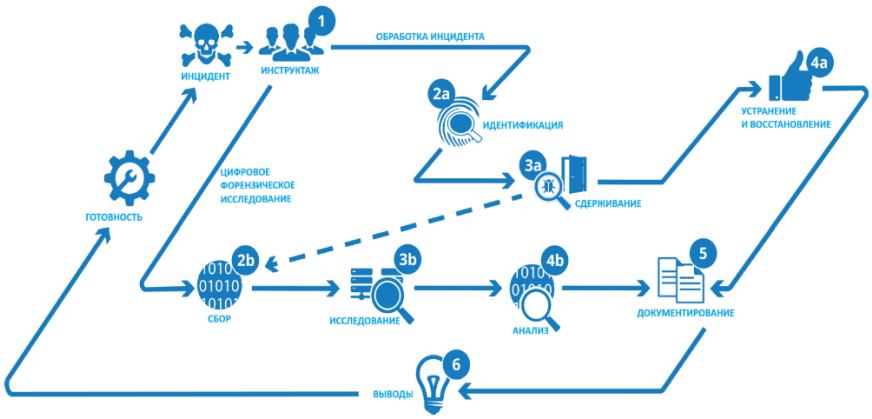

Рисунок 1 – Процесс обнаружения и расследования компьютерных инцидентов

Современные вызовы в области цифровой криминалистики обусловлены усложнением информационных инфраструктур, переходом на удаленные рабочие места и использованием распределенных систем. Это требует от специалистов:

- оперативного сбора данных с сотен компьютеров в различных сегментах сети;
- проведения исследований без физического доступа к оборудованию;
- обеспечения сохранности данных при нестабильных сетевых соединениях;
- обработки больших объемов разнородной информации.

Развитие методов удаленной форензики позволяет решать данные задачи с помощью специализированных программных агентов, устанавливаемых на исследуемые компьютеры. Современные подходы к удаленному сбору данных базируются на модульности архитектуры, минимальном воздействии на систему, локальном хранении данных при недоступности сервера и применении криптографических методов для обеспечения целостности [6].

Важное значение в подготовке специалистов в области компьютерной форензики имеет практико-ориентированное обучение. В учебных пособиях БГУИР [1, 2] рассматриваются основные методы сбора и анализа цифровых артефактов в операционных системах Windows, а также особенности документирования результатов форензического исследования. Лабораторный практикум [2] позволяет освоить практические навыки работы с криминалистически значимыми данными, включая извлечение информации из реестра, журналов событий, файловой системы и оперативной памяти.

Методологические подходы к обеспечению информационной безопасности, включая вопросы организации защиты информации и управления инцидентами, изложены в учебно-методическом пособии [6]. Авторы акцентируют внимание на необходимости системного подхода к построению защиты информационных систем, что напрямую связано с задачами компьютерной форензики. В рамках практикума рассматриваются сценарии реагирования на инциденты, что позволяет сформировать у специалистов целостное представление о процессе расследования.

Особенности расследования компьютерных преступлений в Республике Беларусь регламентируются ведомственными методическими материалами [4], которые учитывают специфику национального законодательства и правоприменительной практики. В учебном пособии Академии МВД рассматриваются организационные и процессуальные аспекты проведения следственных действий, связанных с изъятием и исследованием цифровых доказательств. Особое внимание уделяется вопросам обеспечения цепочки хранения доказательств и соблюдения процессуальных норм при проведении форензических исследований.

Современные научные исследования в области цифровой криминалистики отражены в сборнике научных трудов БГУИР [5], где представлены результаты разработок в области методов сбора и анализа цифровых артефактов, а также подходы к автоматизации форензических исследований. Среди актуальных направлений исследований можно выделить:

- разработку методов обнаружения скрытых и удаленных данных;
- создание алгоритмов автоматизированного анализа больших объемов цифровых доказательств;
- совершенствование методов извлечения информации из памяти работающих систем;
- развитие подходов к удаленному сбору данных в распределенных сетях.

Компьютерная форензика находит широкое применение в правоохранительной деятельности, корпоративном секторе, а также в образовательном процессе при подготовке специалистов в области информационной безопасности [4, 5]. В правоохранительной деятельности методы форензики используются для раскрытия киберпреступлений и сбора доказательств, имеющих юридическую силу. В корпоративном секторе компьютерная форензика применяется при расследовании инсайдерских угроз, утечек конфиденциальной информации и нарушений политик безопасности.

Дальнейшее развитие компьютерной форензики связано с автоматизацией процессов сбора и анализа данных, внедрением методов искусственного интеллекта для выявления скрытых закономерностей, а также разработкой специализированных программных средств, учитывающих особенности современных операционных систем и сетевых инфраструктур.

Таким образом, компьютерная форензика является неотъемлемым элементом системы обеспечения информационной безопасности, позволяющим не только эффективно расследовать произошедшие инциденты, но и вырабатывать превентивные меры по их предотвращению. Развитие методологических основ, совершенствование практических методик и подготовка квалифицированных кадров в этой области являются важнейшими факторами противодействия современным киберугрозам.

Список использованных источников:

1. Веленто, И.И. Компьютерная криминалистика : учеб.-метод. пособие / И.И.Веленто. – Минск : БГУИР, 2021. – 87 с.

2. Веленто, И.И. Компьютерная криминалистика. Лабораторный практикум : учеб.-метод. пособие / И.И. Веленто, Т.А. Пархимович. – Минск : БГУИР, 2022. – 63 с.

3. В Беларуси с начала 2026 года зарегистрировано более 3 тысяч киберпреступлений [Электронный ресурс] // Беларусь сегодня. – 2026. – 31 марта. – Режим доступа: https://www.sb.by/articles/kolichestvo-kiberprestupleniy-v-etom-2026-vyroslo-na-20-protsentov.html (дата обращения: 01.04.2026).

4. Методика расследования компьютерных преступлений : учеб. пособие / под ред. В.А. Гусева. – Минск : Академия МВД Республики Беларусь, 2023. – 145 с.

5. Основы цифровой криминалистики : сб. науч. тр. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: И.И. Веленто – Минск : БГУИР, 2024. – 110 с.

6. Борботько, Т.В. Методология информационной безопасности. Практикум : учеб.-метод. пособие / Т.В. Борботько, О.В. Бойправ. – Минск : БГУИР, 2024.