Буй Дуй Хоанг, курсант,
Краснодарское высшее военное училище

Сидельников Олег Васильевич, старший преподаватель,
Краснодарское высшее военное училище

АЛГОРИТМИЗАЦИЯ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ: СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЙ АЛГОРИТМ И МЕТОДИЧЕСКИЕ ОСНОВАНИЯ

Аннотация. В статье рассматривается алгоритмизация расследования компьютерных инцидентов как организационно-аналитический процесс. На основе сопоставления стандартов и методических документов предложена структурно-функциональный алгоритм, объединяющая верификацию признаков инцидента, начальное реагирование, координацию, восстановление системы и итоговую отчетность. Показано, что научная ценность алгоритма состоит в формализации переходов между этапами, введении обратной связи и определении критерия завершения расследования.

Ключевые слова: Компьютерный инцидент; расследование инцидентов; алгоритм расследования; реагирование на инциденты; информационная безопасность; отчет об инциденте.

В современных условиях развитие информационных систем и сетевой инфраструктуры приводит к тому, что компьютерный инцидент становится не только техническим событием, но и объектом организационного, аналитического и управленческого исследования. После выявления признаков нарушения недостаточно восстановить работоспособность отдельного узла или сервиса. Необходимо установить, какие элементы инфраструктуры были затронуты, какие цифровые следы подтверждают факт воздействия, каким образом развивался инцидент, какие условия способствовали его реализации и какие меры должны быть приняты для предупреждения повторения аналогичной ситуации. Такой подход соответствует современной логике менеджмента инцидентов информационной безопасности, в которой обнаружение, оценка, реагирование, анализ и улучшение рассматриваются как взаимосвязанные элементы единого процесса.

Актуальность исследования определяется тем, что нормативно-методическая база уже содержит значительный массив требований к управлению компьютерными инцидентами, однако эти требования распределены по различным документам и не всегда представлены в виде единого алгоритма расследования. ISO/IEC 27001 задает общую рамку управляемости, оценки рисков и постоянного совершенствования системы менеджмента информационной безопасности [1]. ГОСТ Р ИСО/МЭК ТО 18044-2007 раскрывает структурный подход к менеджменту инцидентов, включая подготовку, использование, анализ и улучшение [2]. ГОСТ Р 59712-2022 конкретизирует стадии обнаружения, регистрации, реагирования и анализа результатов управления компьютерными инцидентами [3]. Следовательно, научная задача состоит не в повторном описании отдельных процедур, а в их алгоритмическом синтезе в форме модели, пригодной для практического применения.

В прикладной плоскости указанная задача особенно значима для организаций, в которых обработка информации связана с повышенными требованиями к конфиденциальности, целостности, доступности и управляемости действий должностных лиц. В таких условиях расследование компьютерного инцидента должно обеспечивать не только

восстановление функционирования, но и получение объективных сведений о причинах, условиях и последствиях нарушения. Для военной и ведомственной среды существенное значение имеют также порядок координации, своевременное уведомление, распределение ответственности и сохранение конфиденциальности информации, получаемой в ходе реагирования, что отражено в нормативных актах о координации и реагировании на сетевые инциденты.

Проблема расследования компьютерных инцидентов заключается в необходимости соединить три различные логики: техническую, доказательную и управленческую. Техническая логика ориентирована на обнаружение признаков воздействия, анализ журналов, сетевых соединений, учетных записей, изменений конфигурации и состояния средств защиты. Доказательная логика требует сохранения цифровых следов, фиксации последовательности действий и обоснования выводов о причине и механизме инцидента. Управленческая логика связана с координацией исполнителей, принятием решений, распределением ответственности и документированием результатов. Если эти логики не объединены в общую процедуру, расследование приобретает фрагментарный характер и теряет воспроизводимость.

ГОСТ Р 59712-2022 указывает, что управление компьютерными инцидентами включает регистрацию признаков возможного инцидента, подтверждение инцидента, определение вовлеченных элементов инфраструктуры, локализацию, выявление и ликвидацию последствий, фиксацию материалов, установление причин и условий возникновения инцидента, а также оценку эффективности реагирования [3]. Эти положения являются важной основой для построения алгоритма, поскольку задают не только перечень действий, но и логику перехода от обнаружения признаков к анализу результатов.

ГОСТ Р ИСО/МЭК ТО 18044-2007 дополняет указанную логику акцентом на планирование и подготовку, создание группы реагирования, оценку событий, регистрацию решений и последующее извлечение уроков [2]. В свою очередь, ГОСТ Р 22.3.09-2014 подчеркивает значение командования, управления, оперативной информации, координации и информационного обмена при реагировании на инциденты [4]. Для исследования компьютерного инцидента эти положения имеют прямое значение, поскольку без координационного контура технические действия исполнителей могут быть несогласованными, а результаты анализа – неполными.

Методика оценки угроз безопасности информации ФСТЭК России позволяет связать расследование с анализом негативных последствий, объектов воздействия, источников угроз и сценариев реализации угроз. Это важно потому, что результат расследования должен отвечать не только на вопрос о том, что произошло, но и на вопрос о том, почему инцидент стал возможным и какие уязвимости или организационные условия способствовали его возникновению. Учебно-методическая литература по расследованию инцидентов информационной безопасности также подтверждает необходимость привлечения специалистов, осмотра средств компьютерной техники, анализа электронных документов и сбора свидетельств инцидента.

Методологическую основу статьи составляет сравнительный анализ нормативно-методических источников, функциональная декомпозиция процесса расследования и структурно-логическое моделирование последовательности действий. Сравнительный анализ позволяет выделить устойчивые элементы, повторяющиеся в различных стандартах и руководствах: обнаружение события, верификация признаков, регистрация, сбор данных, оценка последствий, локализация, восстановление, анализ причин и формирование итогового отчета.

Структурно-функциональный алгоритма расследования компьютерных инцидентов

Предлагаемый алгоритм строится как четырехэтапная процедура. Первый этап обеспечивает обнаружение и первичную верификацию признаков возможного компьютерного инцидента. Исходной точкой алгоритма является не уже установленный инцидент, а сообщение, событие мониторинга, сигнал средства защиты, обращение пользователя или иная информация, указывающая на возможное нарушение. Введение узла «инцидент подтвержден?» принципиально важно, поскольку позволяет разграничить ложное срабатывание, технический сбой, штатное отклонение и действительно значимый инцидент [2].

Если инцидент не подтверждается, процесс не должен завершаться простым отказом от дальнейших действий. Отрицательный результат проверки также является аналитически значимым: он подлежит фиксации, используется для уточнения правил мониторинга, корректировки критериев классификации и повышения качества последующего обнаружения. Тем самым в алгоритм вводится контур обратной связи, обеспечивающий накопление опыта и снижение количества ложных срабатываний.

Второй этап включает сбор данных и начальное реагирование. Его задача состоит в том, чтобы синхронизировать сохранение цифровых следов с первичными мерами локализации и минимизации ущерба. На этой стадии собираются журналы событий, сведения об учетных записях, сетевых соединениях, изменениях прав доступа, конфигурации, состоянии средств защиты и затронутых ресурсах. Одновременно определяются меры, которые допустимо выполнить без разрушения значимых следов, поскольку несогласованное восстановление системы может привести к утрате доказательной информации.

Третий этап представляет контур. В его рамках осуществляется реконструкция последовательности событий, анализ характера инцидента, определение вовлеченных элементов инфраструктуры, оценка последствий, распределение задач между исполнителями и согласование решений. Координация рассматривается не как внешняя административная функция, а как непрерывный элемент алгоритма, обеспечивающий управляемость расследования, своевременный обмен информацией и согласование технических и организационных действий.

Четвертый этап связан с восстановлением нормального функционирования системы, оценкой результатов расследования и подготовкой итогового отчета. Критерий завершения основной части процесса задается не формальным окончанием работ, а подтверждением того, что система функционирует в штатном режиме, последствия инцидента устранены, материалы зафиксированы, причины и условия возникновения инцидента установлены, а выводы оформлены в документированном виде.

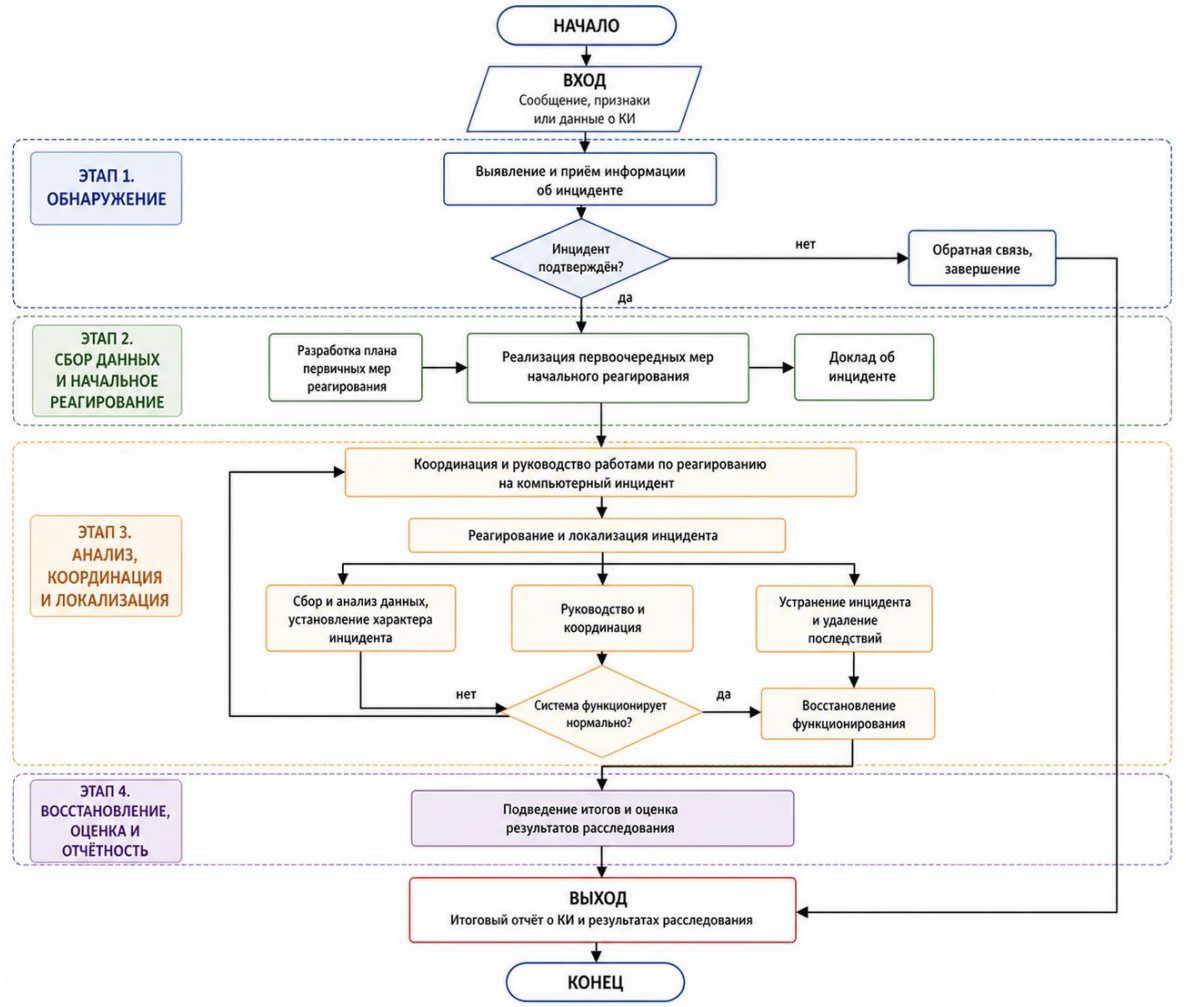

Рисунок 1. Структурно-функциональная схема алгоритма расследования компьютерных инцидентов

Функциональный алгоритм

Для повышения воспроизводимости предложенного подхода этапы алгоритма целесообразно представить через их функцию, основной результат и нормативно-методическую опору. Такая декомпозиция показывает, что каждый блок алгоритма имеет самостоятельное назначение и одновременно связан с последующими действиями расследования.

Таблица 1

Этап алгоритма	Основное содержание	Результат этапа
Обнаружение и верификация	Получение сообщения или сигнала мониторинга, первичная оценка признаков, решение о подтверждении инцидента.	Подтвержденный инцидент либо зафиксированное неподтвержденное событие с обратной связью.
Сбор данных и начальное реагирование	Фиксация журналов, цифровых следов, сведений об учетных записях, сетевых соединениях и затронутых ресурсах; первичная локализация.	Сохраненная доказательная база и сниженный риск дальнейшего распространения инцидента.

Аналитико-координационная обработка	Реконструкция хронологии, определение характера и последствий инцидента, распределение задач, согласование решений.	Установленные обстоятельства, вовлеченные элементы инфраструктуры и предварительные выводы.
Завершение и отчетность	Проверка восстановления штатного режима, оценка результатов реагирования, оформление причин, условий и рекомендаций.	Итоговый отчет, пригодный для управленческого анализа и совершенствования защиты.

Научная новизна и практическая значимость предложенного алгоритма

Научная новизна предлагаемого подхода состоит в том, что расследование компьютерного инцидента рассматривается как самостоятельный организационно-аналитический процесс, а не как совокупность отдельных технических действий. В отличие от описательных схем реагирования, предложенный алгоритм формализует переходы между этапами, устанавливает входные и выходные данные, вводит узлы принятия решений и связывает технический анализ с управленческим контуром.

Первым элементом новизны является выделение узла верификации признаков инцидента. Это позволяет избежать методической ошибки, при которой любое событие безопасности автоматически трактуется как инцидент. Вторым элементом является введение обратной связи при неподтверждении инцидента. Данный элемент показывает, что даже ложное срабатывание имеет ценность для совершенствования правил мониторинга и классификации. Третьим элементом является включение непрерывной функции координации, обеспечивающей согласование действий технических специалистов, руководителей и иных участников процесса. Четвертым элементом является использование критерия завершения по факту восстановления штатного функционирования системы и оформления результатов расследования.

Практическая значимость алгоритма определяется возможностью ее применения при разработке локальных регламентов расследования, типовых планов реагирования, учебных материалов и шаблонов отчетности. Использование такого алгоритма позволяет снизить риск утраты цифровых следов, повысить воспроизводимость аналитических выводов, упорядочить взаимодействие между участниками расследования и обеспечить единый подход к документированию результатов. Кроме того, алгоритм может использоваться как основа для имитационного моделирования компьютерных инцидентов на инструментальном стенде, где проверяется не только работа отдельных программных средств, но и согласованность всей процедуры расследования.

Ограничения исследования и направления дальнейшей разработки

Предложенный алгоритм имеет методический, а не программно-технический характер. Она не заменяет специализированные средства мониторинга, SIEM, EDR, системы управления уязвимостями, средства анализа сетевого трафика и инструменты компьютерной криминалистики. Ее назначение состоит в том, чтобы задать последовательность действий и связи между ними. Эффективность применения модели на практике будет зависеть от полноты журналирования, квалификации специалистов, качества локальных регламентов, доступности исходных данных и организационной дисциплины.

Дальнейшая разработка может быть направлена на создание матрицы соответствия между этапами алгоритма и конкретными типами цифровых следов, разработку шкалы приоритизации инцидентов, формализацию критериев подтверждения инцидента, построение типовых шаблонов отчета и проверку алгоритма на имитационных сценариях. Отдельным

направлением является адаптация алгоритма к ведомственным условиям, где особое значение имеют разграничение полномочий, конфиденциальность сведений, порядок докладывания и взаимодействие между подразделениями.

Заключение

Наличие технических средств мониторинга и реагирования является необходимым условием, однако без единой логики действий они не обеспечивают полноты, воспроизводимости и управляемости расследовательского процесса.

Предложенная структурно-функциональный алгоритм объединяет обнаружение признаков инцидента, первичную верификацию, сбор и фиксацию цифровых следов, начальное реагирование, аналитико-координационную обработку, восстановление функционирования системы и подготовку итогового отчета. Научная ценность алгоритма заключается в алгоритмическом синтезе требований стандартов, методических документов и практических процедур расследования. Практическая ценность состоит в возможности использования алгоритма как основы для локальных регламентов, учебной подготовки специалистов и построения процедур документирования результатов расследования компьютерных инцидентов.

Список литературы:

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

2. ГОСТ Р 59712-2022. Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты.

3.ISO/IEC 27035-1:2023. Информационная безопасность, кибербезопасность и защита конфиденциальности. Менеджмент инцидентов информационной безопасности. Часть 1. Принципы и процесс.

4. ISO/IEC 27035-2:2023. Информационная безопасность, кибербезопасность и защита конфиденциальности. Менеджмент инцидентов информационной безопасности. Часть 2. Руководство по планированию и подготовке реагирования на инциденты.