**УДК 004**
**DOI 10.26118/2782-4586.2025.90.55.030**

**Панюкова Екатерина Владимировна**
Самарский государственный технический университет

## Актуальные методы анализа в управлении IT-инцидентами

**Аннотация**. Данная статья посвящена анализу современных подходов и методов, используемых для анализа и управления инцидентами в сфере информационных технологий. Автор анализирует принципы и условия использования методов анализа инцидентов, применительно к IT системам. Особое внимание уделяется применению методов анализа данных, машинного обучения в управлении инцидентами (ITSM). В статье также обсуждаются проблемы, связанные с увеличением сложности IT-инфраструктур и необходимостью оперативного реагирования на инциденты. Предложены рекомендации по внедрению эффективных практик и инструментов для повышения устойчивости IT-систем и минимизации последствий сбоев. Работа будет полезна специалистам в области IT-безопасности, управления инфраструктурой и аналитикам данных.

**Ключевые слова**: ITIL, информационные технологии, инцидент, методы анализа инцидентов, управление IT инцидентами, классификация инцидентов.

**Panyukova Ekaterina Vladimirovna**
Samara State Technical University

## Current analysis methods in IT incident management

**Abstract**. This article is devoted to the analysis of modern approaches and methods used for incident analysis and management in the field of information technology. The author analyzes the principles and conditions of using incident analysis methods in relation to IT systems. Special attention is paid to the application of data analysis methods and machine learning in incident management (ITSM). The article also discusses the problems associated with the increasing complexity of the IT infrastructure and the need for rapid response to incidents. Recommendations on the implementation of effective practices and tools to increase the stability of IT systems and minimize the consequences of failures are proposed. The work will be useful for IT security specialists, infrastructure management and data analysts.

**Keywords:** ITIL, information technology, incident, incident analysis methods, IT incident management, incident classification.

**Введение.** Современные программные продукты представляют собой системы, состоящие из большого количества компонентов – серверов, сетевых устройств, микросервисов, облачных платформ и т.д. В таких условиях даже незначительная ошибка может привести к каскадным сбоям. Такие сбои, отказы в информационных системах, сервисов влекут за собой не только частичную или полную остановку, но и приводят к потерям, рискам и нарушениям SLA. Поэтому ITIL рассматривает анализ и классификацию инцидентов как инструменты управления IT-инцидентами, которые позволяют эффективно выявлять, оценивать и прогнозировать сбои, отказы в работе информационных систем и сервисов [13].

Применение методов и инструментов анализа IT-инцидентов расширяет возможности оценивания минимизировать последствия инцидентов, а также улучшать общую устойчивость и безопасность системы.

Применение методов и инструментов анализа IT-инцидентов расширяет возможности оценки возникновения подобных инцидентов и их последствий, устойчивости

IT-инфраструктуры к подобным сбоям или отказам. Процесс анализа в управлении IT-инцидентами способствует снижению времени простоя и минимизации ущерба, а также позволяет прогнозировать и предотвращать потенциальные угрозы за счет использования современных технологий, таких как машинное обучение и автоматизированные системы мониторинга.

Целью настоящей работы является исследование и систематизация актуальных методов анализа IT-инцидентов, оценить их эффективность и предложить рекомендации по их применению в современных IT-системах.

Объектом исследования являются процессы управления IT-инцидентами, включая выявление, анализ, устранение и предотвращение инцидентов.

Предмет исследования - методы анализа IT-инцидентов, такие как Root Cause Analysis (RCA), Fault Tree Analysis (FTA), STAMP, CAPA, Event Chain Analysis и другие.

Проблема исследования- несмотря на наличие множества методов анализа IT-инцидентов, их эффективность во многом зависит от контекста применения, сложности системы и доступности данных. Существует проблема выбора наиболее подходящего метода для конкретной ситуации, а также интеграции этих методов в процессы управления инцидентами.

**Основная часть:** Актуальность исследования существующих подходов и методов анализа, используемых для оценки и классификации инцидентов обусловлена множеством факторов - сложностью инфраструктур современных IT-систем, увеличением числа кибератак, возросшими требованиями к надежности и доступности.

Современные IT-системы включают множество компонентов, таких как облачные сервисы, микросервисы и контейнеры, что увеличивает вероятность возникновения инцидентов.

Кибератаки становятся все более изощренными, что требует применения современных методов анализа для их предотвращения и устранения последствий.

Требования в плане доступности, надежности и нагрузки IT-систем критически важны, так как функционирование бизнес-процессов компании зависит от времени простоя и непрерывности работы IT-систем.

И не забываем, что автоматизация бизнес-процессов и функционирование IT-систем должно соответствовать стандартам и подходам в управлении системами, сервисами и услугами в IT-технологиях – ГОСТ Р ИСО/МЭК 20000- 1 «Информационные технологии. Управление услугами. Часть 1. Требования к системе управления услугами», ISO/IEC 27001 «Информационная безопасность, кибербезопасность и защита конфиденциальности - системы управления информационной безопасностью. Требования», ГОСТ Р ИСО 22301 «Системы менеджмента непрерывности бизнеса. Общие требования», ГОСТ Р ИСО 9001 «Системы менеджмента качества. Требования», ITIL [13], COBIT (Control Objectives for Information and Related Technologies), NIST (National Institute of Standards and Technology), DevOps (development, operations), SRE (Site Reliability Engineering) и т.д.

Исследование методов анализа инцидентов показал, что для анализа причин возникновения инцидента достаточно часто используют следующие подходы:

- Root Cause Analysis (RCA) – метод анализа первопричин инцидентов. Метод направлен в первую очередь на выявление глубинных, основных причин инцидентов. [1].

К основным преимуществам данного метода можно отнести определение основных причин инцидентов и как следствие предотвращение их повторений. Однако метод RCA требует значительных временных и ресурсных затрат и может быть сложным для применения в сложных системах.

- PIP (Problem Impact Process) - структурированный подход к управлению инцидентами. Метод помогает быстро и эффективно анализировать проблемы, оценивать их влияние и определять процесс их устранения [2, 3].

Данный метод широко используется в рамках методологии ITIL (Information Technology Infrastructure Library) и других фреймворков управления инцидентами.

Метод PIP показал хорошие результаты в управлении инцидентами. Это конечно связано с простотой его использования и структурированности. Метод позволяет быстро определить ключевые аспекты инцидента, расставить приоритеты и оценить влияние на бизнес-процессы.

У данного метода есть существенный недостаток - ограниченная глубина анализа. Это связано с тем, что метод больше подходит для оперативного реагирования, чем для глубокого анализа корневых причин. Также эффективность метода зависит от качества данных – ее точности, полноты информации о проблеме.

- ICAM (Incident Cause Analysis Method) – метод для систематического подхода к анализу причин инцидентов. Часто используется в различных отраслях - авиация, энергетика, здравоохранение и промышленность. ICAM фокусируется на выявлении не только непосредственных причин инцидента, но и системных факторов, которые способствовали его возникновению. Этот метод помогает предотвратить повторение подобных инцидентов в будущем [4-6].

Метод ICAM позволяет выявить не только прямые, но и системные причины инцидентов. Действие метода направлено на предотвращение повторений инцидентов за счет устранения основных причин.

Для проведения анализа инцидентов данным методом требуются значительные ресурсы - временные и инструментальные. Также, как и при использовании метода PIP, эффективность результата анализа зависит от полноты и точности исходной информации.

- STAMP (Systems-Theoretic Accident Model and Processes) - метод анализа инцидентов, основанный на системной теории.

Анализ [7] показал, что данный подход анализа инцидентов рассматривает сбой не как цепочку событий, а как результат нарушения контроля в системе.

Также можно отметить, что метод STAMP акцентирует внимание на взаимодействие между компонентами системы и окружением. При этом система рассматривается не как структура взаимодействующих компонентов, а как иерархия уровней контроля. Каждый уровень системы обеспечивает управление и ограничения для нижестоящих уровней.

- CAPA (Corrective and Preventive Action) - систематический подход к управлению инцидентами, который направлен не только на устранение текущих проблем, но и на предотвращение их повторения в будущем.

CAPA широко используется в различных отраслях, включая производство, здравоохранение, фармацевтику и IT, и является ключевым элементом систем управления качеством (например, ISO 9001) [8].

Анализ методом CAPA основывается на комплексном подходе – направлен на устранение текущих проблем и предотвращение будущих.

К основным недостаткам данного подхода можно отнести потребность в значительных временных и ресурсных затрат при проведении анализа, а также зависимость результата от точности выявления корневых причин.

- Event Chain Analysis (ECA) - метод анализа инцидентов, который фокусируется на изучении последовательности событий, приведших к инциденту.

ECA помогает выявить ключевые события, их взаимосвязи и влияние на конечный результат, широко используется в управлении проектами, авиации, производстве и других областях, где важно понимать цепочку событий, приводящих к инцидентам.

Анализ [9] показал, что при анализе события отображаются в виде цепочки событий, что упрощает понимание инцидентов, особенно простых. Данный метод фокусируется на ключевые события, которые привели к инциденту.

При использовании ECA необходимо учитывать ограничения - не учитываются системные факторы и глубинные причины, эффективность анализа зависит от полноты и точности информации о событиях, не подходит для анализа сложных или многоуровневых системах.

- Анализ дерева отказов (Fault Tree Analysis, FTA) - метод анализа инцидентов, который использует логические схемы для выявления причин возникновения отказов или инцидентов.

FTA широко применяется в отраслях с высокими требованиями к безопасности, таких как авиация, энергетика, ядерная промышленность и производство. FTA помогает визуализировать взаимосвязи между различными факторами, которые могут привести к инциденту, и оценить вероятность его возникновения.

К достоинствам данного подхода относят легкость визуализации причин и их взаимосвязей в виде структурного дерева. Позволяет выявлять как прямые, так и косвенные причины инцидента. Также выделяют возможность расчета вероятности возникновения инцидента на основе данных о базовых событиях [10-11].

К недостаткам анализа дерева отказов можно отнести зависимость эффективность результата анализа от точности и полноты данных о базовых событиях. И самое главное – сложен в плане применения для анализа инцидентов в системах с высокой степенью взаимодействия компонентов.

- Анализ причин и последствий (Cause and Effect Analysis) - метод анализа инцидентов, который помогает выявить и визуализировать причины проблемы и их взаимосвязи.

Этот метод широко используется в управлении качеством, производстве, здравоохранении и других областях для анализа инцидентов и поиска решений.

С помощью метода Cause and Effect Analysis легко визуализировать причины и их взаимосвязи, но присутствуют ограничения - не всегда возможно выявить глубинные или системные причины и не подходит для количественного анализа. С помощью данного метода нельзя оценить вероятность или влияние причин [12].

По результату анализа методов анализа отказов можно сделать следующие выводы:

1. Традиционные методы анализа инцидентов (например, Cause and Effect Analysis, FTA) эффективны для быстрого выявления и устранения непосредственных причин, особенно в простых системах. Это связано с тем, что данные подходы фокусируются на цепочке событий или человеческих ошибках.
2. Для анализа сложных инцидентов и предотвращения их повторения в будущем рекомендуется использовать более системные подходы, такие как STAMP или ICAM. Метод STAMP позволяет выявлять не только непосредственные причины, но и системные узкие места, которые могут привести к будущим проблемам. Однако данные подходы имеют ограничения, особенно при анализе сложных систем.
3. Для анализа IT-инцидентов лучше использовать методы, которые не только выявляют причины проблем, но и оценивают их последствия. Выбор метода зависит от сложности инцидента, доступных данных и целей анализа.
4. Комбинирование различных методов позволяет получить более полное и всестороннее понимание причин и последствий инцидентов.

Комбинирование методов RCA и STAMP даст более полное и системное представление о причинах инцидентов, так как учитывает не только технические, но и человеческие факторы. Данный подход подойдет для анализа сложных инцидентов, где важно понять взаимодействие компонентов системы.

Комбинирование методов RCA и FTA даст результат, который фокусируется на логических связях между событиями и их вероятностями. Этот подход подойдет для анализа технических инцидентов, где важно выявить конкретные причины и риски. Система комбинирования методов для анализа IT-инцидентов будет зависеть от типов инцидентов, целей анализа и исходных данных.

5. Для более полного понимания причин и последствий IT-инцидентов, выявления аномалий и прогнозирования отказов в работе IT-систем предлагается системное использование инструментов машинного обучения и методов анализа данных.

Применение методов машинного обучения направлено на исследовательский анализ и классификацию инцидентов по категориям и приоритетам на основе алгоритмов и шаблонов, обученных на основе собранных ранее данных инцидентов [14].

**Заключение.** Анализ IT-инцидентов является критически важным элементом управления современными IT-системами. Использование как традиционных, так и подходов для анализа сложных систем, позволит не только устранить текущие проблемы, но и предотвратить их повторение в будущем. Комбинирование этих методов с современными технологиями поможет устранить ограничения, присущие каждому отдельному методу.

## Список источников


1. Himanish Ganguly Implementing Effective Root Cause Analysis (RCA) in Incident Management [Электронный ресурс]: https://www.infizo.com/desk-blog-posts/implementing-effective-root-cause-analysis-rca-in-incident-management
2. ITIL® 4: the framework for the management of IT-enabled services [Электронный ресурс]: https://www.axelos.com/certifications/itil-service-management
3. Incident management for high-velocity teams [Электронный ресурс]: https://www.atlassian.com/incident-management
4. Luke Dam The Benefits of the ICAM Incident Investigation Process [Электронный ресурс]: https://www.safetywise.com/post/2016/02/24/the-benefits-of-the-icam-incident-investigation-process
5. Identity, Credential, and Access Management ICAM Best Practices [Электронный ресурс]: https://identitymanagementinstitute.org/identity-credential-and-access-management-icam-best-practices/
6. . Landre J., Irving M., Hodges I., Weston B. Learning from accidents and incidents [Электронный ресурс]: https://identitymanagementinstitute.org/identity-credential-and-access-management-icam-best-practices/
7. Nancy G. Leveson Engineering a Safer World: Systems Thinking Applied to Safety. Massachusetts Institute of Technology – 2011, 555 p.
8. Corrective and Preventive Action (CAPA): The Definitive Guide (Updated for 2025) [Электронный ресурс]: https://www.thefdagroup.com/blog/definitive-guide-to-capa
9. Event Chain Methodology [Электронный ресурс]: https://intaver.com/technology/event-chain-methodology/
10. Jade Morales Fault Tree Analysis: A Step-by-Step Guide to Identifying System Failures [Электронный ресурс]: https://www.mindonmap.com/blog/fault-tree-analysis/
11. Rutan Bhattacharyya Fault Tree Analysis [Электронный ресурс]: https://www.wallstreetmojo.com/fault-tree-analysis/
12. Ishikawa Diagram: A Comprehensive Guide to Cause and Effect Analysis [Электронный ресурс]: https://www.iienstitu.com/en/blog/ishikawa-diagram
13. ITIL Foundation: ITIL 4 Edition [Электронный ресурс] https://itil.press/wp-content/uploads/2021/09/itil-foundation-4-edition.pdf
14. Панюкова Е. В. Автоматизация управления IT-инцидентами компании / Е. В. Панюкова, К. В. Портнов // Журнал монетарной экономики и менеджмента. – 2024. – № 3. – С. 89-94. – DOI 10.26118/2782-4586.2024.98.80.013. – EDN CJIIST


## Сведения об авторе


**Панюкова Екатерина Владимировна,** к.п.н.. доцент кафедры «Информатика и вычислительная техника», ФГБОУ ВО «Самарский Государственный Технический Университет», г. Самара, Россия


## Information about the author


**Panyukova Ekaterina Vladimirovna,** Candidate of Pedagogical Sciences, Associate Professor of the Department of Computer Science, Federal State Budgetary Educational Institution of Higher Education "Samara State Technical University", Samara, Russia