12.2. Процесс: INCIDENT MANAGEMENT - Управление инцидентами

Управление инцидентами (Incident Management) - *процесс, отвечающий за управление жизненным циклом всех инцидентов. Основная цель Управления инцидентами - скорейшее восстановление услуги для пользователей.*

Инцидент (Incident) - *незапланированное прерывание услуги или снижение качества услуги. Сбой конфигурационной единицы, который еще не повлиял на услугу, также является инцидентом. Например, сбой одного диска из массива зеркалирования.*

Как видно из определения процесса, Управление инцидентами предназначено для **максимально быстрого** восстановления нормальной эксплуатации услуги и минимизации неблагоприятного влияния на бизнес в случае возникновения инцидента.

Под "нормальной эксплуатацией услуги" здесь понимается *эксплуатация* в соответствии с *SLA*. Процесс рассматривает все события, которые нарушают или могут нарушить нормальную эксплуатацию услуги.

Информация о таких событиях может поступать из разных источников, основными из которых являются звонки пользователей и технического персонала в сервис-деск и *процесс Управления* Событиями.

Ценность Управления инцидентами для бизнеса более очевидна, чем у других процессов этапа Преобразования. Часто именно этот процесс является основой для формирования обоснования бизнесу о необходимости остальных процессов этапа Преобразования. В частности, Управление инцидентами помогает бизнесу тем, что:

- Быстро находит и разрешает инциденты, в результате чего снижается время простоя услуг, что в целом увеличивает показатели доступности услуг;
- Выравнивает деятельности IT в соответствии с приоритетами бизнеса;
- Увеличивает способность выявления возможностей для улучшения услуг в результате расследования инцидентов;
- Сервис-деск, разрешая инциденты, определяет дополнительные требования IT и бизнеса к услугам и обучению.

Время разрешения инцидента обычно формализовано в рамках *SLA*, OLA и других базовых соглашений. Команды поддержки должны быть готовы к соблюдению временных ограничений.

***ITIL* вводит также понятие Модель инцидентов, которая включает в себя:**

- Шаги, которые необходимо предпринять для того, чтобы разрешить инцидент;
- Хронологический порядок шагов;
- Распределение ответственностей - кто и что делает;
- Временные рамки и пороговые величины для завершения каждого действия;
- Вопросы того, с кем необходимо связать и на каком этапе;

Таким образом, Модель инцидентов описывает последовательность действий при возникновении определенного типа инцидентов. Использование моделей инцидентов позволяет стандартизовать *процесс Управления* инцидентами и ускорить его.

Этот подход применим в отношении часто возникающих "стандартных" инцидентов. "Нестандартные" случаи обрабатываются отдельно, например, инциденты, связанные с информационной безопасностью.

В отдельную категорию выделяются "значительные инциденты", которые должны разрешаться максимально быстро. Значительный инцидент (Major *Incident*) наивысшая категория влияния для инцидента. Значительный инцидент означает значительные потери для бизнеса. То, какие инциденты будут считаться значительными, каждая организация решает индивидуально.

На рис. 12.2 схематически отображены основные деятельности в рамках Управления инцидентами.

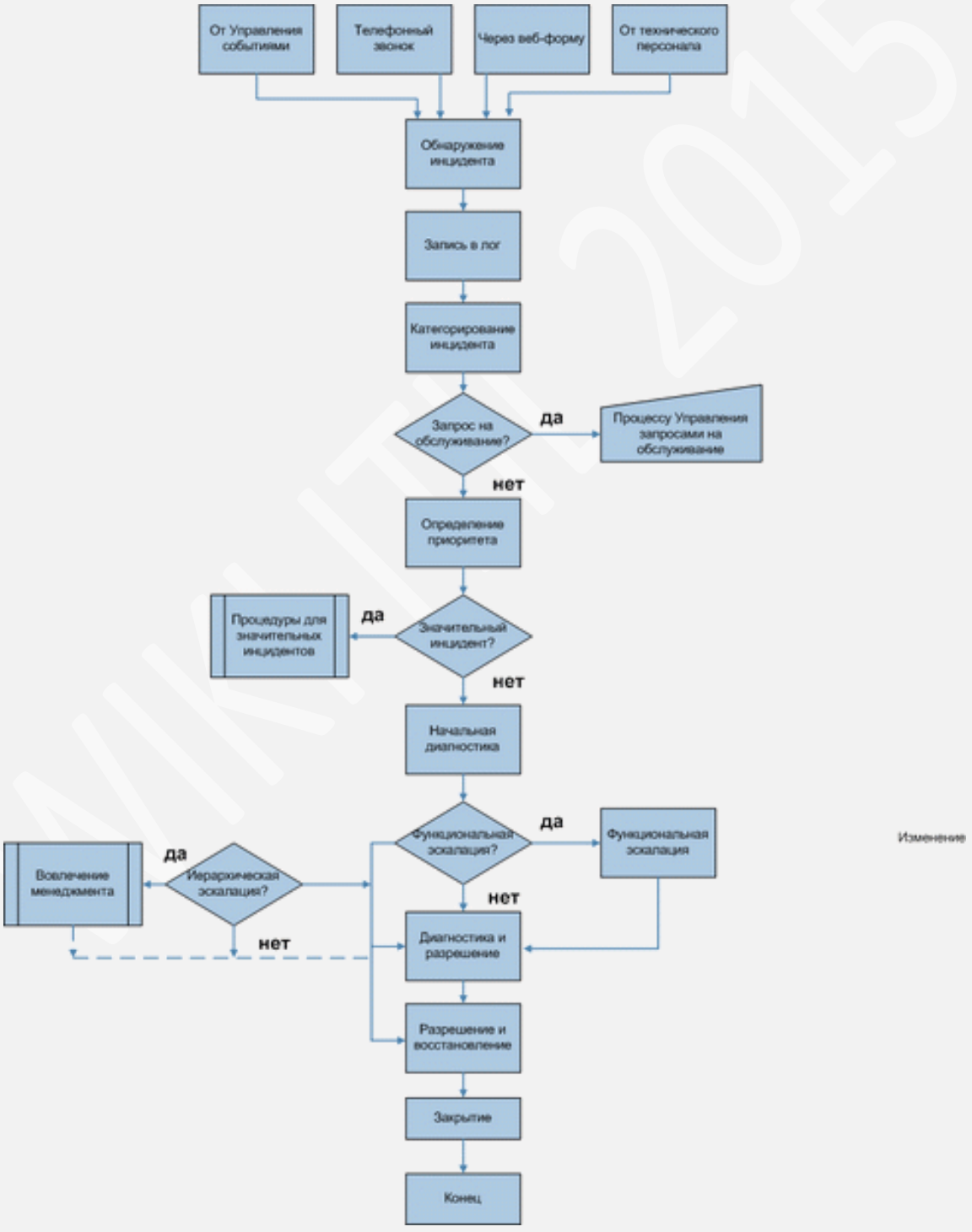

Рис. 12.2. Процесс Управления инцидентами

Рассмотрим основные этапы, изображенные на рис. 12.2.

Для того чтобы разрешить инцидент, его необходимо сначала обнаружить, то есть **идентифицировать**.
С точки зрения непрерывности бизнеса неприемлемо ждать обращений пользователей или технического персонала в сервис-деск. Все ключевые компоненты должны контролироваться, чтобы своевременно обнаруживать сбои или возможности их возникновения.

После того, как инцидент обнаружен, информацию о нем необходимо занести в лог. В логе должно быть отображено время обнаружения инцидента, вне зависимости от того, как он был обнаружен - по звонку в сервис-деск или в результате работы автоматических агентов. В логе также необходимо записать всю связанную с инцидентом информацию. *Запись* об инциденте должна послужить базой для его разрешения соответствующей командой поддержки.

***Запись* об инциденте должна включать:**

- Уникальный идентификатор инцидента;
- Категорию инцидента;
- Срочность инцидента.
  Срочность (urgency) *- мера того, насколько быстро с момента своего появления инцидент, проблема или изменение приобретет существенное влияние на бизнес. Например, инцидент с высоким уровнем влияния может иметь низкую срочность до тех пор, пока это влияние не затрагивает бизнес в период закрытия финансового года. Влияние и срочность используются для назначения приоритета.*
- Влияние инцидента;
- Приоритет инцидента;
- Дата и время записи;
- Имя/id человека или группы, сделавшей запись об инциденте;
- Метод уведомления;
- Имя/отдел/номер/расположение пользователя;
- Метод обратной связи;
- Описание симптомов;
- Статус инцидента;
- Связанные конфигурационные единицы;
- Группа поддержки/сотрудник, к кому переадресован инцидент;
- Связанная с инцидентом проблема/известная ошибка;
- Деятельности, осуществленные для разрешения инцидента;
- Время и дата разрешения инцидента;
- Категория закрытия;
- Время и дата закрытия.

Следующий этап разрешения инцидента - ***категорирование***. Оно необходимо для дальнейших *работ*, в частности, поиска известных ошибок и проблем, которые могли послужить причиной для возникновения инцидента.

Обычно используется три-четыре уровня *категорирования* (рис. 12.3).

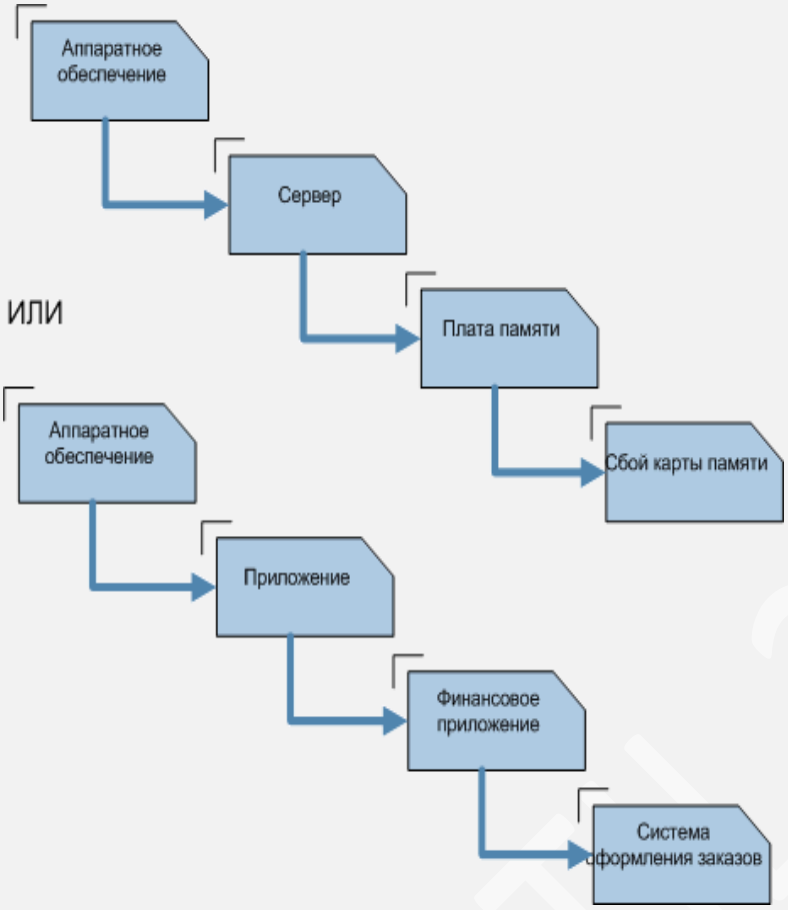

Рис. 12.3. Варианты категорирования инцидентов

Нет стандартных методов для *категорирования* инцидентов, каждая организация сама определяет, какие категории будет использовать.

Приоритет инцидента определяется исходя из двух понятий - срочности и влияния. Влияние в отношении инцидентов чаще всего определяется на основе количества пользователей, которые он затронул. Тем не менее, этот показатель не всегда является объективным. В некоторых случаях влияние инцидента даже на одного единственного пользователя может оказать значительное негативное влияние на бизнес в целом.

Другие факторы, которые можно использовать для оценки влияния:

- Риск для жизни или сегмента;
- Количество услуг, которые затрагивает инцидент;
- Уровень финансовых потерь;
- Влияние на бизнес-репутацию;
- Возникновение нарушений законодательства и требований регуляторов.

Ниже приведен пример матриц для определения **приоритета инцидента** и времени, в течение которого его необходимо разрешить.

Код приоритета определяют влияние и срочность	Влияние		
	Высокое	Среднее	Низкое
Высокая	1	2	3
Средняя	2	3	4
Низкая	3	4	5

Код приоритета	Описание	Крайний срок исполнения
1	Критический	1 час
2	Высокий	8 часов
3	Средний	24 часа
4	Низкий	48 часов
5	Планируемый	В соответствии с планом

Для персонала поддержки необходимо разработать четкие инструкции определения приоритета инцидента на основе срочности и влияния на бизнес. Необходимо отметить, что приоритет инцидента может меняться в зависимости от изменения окружающих условий и требований бизнеса.

Далее следует **этап начальной диагностики**.

В первую *очередь* он относится к инцидентам, поступившим в сервис-деск. Специалист службы сервис-деск должен попытаться найти причину, вызвавшую инцидент, понять, что именно работает некорректно и выявить максимальное количество характеристик инцидента во время связи с пользователем, например, по телефону. Другими словами, специалист должен попытаться решить инцидент и закрыть его. Если это невозможно, он сообщает пользователю идентификационный номер инцидента.

Если сервис-деск не может разрешить инцидент или сроки первой ступени разрешения инцидентов истекли, инцидент должен быть немедленно передан дальше.

Эскалация (Escalation) - *деятельность*, направленная на получение дополнительных ресурсов, когда это необходимо для достижения Целевых показателей уровня услуги или ожиданий заказчиков. Эскалация может потребоваться в рамках любого процесса Управления услугами, но наиболее часто ассоциируется с Управлением инцидентами, Управлением проблемами и управлением жалобами заказчика. Существует два типа эскалации: функциональная эскалация и Иерархическая эскалация.

- **Функциональная эскалация.** Функциональная эскалация подразумевает передачу инцидента в группу поддержки с более высокой квалификацией и компетенцией. При этом если очевидно, что второй *уровень поддержки* не сможет разрешить инцидент, его можно сразу передать на третий *уровень поддержки*. Третий *уровень поддержки* может включать в себя не только сотрудников организации, но и поставщиков, вендоров и т.п. При этом ответственность за уведомление пользователя о ходе разрешения инцидента остается на сервис-деске, вне зависимости от того, где инцидент рассматривается на данный момент.
- **Иерархическая эскалация.** Иерархическая эскалация подразумевает вовлечение или просто информирование руководителей более высокого уровня о возникновении инцидента. Она способствует своевременному принятию решений относительно выделения дополнительных ресурсов и вовлечения внешних организаций в процесс разрешения инцидента.

Следующий этап разрешения инцидентов называется **исследование и диагностика**.
В случаях, когда пользователи обращаются только для поиска информации, сервис-деск должен предоставить ее в минимальные сроки. Но если сообщается о наличии сбоя, это требует определенных действий по исследованию и диагностике инцидента. При этом все предпринятые действия должны быть отображены в записи об инциденте.

Действия чаще всего включают в себя:

- Установление того, что именно не работает или что именно ищет пользователь;
- Определение хронологии событий;
- Оценка влияния инцидента, в том числе количества пользователей, которых он затронул;
- Поиск в базе знаний аналогичных случаев в прошлом.

Когда потенциальное разрешение инцидента определено, необходимо провести тестирование того, что действия по восстановлению завершены, и услуга полностью восстановлена для пользователей. *Группа*, разрешившая инцидент, должна передать его на закрытие сервис-деску.

Сервис-деск, в свою *очередь* проверяет, что все действия, необходимые для разрешения инцидента, выполнены, пользователи удовлетворены и согласны закрыть инцидент.

Это включает в себя следующее:

- Закрытие *категорирования* - производится проверка корректности изначально установленной категории инцидента. Если она оказалось неправильной, ее исправление и занесение изменений в запись об инциденте;
- Опрос удовлетворенности пользователей - - осуществляется по звонку или электронной почте для статистики и отображения эффективности работы сервис-деска;
- Проверка полноты записи об инциденте;
- Определение того, какая проблема вызвала инцидент, является она постоянной или периодически повторяющейся. Сюда относится также определение проактивных действий по предотвращению инцидентов этого типа в дальнейшем и формирование записи о проблеме, если она новая;
- Формальное закрытие инцидента - формальное закрытие записи об инциденте.

В некоторых случаях инцидент может быть повторно открыт даже после формального закрытия. Правильным будет заранее определить правила о том, как, когда и при каких условиях инцидент может быть повторно открыт. Это используется, в частности, когда в один и тот же день возникают одинаковые инциденты. Для нового инцидента, тем не менее, необходимо сформировать новую *запись* со ссылкой на предыдущий инцидент. *Запись* о предыдущем инциденте может быть использована для разрешения нового.

Метриками эффективности процесса Управления инцидентами могут быть:

- Общее количество инцидентов;
- Количество инцидентов, находящихся на разных стадиях - закрыт, в работе, передан и т.п.
- Размер текущего лога об инцидентах;
- Количество значительных инцидентов;
- Среднее время разрешения инцидентов;
- Процент инцидентов, разрешенных в согласованное время разрешения инцидентов;
- Средние затраты на инцидент;
- Количество повторно открытых инцидентов и их процентное соотношение к общему количеству инцидентов;
- Количество инцидентов, неправильно назначенных в команды поддержки;
- Количество инцидентов, для которых были неправильно определены категории;
- Количество удаленно разрешенных инцидентов (без персонального присутствия);
- Количество инцидентов, разрешенных с использованием каждой модели инцидентов;
- Количество инцидентов в разрезе определенных интервалов дня.

Для эффективного Управления инцидентами необходимо обеспечить следующее:

- Способность обнаруживать инциденты как можно раньше. Это включает в себя обучение пользователей немедленно сообщать об инцидентах и конфигурирование инструментов управления событиями;
- Убедить персонал в том, что все инциденты должны быть занесены в журнал;
- Доступность информации об известных проблемах и ошибках. Это позволит персоналу использовать опыт предыдущих инцидентов;
- Взаимодействие с cms для определения взаимосвязей конфигурационных единиц и обращения к их истории для поддержки первого уровня;
- Взаимодействие с *slm* для корректной оценки инцидентов, расстановки приоритетов и выполнения процедур эскалации. *Slm* в свою очередь может использовать информацию от управления инцидентами для определения того, что целевые уровни производительности реалистичны и могут быть достигнуты.

Основные риски для процесса Управления инцидентами:

- Большое количество инцидентов, которые не могут быть разрешены в установленные сроки в связи с недостатком ресурсов или их недостаточной подготовкой;
- Приостановка разрешения инцидентов из-за некорректной работы поддерживающих инструментов;
- Недостаточность или несвоевременность информации из-за некорректной работы поддерживающих инструментов или плохой взаимосвязи с другими процессами;
- Несоответствия с основными контрактами и соглашениями, которые возникают вследствие их плохой проработки и не-реалистичности согласованных целевых показателей.