УДК 519.876.2

К ПОСТРОЕНИЮ ПРОЦЕДУР ПРОТИВОДЕЙСТВИЯ ПРОИСШЕСТВИЯМ, ВОЗНИКАЮЩИМ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ ИТ-СЕРВИСОВ

С. М. Кулаков, М. В. Пургина, В. В. Зимин, Р. С. Койнов

Сибирский государственный индустриальный университет

Поступила в редакцию 17.03.2015 г.

Аннотация. В статье выполнена математическая постановка частных задач противодействия ИТ-происшествиям (событиям, инцидентам, проблемам), возникающим в процессе эксплуатации ИТ-сервисов и предложена комплексная процедура их обработки, включающая алгоритм распознавания категории каждого ИТ-происшествия, а также человеко-машинные механизмы предотвращения воспроизводства нежелательных происшествий.

Ключевые слова: жизненный цикл сервиса, стадия эксплуатации, ИТ-сервис, ИТ-провайдер, ИТ-актив, ИТ-событие, ИТ-происшествие, ИТ-инцидент, ИТ-проблема, процедура распознавания.

Annotation. In the article the mathematical formulation of the specific objectives of combating IT-occurrences (events, incidents, problems) that occur during operation of IT- services is made and the complex procedure of their processing, including the recognition category algorithm for each IT- incident suggested, as well as man-machine mechanisms of the reproduction of undesirable incidents prevention.

Keywords: service life cycle, operation stage, IT- service, IT-provider, IT-asset, IT-event, IT-occurrence, IT-incident, IT-problem, recognition procedure.

ВВЕДЕНИЕ

Одним из концептуальных положений, составляющих основу современного подхода к организации ИТ-деятельности, является ее структуризация на основе представлений *о жизненном цикле* продукта (результата) деятельности, которым является ИТ-сервис. В соответствие со стандартом ISO 9004-1 – *жизненный цикл изделия (сервиса) (ЖЦИ)* – совокупность взаимосвязанных процессов, выполняемых от момента выявления потребностей в определенном продукте (сервисе) до момента удовлетворения этих потребностей и утилизации продукта (сервиса) [1, 2].

Все стадии жизненного цикла ИТ-сервиса (разработка стратегии, проектирование, внедрение, эксплуатация, утилизация) имеют важное значение не только для разработчика и поставщика, но и для потребителя этого сервиса. На стадиях стратегии, проектирования и внедрения разрабатываются и тестируются модельные и натурные компоненты ИТ-сервиса, которые при итоговом развертывании в продуктивной ИТ-среде трансформируются в реальные сервисные активы. На стадии *эксплуатации* осуществляется повседневная работа с инфраструктурой, которая используется для поставки ИТ-сервисов. Важнейшая цель провайдера на этой стадии – координация выполнения работ и процессов, необходимых для предоставления и управления сервисами в соответствии с согласованным уровнем обслуживания SLA [3]. На стадии эксплуатации сервиса реализуются следующие процессы, играющие важную роль в системе управления ИТ-сервисами: обработка событий, инцидентов, разрешение проблем, выполнение запросов на обслужи-

вание, управление правами доступа к сервисам, реализация приложений и др. Повышая эффективность процессов, ИТ-провайдер улучшает качество предоставляемых потребителю сервисов (услуг) [4].

При значительном количестве поставляемых ИТ-провайдером сервисов, а также в силу большого многообразия сервисных активов, различных внешних и внутренних возмущающих воздействий (внедрение нового оборудования и программного обеспечения; изменение законодательства или других нормативных актов; изменение потребностей бизнеса; повышение требований к качеству процесса, процедуры, инструментария; организационные изменения и т. п.), функционирование реальных ИТ-сервисов в бизнес-процессах потребителей может не соответствовать функционированию, предписываемому нормативными моделями. При этом возникает большое количество отклонений в работе сервисов (ИТ-происшествий[1]) от их нормативного функционирования, исчисляемое сотнями и тысячами в сутки. Вследствие этого снижается результативность активов потребителя ИТ-сервиса. Эффективность стадии эксплуатации во многом определяется возможностями ИТ-провайдера контролировать состояние ИТ-активов, способностью своевременно обнаруживать и устранить отклонения от нормативного или ожидаемого функционирования режима функционирования ИТ-активов.

Качественная обработка и устранение интенсивного потока отклонений, существенно влияющих на удовлетворенность клиентов, и, следовательно, на конкурентоспособность ИТ-провайдера, представляет собой непростую задачу и требует создания специальной системы управления. Цель этой системы состоит в эффективном, то есть с минимальным снижением удовлетворенности клиента и с допустимыми затратами, восстановлении нормативного функционирования сервисов при возникновении отклонений.

[1]ИТ-происшествие – проявление (результат) контролируемого или неконтролируемого возмущающего воздействия в форме отклонения от нормативного режима функционирования какого-либо сервисного ИТ-актива.

Широко применяется разбиение множества возможных отклонений (ИТ-происшествий) на классы. В качестве оснований для классификации обычно используются два основных свойства ИТ-происшествий:

– Активообусловленность (тип) происшествия, то есть его связь с типом некорректно функционирующего ИТ-актива, который определяет специализацию ИТ-деятельности по восстановлению штатного функционирования актива. ITIL-3 различает девять типов ИТ-активов: финансовый капитал, инфраструктура, приложения, информация, управленческие активы, организационные решения, знания, персонал, ИТ-процессы;

– Степень влияния (вид) происшествия на ключевую для клиента характеристику сервисов – доступность[2]. Знание степени влияния позволяет сформулировать цель системы противодействия ИТ-происшествиям, исходя из интересов потребителей сервиса, на практике по этому свойству различают три вида происшествий: *события*, *инциденты*, *проблемы* [4].

Событие – обнаруженное некорректное функционирование любого ИТ-актива, не приводящее к недоступности сервиса (сервисов) для пользователей. Событие является «предвестником» будущей недоступности сервисов. С позиции теории управления событие представляет собой эффект контролируемого возмущения для системы управления эксплуатацией сервисов.

Инцидент – обнаруженное некорректное функционирование ИТ-актива, которое приводит к потере доступности ИТ-сервиса (сервисов) для пользователей, и которое не связано с ошибкой проектирования или неэффективным проектным решением. С позиции теории управления инцидент также является эффектом контролируемого возмущения.

Проблема – обнаруженное некорректное функционирование ИТ-актива, которое приводит к потере доступности ИТ-сервиса для пользователей и связано с наличием ошибки

[2]Доступность сервиса – готовность ИТ-сервиса к реализации предусмотренной процедуры в согласованное время.

или неэффективностью проектного решения. Проблема проявляется в многократно воспроизводящихся инцидентах («проблемных» инцидентах). С позиции теории управления проблема является эффектом неконтролируемого возмущения.

Категория конкретного ИТ-происшествия определяется сочетанием вида и типа происшествия. При девяти типах активов и трех видах происшествий получаем двадцать семь возможных категорий и соответствующих им классов ИТ-происшествий. Для каждого класса необходим специализированный механизм (процедура) распознавания, предотвращения и снижения последствий происшествий (механизмы управления и противодействия).

Важнейший принцип, которому должен следовать ИТ-провайдер при управлении доступностью сервисов состоит в постоянном выявлении проблемных областей, определении и реализации мер, которые увеличивают удовлетворенность потребителя. Для этого необходимо, чтобы механизм управления доступностью взаимодействовал с механизмом обработки инцидентов и был ориентирован на снижение продолжительности устранения каждого инцидента, а также на исключение их повторения. Такое взаимодействие позволит механизму управления доступностью учитывать фактические значения показателей инцидентов, а также данные для анализа трендов. Эти сведения могут быть использованы в качестве исходных данных для процедуры анализа отказов сервисов (SFA), для корректировки плана непрерывных улучшений (SIP) и регулярной отчетности. Кроме того они позволяют установить целевые значения для показателей качества отдельных этапов жизненного цикла инцидента. Достижение требуемых уровней доступности и обеспечение быстрого восстановления ИТ-сервиса после отказа требует инвестиций в систему эксплуатации и инструментальные средства управления. Последние являются существенным ресурсом, который помогает обеспечить высокий уровень доступности и сократить продолжительность простоя ИТ-сервиса [4].

1. ЗАДАЧА РАСПОЗНАВАНИЯ КАТЕГОРИИ ИТ-ПРОИСШЕСТВИЯ

Распознавание происшествия вида события является тривиальной задачей, так как инструмент его обнаружения регистрирует необходимые данные для определения категории [5]. Далее ограничимся рассмотрением задачи распознавания «*проблемных*» и «*не проблемных*» (простых) инцидентов. Первые могут быть устранены посредством инициирования и реализации изменений ИТ-сервиса. Результат распознавания может быть как верным (простой инцидент распознается как «простой» а проблемный – как «проблемный»), так и неверным (простой инцидент распознается как «проблемный», а проблемный – как простой). При неверном распознавании реализуется «холостой» проектный цикл изменения ИТ-актива механизмом $P(J_k)$ устранения проблем, либо разрешение реальной проблемы откладывается, что приводит к увеличению числа повторных «проблемных» инцидентов.

Пусть $CI^q = \{ci_n^q \mid n = \overline{1, N^q}\}$ – некоторая ИТ-конфигурация[3], которая отражена в базе данных конфигураций (CMDB) ИТ-провайдера, здесь ci_n^q – компоненты конфигурации[4], N^q – количество компонентов конфигурации [2], а $b(ci_n^q) = \{b_m(ci_n^q) \mid m = \overline{1, M_n^q}\}$ – базовый уровень характеристик компоненты конфигурации ci_n^q, описываемый совокупностью нормативных значений его параметров b_m и количеством параметров M_n^q, соответствующих штатному режиму функционирования. Определим базовый уровень $B(CI^q)$ характеристик конфигурации CI^q как совокуп-

[3]**Конфигурация** (стадия «Внедрение сервиса») – общий термин, применяемый для описания совокупности взаимосвязанных частей поставляемого ИТ-сервиса. Термин «конфигурация» также применяется для описания параметров настройки одной или нескольких конфигурационных единиц.

[4]**Компонента конфигурационного элемента** – конфигурационный элемент, являющийся частью процедуры сборки. Например, конфигурационный элемент «CPU», или «память», может быть частью конфигурационного элемента «сервер».

ность базовых уровней характеристик ее компонентов: $B(CI^q)=\{b(ci_n^q)\,|\,n=1,N^q\}$. Под ИТ-происшествием $b^{\Delta}(ci_n^q)$ с конфигурационным элементом ci_n^q будем понимать зафиксированное отклонение фактических значения характеристики b конфигурационного элемента ci_n^q от нормативного уровня: $b^{\Delta}(ci_n^q)=\{b_i^{\Delta}(ci_n^q)\,|\,l\in L\subset 1,M_n^q\}$, где L – количество характеристик конфигурационного элемента, не соответствующих базовому уровню, b_i^{Δ} – отклонение фактического значения характеристики от нормативного. Определим происшествие $B^{\Delta}(CI^q)=\{b^{\Delta}(ci_n^q)\,|\,n=1,N^q\}$ с конфигурацией CI^q, как совокупность происшествий с составляющими её компонентами. Обозначим через $\sigma(b^{\Delta}(ci_n^q))$ процедуру распознавания происшествия $b^{\Delta}(ci_n^q)$, вызвавшего отклонение.

Пусть $I=\bigcup_{k=1}^{K} I_k$ – множество инцидентов, а $J=\bigcup_{k=1}^{K} J_k$ – множество проблем, являющихся результатом распознавания процедурой $\sigma(b^{\Delta}(ci_n^q))$ происшествий в плановом периоде времени $[0,T]$, где k – тип ИТ-актива,

$$I_k=I_k^{er}(\sigma(b^{\Delta}(ci_n^q))\bigcup I_k^{cor}(\sigma(b^{\Delta}(ci_n^q)),$$

$$J_k=J_k^{\mathrm{er}}(\sigma(b^{\Delta}(ci_n^q))\bigcup J_k^{cor}(\sigma(b^{\Delta}(ci_n^q)),$$

а $I_k^{er}(\sigma(b^{\Delta}(ci_n^q)))$, $J_k^{er}(\sigma(b^{\Delta}(ci_n^q)))$ – множества некорректно распознанных процедурой $\sigma(b^{\Delta}(ci_n^q))$ происшествий с активами типа k. Некорректно распознанные инциденты $-I_k^{er}$ порождают в плановом периоде множество $-I_k(I_k^{er})$ повторных инцидентов.

Пусть также $z(P(I_k))$ и $z(P(J_k))$ – нормативные затраты на минимизацию последствий, соответственно, одного инцидента и одной проблемы k-го типа.

Тогда математическую постановку задачи разработки процедуры $\sigma(b^{\Delta}(ci_n^q))$ распознавания происшествий можно формализовать следующим образом:

$$Z_k^{er}=\sum_{k=1}^{K}|\,I_k(J_k^{er}(\sigma_k(b^{\Delta}(ci_n^q))))\,|\,z(P(I_k))+$$

$$+\sum_{k=1}^{K}|\,I_k^{er}(\sigma_k(b^{\Delta}(ci_n^q)))\,|\,z(P(J_k))\to\min_{\{\sigma_k(b^{\Delta}(ci^q))\}}\qquad(1)$$

$$\sum_{k=1}^{K}\{|\,I_k\,|\,z(P(I_k)+|\,J_k\,|\,z(P(J_k)\}\le Z^*.$$

Содержательно запись (1) соответствует разработке такой процедуры $\sigma(b^{\Delta}(ci_n^q))$ распознавания ИТ-происшествий, которая минимизирует совокупные затраты на устранение повторных инцидентов и ошибочно выявленных проблем (некорректно распознанных инцидентов) при затратах на устранение последствий всех инцидентов и проблем в расчетном периоде $[0,T]$, не превосходящих Z^*. При неразвитом экономическом менеджменте ИТ-провайдера, не позволяющем оценить затраты на устранение инцидентов и проблем, задачу (1) можно упростить и минимизировать, например, общее количество повторных инцидентов, то есть построить процедуру $\sigma(b^{\Delta}(ci_n^q))$ распознавания категории происшествия по критерию количества повторных инцидентов за период $[0,T]$. На рис. 1 приведена упрощенная процедура распознавания категории ИТ-происшествия, которая в явном виде не учитывает критерий Z_k^{er}. Для включения в нее алгоритма оптимизации распознавания необходимо оценить частоту повторных инцидентов и ошибок выявления проблем (по данным о работе действующей системы).

На рис. 1 CMDB – конфигурационная база данных, KMDB – база знаний.

2. ЗАДАЧА РАЗРАБОТКИ ПРОЦЕДУРЫ УСТРАНЕНИЯ (МИНИМИЗАЦИИ ПОСЛЕДСТВИЙ) ИНЦИДЕНТОВ

Пусть $I=\{i\}$ – множество инцидентов, произошедших на некотором плановом интервале времени $[0,T]$, а $\{I_k\,|\,k\in\overline{1,K}\}$ – разбиение множества I на классы, где I_k – подмножество инцидентов типа k, т. е. $I=\bigcup_{k=1}^{K} I_k$ и $I_k\bigcap I_p=\varnothing,\quad k\ne p.$ Пусть также $P^*(I)=\{P^*(I_k)\,|\,k\in\overline{1,K}\}$ – искомая процедура устранения инцидентов и минимизации их последствий, $z(P^*(I_k))$ – нормативные затраты на минимизацию последствий инцидента типа k, а $\tau(i\,|\,P^*(I_k))$ – нормативная длительность работы процедуры $P^*(I_k)$ одного инцидента. Обозначим через $S_i=\{s_i\}$ совокупность сервисов, потерявших доступность из-за инцидента i, а $d(s_i)$ – добавленная сто-

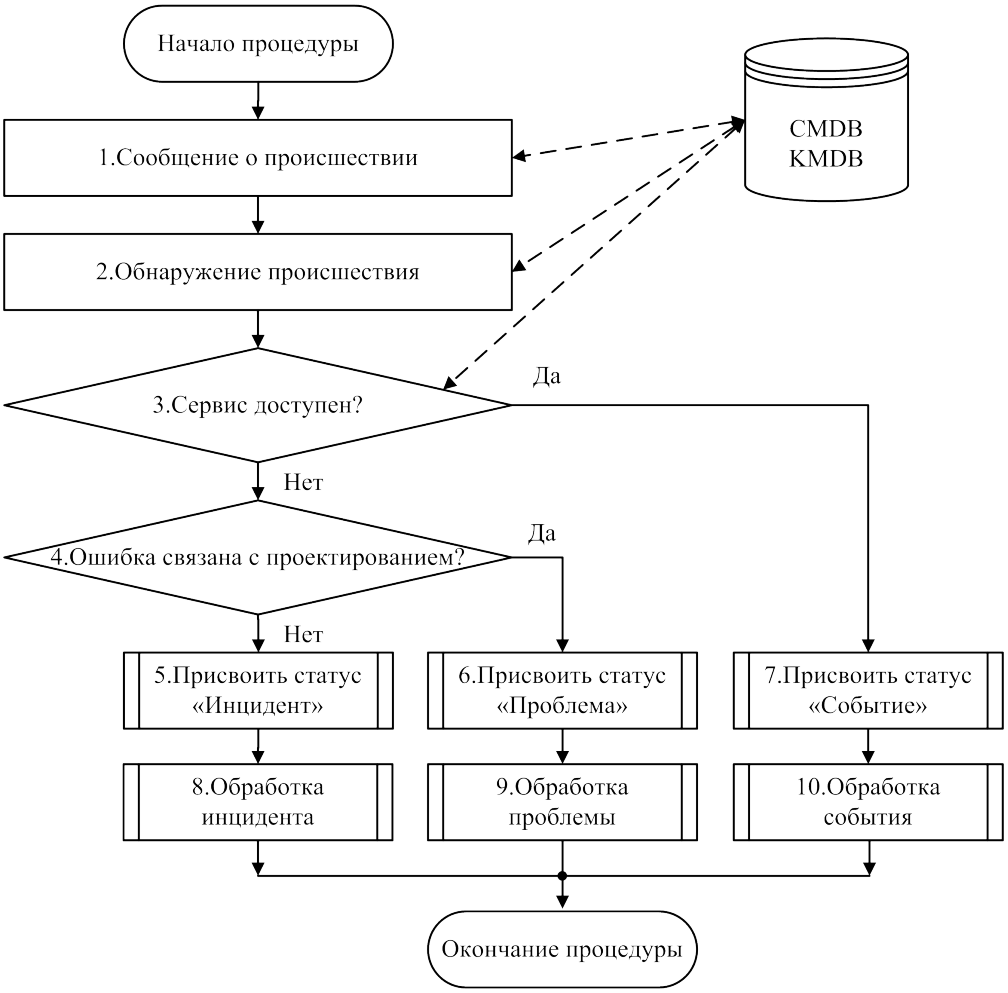

Рис. 1. Упрощенная процедура распознавания категории ИТ-происшествия

имость, создаваемая сервисом s_i в единицу времени. Тогда задачу синтеза процедуры $P^*(I) = \{P^*(I_k) \mid k = \overline{1,K}\}$ устранения (минимизации последствий) инцидентов на интервале времени $[0,T]$ можно представить следующим образом:

$$Q_{n_1} = \sum_{k=1}^{K} \sum_{i \in I_k} \sum_{s \in S_i} d(s_i)\tau(i \mid P^*(I_k)) \to \min_{P^*(I)},$$
$$\sum_{k=1}^{K} |I_k| z(P^*(I_k)) \le Z^*(I), \qquad (2)$$

где $|I_k|$ – мощность множества I_k, Z^* – плановые затраты на противодействие инцидентам в периоде $[0,T]$.

Содержательно запись (2) соответствует разработке процедуры функционирования $P^*(I) = \{P^*(I_k) \mid k = \overline{1,K}\}$, которая минимизирует потери потребителей из-за недоступности сервисов вследствие происшедших инцидентов и затраты на которую не превышают заданной величины $Z^*(I)$. При «незрелых» процессах ИТ-провайдера, величины $d(s_i)$ могут быть оценены по значению приоритета инцидента [3] и задачу (2) можно записать по-другому:

$$Q_{n_2} = \sum_{k=1}^{K} \sum_{i \in I_k} \tau(i \mid P^*(I_k)) \to \min_{P^*(I)},$$
$$\sum_{k=1}^{K} |I_k| z(P^*(I_k)) \le Z^*(I). \qquad (3)$$

Запись (3) соответствует минимизации общего времени недоступности сервисов из-за происшедших инцидентов.

На рис. 2 приведена общая процедура устранения инцидентов, которая ориентирована на поэтапное формирование оптимального (по критерию Q_{n_1} или Q_{n_2}) порядка действий службы эксплуатации ИТ-сервисов при обработке потока инцидентов.

Для подтверждения работоспособности вышеописанной процедуры приведем гра-

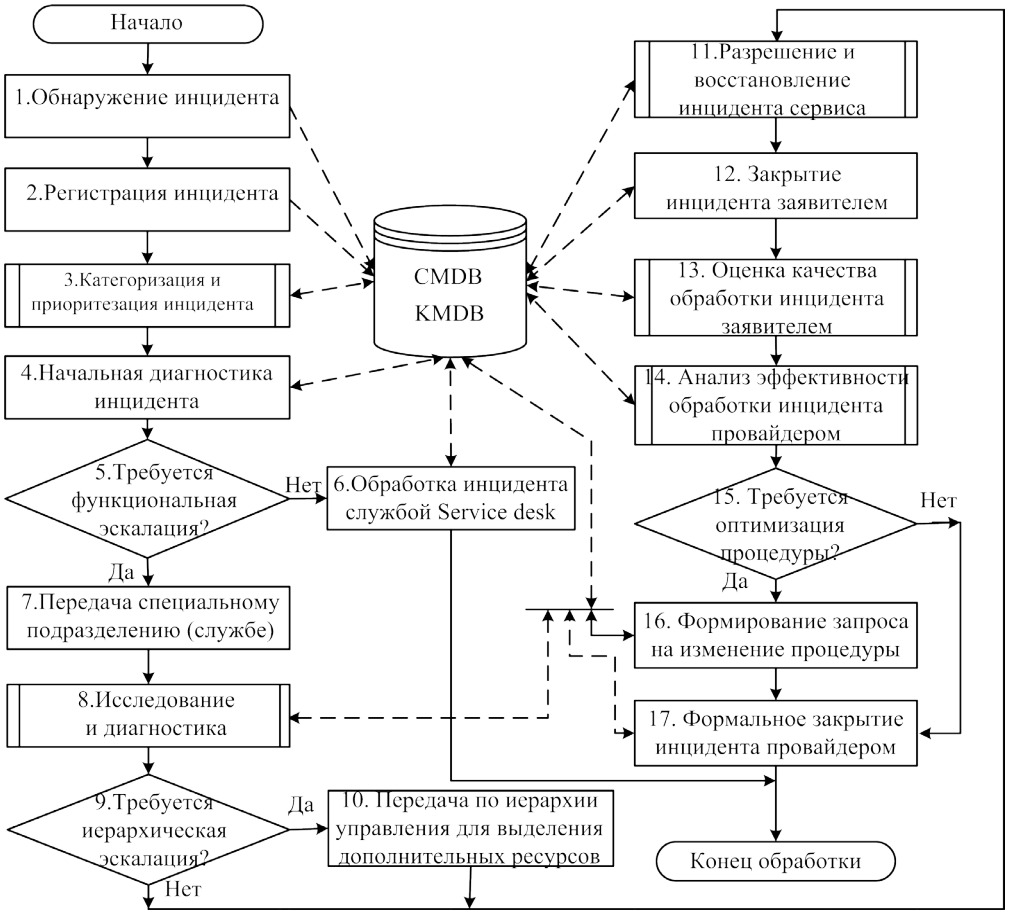

Рис. 2. Процедура устранения инцидентов

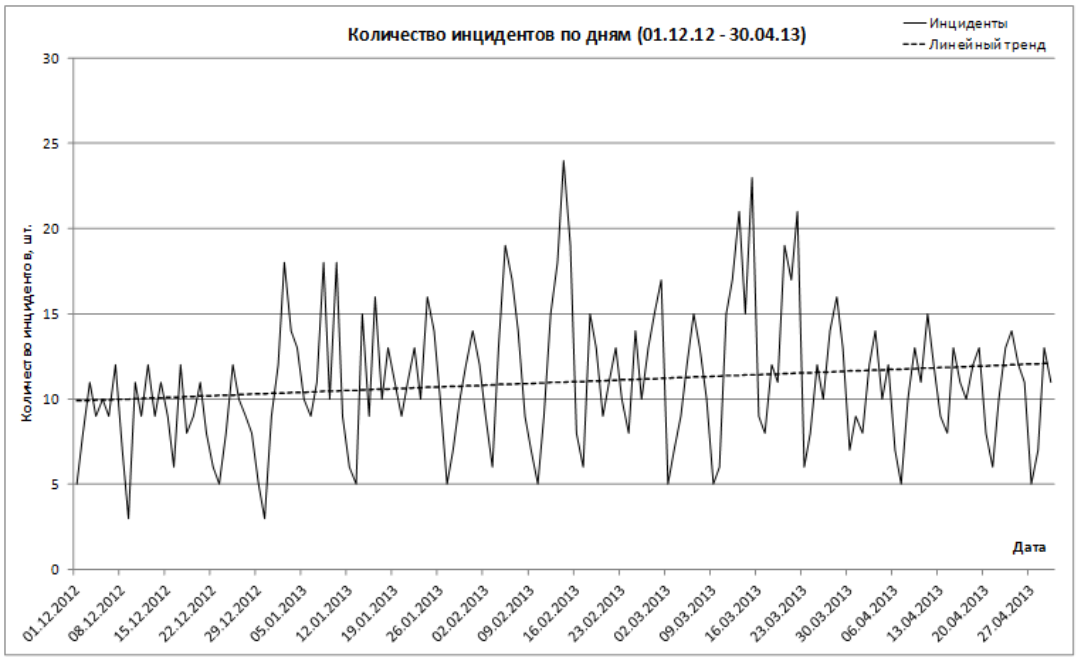

Рис. 3. Ежемесячное распределение инцидентов за период, предшествующий внедрению

фики (рис. 3, 4), построенные на основе базы данных службы эксплуатации поставщика ИТ-сервисов металлургической компании. Графики содержат информацию о пятимесячном распределении ИТ-происшествий вида «инцидент» за период, предшествующий вне-

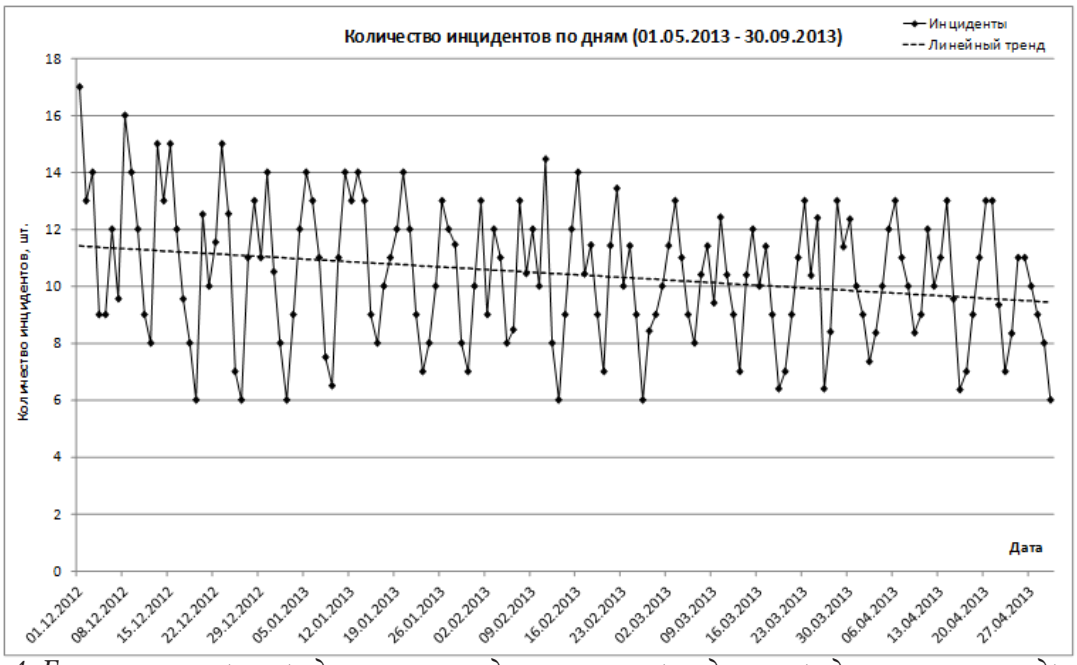

Рис. 4. Ежемесячное распределение инцидентов за период непосредственного внедрения процедуры устранения инцидентов

дрению (01.12.12–30.04.13), и период непосредственного внедрения процедуры устранения инцидентов (01.05.13–30.09.13).

Из приведенных графиков (рис. 3, 4) видно, что благодаря внедрению описанной процедуры количество инцидентов за пять месяцев снизилось на 5 %.

ЗАКЛЮЧЕНИЕ

Выполнены математические постановки задач распознавания категории конкретных ИТ-происшествий и устранения инцидентов, возникающих в процессе эксплуатации ИТ-сервисов. Предложена комплексная процедура их обработки, включающая алгоритм распознавания категории каждого ИТ-происшествия, а также человеко-машинные механизмы предотвращения их воспроизводства. Описанная процедура позволяет минимизировать потери потребителей из-за недоступности сервисов вследствие происшедших инцидентов.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО 9004-2010 «Менеджмент для достижения устойчивого успеха организации. Подход на основе системы менеджмента качества».

2. *Гончаров И. В.* Методический подход формирования модели затрат на процессы системы менеджмента качества организации / И. В. Гончаров, Ю. Г. Кирсанов, Н. И. Гончаров // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2014. – № 4. – С. 39–44.

3. OGC-ITIL V3- 6 – Service Lifecycle – Introduction ITIL TSO 2007. – 173 p.

4. Основы управления жизненным циклом сервисов систем информатики и автоматизации (лучшие практики ITIL): учеб. пособие / В. В. Зимин, А. А. Ивушкин, С. М. Кулаков, К. А. Ивушкин. – Кемерово : Кузбассвузиздат, 2013. – 500 с.

5. *Зимин В. В.* Формализация задач классификации, распознавания, предотвращения и минимизации последствий происшествий на стадии эксплуатации ИТ-сервисов / В. В. Зимин, С. М. Кулаков, М. В. Пургина, Р. С. Койнов // Известия вузов. Черная металлургия. – 2013. – № 12. – С. 34–38.

Кулаков Станислав Матвеевич – д.т.н., профессор, заведующий кафедрой автоматизации и информационных систем Сибирского государственного индустриального университета.
Тел. (3843)-76-56-70
E-mail: kulakov-ais @mail.ru

Kulakov Stanislav Matveevich – Prof. Siberian State Industrial University.
Tel.: (3843) 76-56-70
E-mail: kulakov-ais@mail.ru

Пургина Марина Владимировна – соискатель, старший преподаватель кафедры автоматизации и информационных систем Сибирского государственного индустриального университета.
Тел. (3843)-71-58-88
E-mail: pur-11@yandex.ru

Purgina Marina Vladimirovna – Degree-seeking student, senior teacher
Siberian State Industrial University.
Tel.: (3843) 71-58-88
E-mail: pur-11@yandex.ru

Зимин Валерий Викторович – к.т.н., доцент, профессор кафедры автоматизации и информационных систем Сибирского государственного индустриального университета.
Тел. (3843)-76-97-12
E-mail: zimin.1945@mail.ru

Zimin Valerij Viktorovich – Prof. Siberian State Industrial University.
Tel.: (3843) 76-97-12
E-mail: zimin.1945@mail.ru

Койнов Роман Сергеевич – соискатель, зав. сектором информационного обеспечения НТБ Сибирского государственного индустриального университета.
Тел. (3843)-74-26-34
E-mail: koynov_rs@mail.ru

Koynov Roman Sergeevich – Degree-seeking student, senior teacher Siberian State Industrial University.
Tel.: (3843) 78-43-76
E-mail: koynov_rs@mail.ru