ПРИМЕНЕНИЕ РЕЗОНАНСА В АВАРИЙНЫХ СИТУАЦИЯХ В ИТ-ЛАНДШАФТЕ ОРГАНИЗАЦИИ

Гадасин Д.В., Пантелеева К.А.
Московский технический университет связи и информатики, Москва, Россия
dengadiplom@mail.ru, k.a.panteleeva@mail.ru

Аннотация. Для быстрого реагирования на аварийные ситуации в ИТ-ландшафте организации необходимо внедрять систему для реагирования и управления аварийными ситуациями, которая выполняет функцию панели диспетчера, по аналогии с панелью управления летчиков, и помогает организовывать быстрый сбор профильных специалистов для восстановления сломанной системы.

Ключевые слова: аварийный процесс, система управления, ITSM, ITIL, восстановление системы.

Введение

Многие мировые компании и корпорации используют методологию ITIL и решения ITSM, который вырос из ITIL, для повышения качества предоставляемых услуг, а также отказоустойчивости и надежности выпускаемых и используемых решений. В отчете компании Reportlinker.com “Cloud-Based ITSM Global Market Report 2022”, который предоставляет статистику рынка облачного ITSM, говорится, что, по ожиданиям, мировой рынок решений ITSM на основе облачных технологий вырастет с 6.65 миллиардов долларов в 2021 году до 7.83 миллиардов долларов в 2022 году при совокупном годовом темпе роста 17.85%, а к 2026 году объем рынка достигнет значения в 15.38 миллиардов долларов.

Все большее внедрение облачных приложений также поспособствуют стимуляции роста рынка в прогнозируемом периоде. Согласно опросу O’Reilly, в 2020 году 88% респондентов использовало облако, а в 2021 году уже 90% предприятий использовало облачные вычисления.

Технологические инновации также являются ключевой тенденцией: крупные игроки рынка, представленные на рынке облачных ITSM, сосредоточены на оказывают услуги технологически передовых решений и платформ для укрепления своих позиций на рынке, внедряя виртуализацию, grid computing, ИИ (искусственный интеллект) [1], сервис-ориентированную архитектуру, майнинг, автоматизированную облачную оркестровку и т.д. и т.п. Так, в апреле 2020 года американская компания ServiceNow запустила решение Cloud Call Center, представляющее из себя инновационное решение CCaaS на базе ИИ для ИТ-поддержки, помогающее экономить расходы, улучшая качество обслуживания звонящих и агентов за счет автоматизации работы службы поддержки. Объем китайского и европейского рынков глобального управления облачными ИТ-сервисами также ожидается рост. Ключевыми мировыми производителями облачных ИТ-сервисов для управления являются ServiceNow, HPE, IBM, BMC Software, CA Technologies и другие.

На основе нынешних и будущих тенденций был оценен размер рынка в период с 2018 по 2023 год, разделенного на компоненты и представленного на рисунке 1.

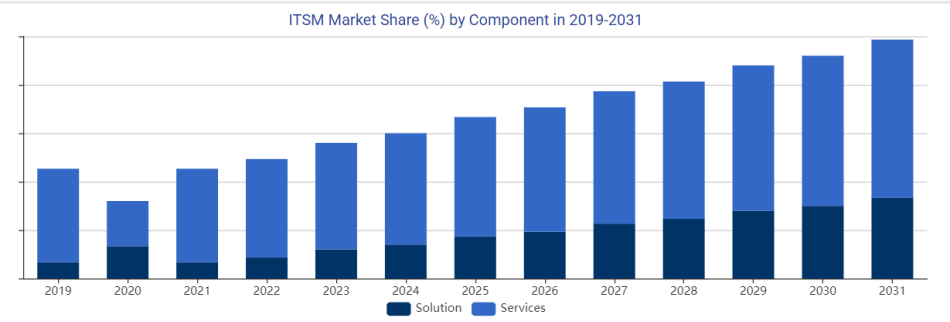

Рис. 1. Доля рынка ITSM (%) по компонентам в 2019-2031 годах, где черным выделена доля решений на рынке, а синим – услуг

Источник: https://www.cognitivemarketresearch.com/itsm-market-report

1. Методология ITIL

В методологии ITIL можно выделить следующие процессы и регламенты [2]:

1. Управление инцидентами

2. Управление изменениями
3. Управление каталогом услуг
4. Управление проблемами
5. Управление доступностью
6. Управление непрерывностью обслуживания
7. Управление событиями

Рассмотрим подробнее каждое из них, так как все они взаимосвязаны и составляю вместе единые регламенты, принимаемые в организациях.

1.1. Управление инцидентами

Управление инцидентами – регламентирует процесс обработки инцидентов и обеспечения скорейшего восстановления ИТ-услуг, сервисов, систем.

Инцидент – это нарушение в работоспособности ИТ-службы, сервиса или системы.

Инцидент содержит следующие данные (атрибуты) внутри себя:

1. Что необходимо сделать для его разрешения.
2. Кто что обязан сделать/проверить.
3. Какие сроки по действиям и жизненным циклам связанных сущностей.
4. Данные для эскалации.
5. Действия для сохранения доказательств и хронологи проделанных действий.
6. Приоритет.

Сотрудник службы поддержки проводит начальную диагностику самостоятельно или она проводится автоматически на основе собранной базы знаний. На ее основе определяется приоритет инцидента и производиться передача ответственной рабочей группе, в зону ответственности которой входит его разрешение. В случае, когда служба поддержки не может разрешить инцидент или целевое время для него было превышено, инцидент эскалируется для дальнейшего сопровождения и разрешения.

1.2. Управление изменениями

Изменением называют любое запланированное или незапланированное внесение изменения в систему/сервис/конфигурационную единицу(ы), внедрение которых должно минимально влияет на недоступность затронутых конфигурационных единиц.

Надзор за всеми изменениями осуществляет команда управления изменениями, при этом в самом внедрении она не участвует, так как это уже находится в зоне ответственности команды внедрения участвующих конфигурационных единиц. Чаще всего изменения делятся на стандартные, плановые и экстренные. К стандартным изменениям относятся повторяющиеся изменения с низким уровнем риска, которые уже не раз были протестированы. К плановым относятся все остальные запросы на изменения, которые внедряют для изменений настроек, доработок, кода, операционной системы и прочее, т.е. все остальные изменения, которые не входят в стандартные и экстренные. К экстренным относятся запросы на изменения, которые необходимо внедрить для предотвращения аварийной ситуации.

1.3. Управление каталогом услуг

Процесс управления каталогом услуг предоставляет информацию обо всех согласованных услугах всем уполномоченным лицам, а также создания и поддержки каталога.

Каталог услуг делится на две части по типу внесенных услуг (бизнес или техническая услуга).

1.4. Управление проблемами

Управление проблемами обеспечивает идентификацию проблем и выполняет анализ их первопричин. Проблема - это неизвестная причина одного или нескольких инцидентов. Процесс управления разделяется на два процесса: реактивное и упреждающее.

1.5. Управление доступностью

Управление доступностью контролирует и регламентирует доступность всех сервисов и компонентов в ит-ландшафте организации, и делится на реактивные и активные действия. В реактивные действия входит мониторинг, анализ и управление всеми событиями и остальными сущностями, связанными с недоступностью. В активные действия входят планирование, проектирование и повышение доступностью.

1.6. Управление непрерывностью обслуживания

Управление непрерывностью обеспечивает непрерывность работоспособности системы во время любой аварии.

1.7. Управление событиями

К событию относится то событие, которое имеет значение для предоставления ИТ-услуг. Управление событиями обеспечивает постоянный мониторинг всех конфигурационных единиц и определяет процесс категоризации этих событий.

1.8. Взаимосвязь сущностей процессов ITIL

Рассматривая взаимосвязи сущностей процессов ITIL, а также переход из одной сущности в другую, влияние и их связи, можно схематично изобразить для дальнейшего анализа и понимания. На рисунке 2 изображена схема отношений описанных ранее сущностей.

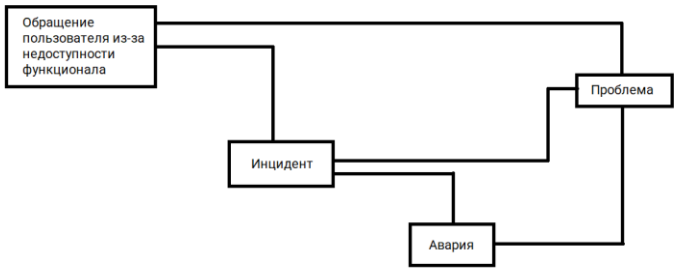

Рис. 2. Схема отношений сущностей «Инцидент», «Авария», «Проблема», «Обращение» процессов ITIL

1.9. Взаимосвязь понятий информационная система и надежности, а также смежных с ним понятиям

В современных тенденциях все большую популярность получают распределенные системы и сервисы. Распределенные системы, которые состоят из множества узлов, серверов и компонентов, часто подвержены различным видам отказов, таким как сбои оборудования, сбои сети, программные ошибки и т. д.

Надежность информационной системы можно разделить на две: функциональную и структурную [3].

Структура представляет собой совокупность элементов и их взаимосвязей. Она может быть изображена графически, описана в терминах теории множеств, представлена матрицами, графами и другими языками моделирования.

2. Система управления аварийными ситуациями

Для обеспечения и контроля непрерывности в организациях выделяют ответственный департамент, управление, отдел или команду. Для более эффективного выполнения поставленных задач повышения надежности и доступности систем, а также снижения времени простоя при сбое, используются системы управления аварийными ситуациями, которые должны быть интегрированы с различными технологиями для сбора, анализа и передачи данных для оперативного реагирования, а также используются HR-сервисы для получения персональных данных сотрудников, чтобы оперативно информировать их через средства связи и учитывать их доступность, избегая излишнего информирования во время их отсутствия на рабочем месте и потери времени на поиск замещающего сотрудника.

Для эффективного использования инструментов реагирования и управления необходимо обучать ответственный персонал, обладающий необходимыми навыками. Регулярные тесты [4] и обновления системы также необходимы для обеспечения ее эффективности и соответствия последним требованиям [5]. При проектировании систем управления и связи в рамках управления авариями в ИТ-услугах следует придерживаться следующих принципов:

1. Уведомление персонала организации, согласно штатного расписания о случившейся не штатной ситуации и/или чрезвычайного события, связанного с IT инфраструктурой. Уведомление должно

происходить по всем возможным доступным каналам связи и осуществляться как в автоматическом, так и в автоматизированном режимах.

2. Необходимость интеграции систем мониторинга, проводящих непрерывный контроль данных в ИТ-среду и ее связь с системой оповещения, что значительно сокращает время реакции на не штатное событие приводящие к аварии, анализ и предлагаемые способы ликвидации [6].

3. Процесс реагирования на аварийную ситуацию и предлагаемый способ ликвидации должен быть построен на разработанных политиках, в которых четко определяются роли субъектов, вовлеченных в процесс ликвидации, их обязанности и пределы допустимых, принимаемых решений.

4. Как процесс возникновения, так и ликвидации аварийной ситуации должен быть задокументирован и подвержен анализу. Результаты анализа должны быть заархивированы и являться исходными данными для построения дополнительных политик и выработок алгоритмов выявления не стандартных ситуаций [7].

5. В том случае, если авария привела к потере работоспособности как отдельных частей системы, так и ее в целом, необходимо иметь разработанный план восстановления, в котором определяется порядок восстановления и временные рамки.

6. На предприятии должен быть организован непрерывный цикл подготовки и переподготовки сотрудников, которые отвечают за инфраструктуру. Данный процесс должен включать в себя способы, методы и алгоритмы определения аварийных ситуаций и видов реакций.

7. Система должна иметь доступность, исходя из формулы 365x24x7, что повышает ее отказоустойчивость и резистентность к авариям.

8. Системы управления должны иметь возможность приспосабливаться к возможным изменениям бизнес процесса организации, перехода работы в различные технические среды, изменения нагрузки на отдельные составляющие.

9. Система должна иметь подсистему мониторинга отзывов и рекомендаций применения.

10. В целях повышения надежности системы, которая выражается в снижении возможных сбоев, в систему должны быть интегрированы методы безопасности приложений.

Исходя из указанных принципов, архитектура системы, которая позволяет системе быть работоспособной в случае аварийной ситуации, представлена на рисунке 3.

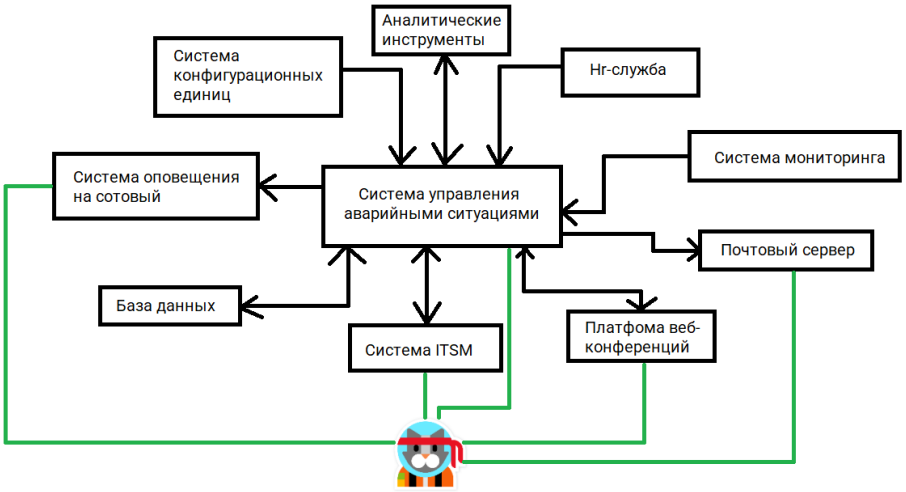

Рис. 3. Архитектура системы управления чрезвычайными ситуациями

На данном рисунке указаны два взаимодействия: первое взаимодействие – межсистемное, второе – пользователь-система, черные и зеленые линии соответственно. Информация о внештатной ситуации доводится до пользователя посредством SMS, сообщения в мессенджере или отправления письма на указанный почтовый ящик. Пользователь посредством системы управления чрезвычайными ситуациями и системы уведомлений взаимодействует с другими пользователями в соответствии с политиками и регламентами, которые позволяют на первом этапе выявить и локализовать произошедшую аварию, а в дальнейшем ее полностью устранить, так же, данные системы позволяют проводить контроль параметров надежности системы в целях обеспечения ее работоспособности. С помощью системы ITSM пользователь может управлять активами, созданными по методологии ITSM.

Поскольку данная система предназначена для оповещения о чрезвычайных ситуациях и их управления, отказоустойчивость является одним из ключевых требований, что гарантирует

стабильную работу системы управления чрезвычайными ситуациями даже при сбоях на других информационных системах. Для реализации этого требования необходимо строить систему с учетом георезервирования (нахождение компонентов системы в нескольких кластерах, развернутых в разных центрах обработки данных (ЦОД)), реализацию закрытой инфраструктуры, дублирование и резервное копирование всей информации, а также предусмотреть возможности масштабируемости и гибкости системы [8].

2.1. Применение конечных автоматов

Набор состояний распределенной информационной системы, которые она может принимать после выполнения определенных методов, является конечным. Переходы между состояниями можно представить с помощью сети, где узлы соответствуют состояниям, а соединения между узлами – переходам.

Конечный автомат представляет собой математическую абстракцию, моделирующую поведение системы при изменении состояний в ответ на определенные триггеры. Конечный автомат можно изобразить в виде графа, который показывает набор состояний и возможные переходы между ними, что позволяет оценить надежность системы, моделируя все возможные состояния и переходы и ведет к выявлению потенциальных ошибок и узких мест, которые могут привести к сбоям и проблемам с отказоустойчивостью.

Рассмотрим конечный автомат процесса управления чрезвычайными ситуациями, описав алгоритм в виде последовательности действий:

1. Старт: Регистрация аварийной ситуации
2. Шаг 1: Уведомление ответственного лица
3. Шаг 2: Открытие веб-конференции по аварии
4. Шаг 3: Уведомление команды Восстановления
5. Шаг 4: Назначение координатора аварии
6. Шаг 5: Оценка воздействия и определение уровней важности
7. Шаг 6: Принятие решения о плане DRP или Stand-In
8. Шаг 7: Документирование.
9. Шаг 8: Создание объекта проблемы и инструкций по ее предотвращению и не повторению в будущем.
10. Шаг 9: Закрытие аварии

2.2. Применение резонанса

У распределённых информационных систем, в особенности в масштабах крупных организации, в особенности при применении микросервисной архитектуры, частичная потеря функциональности не обозначает полную деградацию системы. В таком случае можно говорить, что у системы существует множество входов и выходов.

Резонанс в физике — это охват колебательной системы периодическим воздействием внешней силы, синхронизирующим колебания системы с частотой внешнего воздействия [9]. В результате этого процесса возрастает амплитуда вынужденных колебаний. Резонанс – это также явление, при котором собственное колебательное движение становится вынужденным и постоянно увеличивает свою амплитуду из-за воздействия окружающей среды. Это явление подразумевает совпадение частоты колебаний данной системы и внешних сил, действующих на неё, что приводит к увеличению амплитуды колебаний системы.

Рассматривая резонанс в плоскости надежности информационных систем, можно говорить, что резонанс – явление, когда из-за воздействия окружающей среды состояния информационная систем значительно колеблются от работоспособного до полной деградации.

В математике при умножении отрицательных чисел «минус на минус» результат становится положительным. По аналогии можно предположить, что в процессе эксплуатации системы могут существовать ситуации, когда засчет одного сбоя решается другой сбой. Примером такой ситуации служит: в случае атаки на сервер рекомендуемым решением является отключение «зараженного» сервера от сети организации, но само отключение сервера от сети является ситуацией сбоя, т.к. теряется работоспособность сервера. Также можно рассмотреть процесс переадресации – подмены одного адреса на другой – что также является сбоем и одновременно в некоторых ситуациях – лекарством. В таком случае в системе управления аварийными ситуациями можно предусмотреть использования таких сценариев, где решением проблемы будет представлять экстренное решение, которое в отдельном случае рассматривалось бы как сбой системы.

3. Заключение

Структурная надежность распределенной системы требует комплексного подхода, который включает в себя не только технические меры, но и правильное проектирование, архитектуру и управление системой. Все это совместно обеспечивает высокий уровень надежности и доступности распределенных систем.

Проблема использования искусственно созданных сбоев для решения других сбоев не до конца изучена, а также инструмент, который бы позволял использовать такие сценарии, не реализован. Данную проблему необходимо изучать и применять в процессе восстановления систем, учитывая, что использование данных сценариев неквалифицированными работниками может привезти к еще более худшим результатам деградации. Хотелось бы отметить, что данный инструмент может позволить кратно сократить время простоя системы при аварийной ситуации на ней, но на данный момент его не существует, так как его неправильное применение может в свою очередь кратно увеличить время простоя, что может принести репутационные, финансовые и регуляторно-правовые риски организации.

Литература

1. *Лорьер Ж.-Л.* Системы искусственного интеллекта – пер. с Франц. – М: Мир, 1991. – 568 с.
2. *Ковалев А.В.* Доступный ITIL: настольная книга ИТ-руководителя. ч. 1: Эксплуатация сервисов. – 1-е изд. – М: Тезаурус, 2018. – 458 с.
3. *Гадасин Д.В., Кольцова А.В., Полякова А.Н.* Отображение жизненного цикла виртуального субъекта в поведенческую модель // Технологии информационного общества: Сборник трудов XIV Международной отраслевой научно-технической конференции. – М: ИД Медиа Паблишер, 2020. – Т. 1. – С. 262– 264.
4. *Zolotukhin P.A., Melkova E.K., Gadasin D.V., Korovushkina V.M.* Using Intelligent Testing as a Tool to Improve the Quality of Transport Information Systems // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications. – US: Institute of Electrical and Electronics Engineers Inc, 2022.
5. *Шведов А.В., Гадасин Д.В., Коровушкина В.М., Мелькова Е.К.* Интеллектуальное тестирование как способ повышения качества информационной системы // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12 N 2. – С. 43– 52.
6. *Гадасин Д.В., Каледина А.В.* Использование современных средств мониторинга для анализа состояния IT-систем // Технологии информационного общества: Сборник трудов XIV Международной отраслевой научно-технической конференции. – М: ИД Медиа Паблишер, 2020. – Т. 1. – С. 267–269.
7. *Ларичев О.И.* Наука и искусство принятия решений. – М: Наука, 1979. – 200 с.
8. *Бритков В.Б.* Архитектура интеллектуальных информационных систем для принятия решений // Проблемы и методы принятия решений в организационных системах управления. – М: ВНИИСИ АН СССР, 1988. – С. 31–32.
9. *Алексеев И. А.* Стихийные явления в природе. – М: Мысль, 1988. – 255 с.