УДК 005.4, 004.056, 658.5
DOI: 10.26102/2310-6018/2023.42.3.002

Разработка и анализ модели бизнес-процесса управления инцидентами с использованием средств IDEF-моделирования

Л.А. Сазанова✉

Уральский государственный экономический университет,
Екатеринбург, Российская Федерация

Резюме. В работе затронута проблема управления инцидентами в рамках функционирования ИТ-службы банка. Актуальность темы обусловлена многообразием видов инцидентов, последствий их влияния на результаты деятельности и качество бизнес-процессов в условиях постоянного совершенствования информационных технологий. Целью работы является исследование процесса управления инцидентами с использованием методологии моделирования IDEF0. Задачи исследования сводятся к построению и анализу соответствующей бизнес-модели на примере рассмотрения деятельности службы ИТ-поддержки банка, а также выработке предложений по совершенствованию информационной системы. При проведении исследования использованы теоретические и эмпирические общенаучные методы: систематизированный сбор данных, работа с электронными источниками, обобщение и анализ, метод IDEF-моделирования, с применением которого построены контекстные диаграммы, отражающие суть, особенности и изменения в анализируемом бизнес-процессе. В ходе анализа выявлены недостатки в реализации процесса управления инцидентами, связанные с регистрацией и дальнейшей передачей информации в системе службы поддержки. Обозначены пути их устранения с последующим сокращением времени на осуществление процесса и экономией человеческих и информационных ресурсов, после чего сформированы требования к модифицируемой информационной системе, предполагающие ведение базы данных примеров технической неисправности. Результатом исследования стало построение концептуальной модели информационного процесса регистрации инцидентов. Сделана декомпозиция процесса и внесены изменения, позволяющие оперативно обновлять информацию о потенциальных инцидентах и оповещать сотрудников службы поддержки о неисправностях. Последующая трансформация информационной системы банка с учетом предложенных изменений способствует оптимизации управления инцидентами, сокращая время реагирования на них и повышая качество работы банка.

Ключевые слова: управление инцидентами, информационная система, бизнес-процесс, автоматизация, IDEF-модель, служба поддержки.

Для цитирования: Сазанова Л.А. Разработка и анализ модели бизнес-процесса управления инцидентами с использованием средств IDEF-моделирования. *Моделирование, оптимизация и информационные технологии.* 2023;11(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1332 DOI: 10.26102/2310-6018/2023.42.3.002

Development and analysis of an incident management business process model using IDEF modeling tools

L.A. Sazanova✉

Ural State University of Economics,
Yekaterinburg, the Russian Federation

Abstract. The paper touches upon the problem of incident management as part of the bank IT service performance. The relevance of the issue is due to the variety of types of incidents, the consequences of their impact on the performance and quality of business processes in the context of continuous

improvement of information technology. The aim of the research is to study the process of managing incidents using IDEF modeling tools. The objectives of the study are reduced to the construction and analysis of an appropriate business model as in the case of considering the activities of the bank IT support service as well as the development of proposals for improving the information system. The study used theoretical and empirical general scientific methods: systematic data collection, review of electronic sources, generalization and analysis, the IDEF modeling method, which was employed to design context diagrams that reflect the essence, features and changes in the analyzed business process. The analysis has demonstrated the shortcomings in the implementation of incident management process related to the registration and further transmission of information in the support service system. The means to eliminate them are outlined with a view to minimizing the time for the implementation of the process and saving human and information resources, after which the requirements for a modified information system are defined that involve maintaining a database with examples of technical malfunctions. The result of the study was the construction of a conceptual model of the information process for registering incidents. The decomposition of the process has been made and changes have been introduced to quickly update information about potential incidents and notify the support staff about malfunctions. The subsequent transformation of the bank information system with due regard for the proposed changes contributes to the optimization of incident management, thus reducing the response time and improving bank performance.

Keywords: incident management, information system, business process, automation, IDEF model, support service.

For citation: Sazanova L.A. Development and analysis of an incident management business process model using IDEF modeling tools. *Modeling, Optimization and Information Technology*. 2023;11(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1332 DOI: 10.26102/2310-6018/2023.42.3.002 (In Russ.).

Введение

Управление инцидентами – важная составляющая функционирования ИТ-сервисов любой организации, от его успешного осуществления напрямую зависит обеспечение качества работы ее информационной системы (далее – ИС). Инцидентом является всякое событие, как-либо нарушающее нормальное течение процесса. Например, это может быть сбой в работе сервисов, остановка или медленная работа бизнес-приложения по причине переполнения канала связи, потеря данных. Инциденты снижают качество обслуживания и, как следствие, эффективность бизнес-процессов, что объясняет повышенное внимание к данной теме со стороны исследователей и практиков в ИТ-сфере. В контексте ITIL [1] управление инцидентами представляет собой процесс своевременного реагирования на любые незапланированные события, призванный гарантировать скорейшее восстановление услуги и минимизировать негативное влияние инцидентов. Даже если инцидент остается незамеченным клиентом или руководителем, он вызывает временны́е, репутационные и финансовые потери. По этой причине необходимо качественно организованное управление инцидентами, обеспечивающее бесперебойную работу всех структур организации и минимизирующее технологические и прочие риски. Как и любому комплексному процессу, управлению инцидентами присущи определенные трудности в его реализации. В настоящей работе сделан анализ организационной составляющей бизнес-процесса управления инцидентами в рамках рассмотрения деятельности ИТ-службы поддержки одного из уральских банков. Предложена модель усовершенствования подпроцесса регистрации инцидентов, предполагающая разработку данных примеров технических неисправностей и предполагающая модификацию информационной системы службы поддержки.

Материалы и методы

Методологическую основу исследования составляют современные общенаучные подходы к исследованию систем управления: системный подход, сравнение, описание и анализ причинно-следственных связей, позволяющие выявить особенности и узкие места в изучаемом процессе и направления повышения его эффективности. Теоретическая основа исследования опирается на изучение ряда отечественных и зарубежных источников, отражающих вопросы организации и информационной поддержки систем управления предприятиями [2-4], и популярных подходов к управлению инцидентами [5, 6]. Основным инструментом для создания и декомпозиции модели изучаемого процесса послужил метод IDEF-моделирования, чье применение к решению задач в ИТ-сфере рассмотрено, например, в работе [7].

Комплекс мероприятий, подразумевающий контроль над жизненным циклом инцидентов и минимизирующий их негативное влияние, подразумевает решение ряда задач, а именно:

– обеспечение стандартизации процедур оперативного реагирования на инциденты, а также их анализа, документирования и ведения отчетности;

– повышение оперативности и наглядности информирования персонала организации об инцидентах и их последствиях;

– обеспечение согласованности в действиях и приоритетах по управлению инцидентами в соответствии с целями бизнеса;

– повышение удовлетворенности внутренних и внешних клиентов организации качеством оказываемых ИТ-услуг.

В ходе решения указанных задач предполагается, что любые события, потенциально способные нарушить работу подразделений и сервисов организации, своевременно регистрируются в системе и становятся известными поставщикам ИТ-услуг. Реализация мер по разрешению возникших проблем часто наталкивается на ряд трудностей, порождаемых как особенностями деятельности организации, так и несовершенством ее регламентов осуществления контроля, узкими местами в работе технических компонентов ИС. Ниже рассмотрен вариант совершенствования процесса управления инцидентами в работе службы поддержки одного из региональных банков Свердловской области.

Результаты и обсуждение

Типичный процесс управления инцидентами подразумевает организацию мероприятий по восстановлению нормального обслуживания ИС с минимальными задержками и влиянием на бизнес-операции, предполагающую выявление инцидентов, их исследование и диагностику, разрешение и закрытие. На данный момент существует ряд подходов к решению комплексной задачи обеспечения качественного управления инцидентами, реализуемых в рамках стандартов, таких как ITIL, COBIT и ГОСТ Р ИСО/МЭК 18044 (например, [1, 8]). Информационная модель данного процесса, построенная с помощью методологии функционального моделирования IDEF0, представлена на Рисунке 1. На диаграмме отображены следующие составляющие: входная информация, включающая сообщение об инциденте и его особенностях; выходная информация, содержащая запись о закрытии инцидента (предполагается, что рано или поздно это произошло); специалисты, реализующие процесс – сотрудник центра управления сетью (данная структура обозначена аббревиатурой NOC), инженер технического отдела и инцидент-менеджер; а также управляющая документация (внутренний регламент работ с инцидентами). Для достижения результативности и эффективности процесса необходимы хорошая координация между пользователями и

специалистами, согласованность сроков разрешения инцидентов с целями бизнеса и корректность всех хранимых данных.

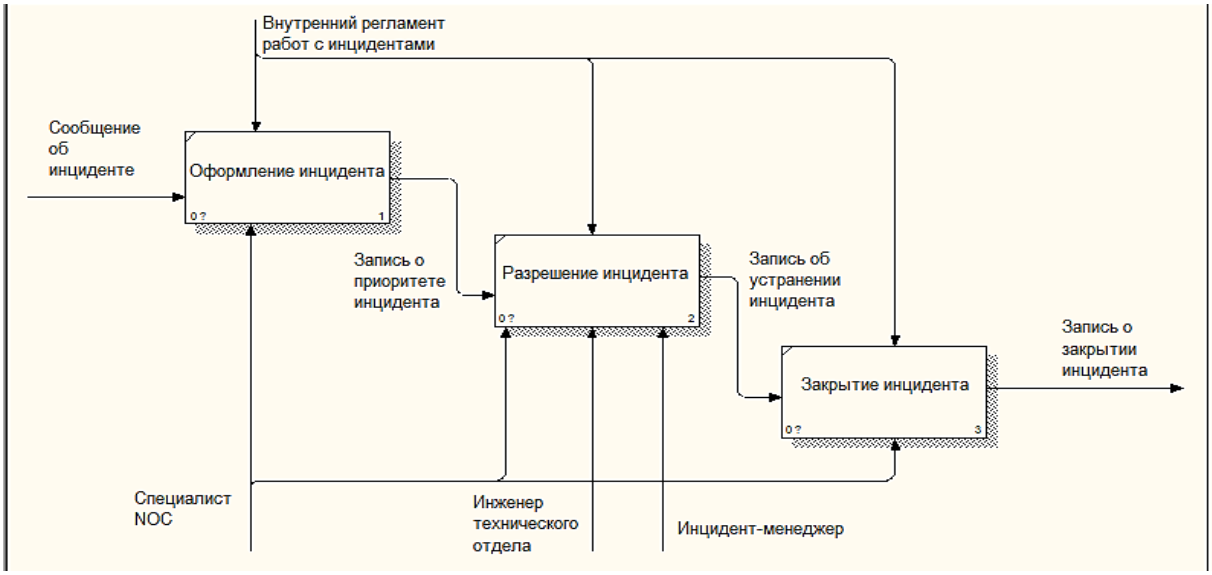

Рисунок 1 – Общая схема процесса управления инцидентами
Figure 1 – General outline of the incident management process

Отслеживание и ликвидация инцидента включают следующие действия:

1) Выявление инцидента и его регистрация в виде заявки (занесение информации об инциденте в журнал инцидентов), содержащей имя человека, сообщившего об инциденте, дату и время сообщения, описание инцидента, уникальный идентификационный номер, присвоенный инциденту для отслеживания.

2) Классификация и категоризация инцидентов, в ходе которых они перенаправляются в нужную группу. Это облегчает поиск причин возникновения инцидентов и определение оптимальных путей их устранения.

3) Назначение приоритета инциденту. Приоритет учитывает оценку ущерба, наносимого инцидентом компании, и скорость разрешения. Для приоритетов разных уровней предусмотрены определенные действия, поэтому клиенты и сотрудники имеют представление, насколько быстро проблема разрешится. На основании приоритета определяется очередность устранения инцидентов.

4) Первоначальная диагностика инцидента. В ходе ее сотрудник службы поддержки формулирует предположение о предполагаемой причине инцидента. Для облегчения решения данной задачи часто используются специализированные базы знаний инцидентов и соответствующие СППР [9], а также готовые руководства по диагностике. Возможно разрешение уже после первоначальной диагностики либо перенаправление инцидента на узконаправленных специалистов службы поддержки.

5) Анализ и углубленная диагностика. Допускается привлечение внешних ресурсов с целью консультирования и получения помощи в разрешении инцидента.

6) Разрешение инцидента и восстановление работоспособности системы. На данном этапе определяющим критерием является время, затрачиваемое на полное восстановление функций. Могут потребоваться переустановка и тестирование всей информационной системы после внесения исправлений.

7) Закрытие инцидента, когда он передается обратно службе поддержки.

Многие инциденты не являются абсолютно новыми, они связаны с тем, что уже происходило ранее и может повториться. По этой причине целесообразно заранее

определить стандартные модели инцидентов, накапливать и пополнять список их примеров и применять соответствующие методы разрешения. Обычно служба поддержки банка начинает действовать только по факту неисправности, многократно решая одну и ту же проблему и не учитывая предыдущий опыт. Внедрение автоматизированного процесса управления инцидентами дает следующие эффекты: уменьшается число проблем и ошибок и степень их влияния на деятельность банка, пополняется база знаний ИС за счет ведения статистики, анализа трендов, растет число инцидентов, успешно разрешаемых при первом обращении. Важную роль в решении поставленной задачи играет наличие в организации так называемого SLA (Service Level Agreement) – соглашения об уровне обслуживания [10, 11]. Данный документ раскрывает детали процесса предоставления услуги со стороны ИТ-службы заказчику (в данном случае – банку) и является эффективным «нейтрализатором» последствий инцидентов. В договоре SLA фиксируются: перечень отслеживаемых ИТ-службой сервисов организации, время реакции на инциденты, а также уровень качества доступности сервиса. При наличии грамотно составленного соглашения стороны однозначно понимают правила и порядок обслуживания, свои права и обязанности, оперируя при этом идентичными терминами. В соглашение включены сроки устранения последствий инцидентов, указаны размеры штрафов, которые выплачивает провайдер, когда метрики качества услуги опускаются ниже заданного уровня. Заказчик получает уверенность в своевременном устранении инцидентов и возможность более эффективно планировать свою бизнес-деятельность, а провайдер избавляется от риска предъявления необоснованных требований к качеству услуг. Для улучшения качества процесса соглашение необходимо максимально детализировать. Уровень детализации зависит от сложности процесса, масштабов деятельности организации и ряда других обстоятельств. На Рисунке 2 представлен процесс регистрации инцидентов, входящий в состав комплексного информационного процесса «оформление инцидента».

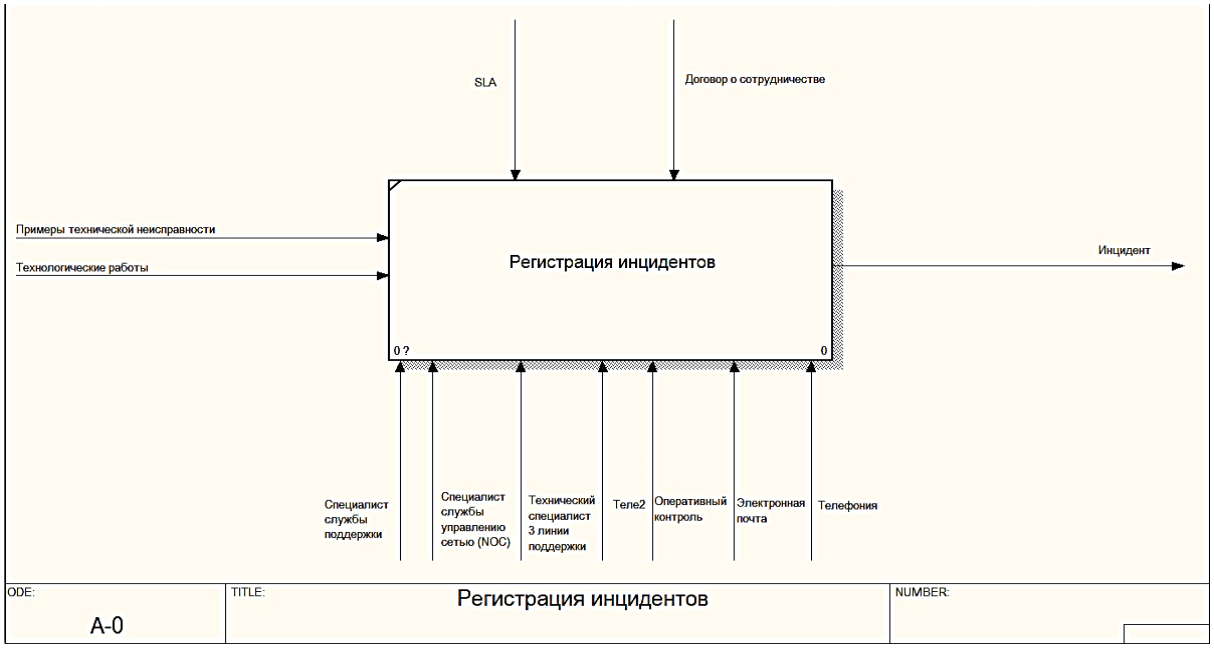

Рисунок 2 – Процесс регистрации инцидентов
Figure 2 – Incident logging process

Здесь и далее предполагается, что основным источником инцидентов являются действия оператора сотовой связи, обслуживающего данную организацию. С

некоторыми оговорками дальнейшие рассуждения и выводы можно распространить и на причины, порождающие другие типы инцидентов. На Рисунке 2 отображены следующие информационные потоки: входная информация, содержащая суть технической неисправности и технологических работ; выходная информация о результате действия инцидента; специалисты, работающие с инцидентом; управленческая составляющая, включающая соглашение об уровне обслуживания и договор о сотрудничестве. Детализация процесса регистрации инцидентов путем его функциональной декомпозиции представлена на Рисунке 3. Каждый из блоков, входящих в общий процесс, может быть, при необходимости, декомпозирован.

++

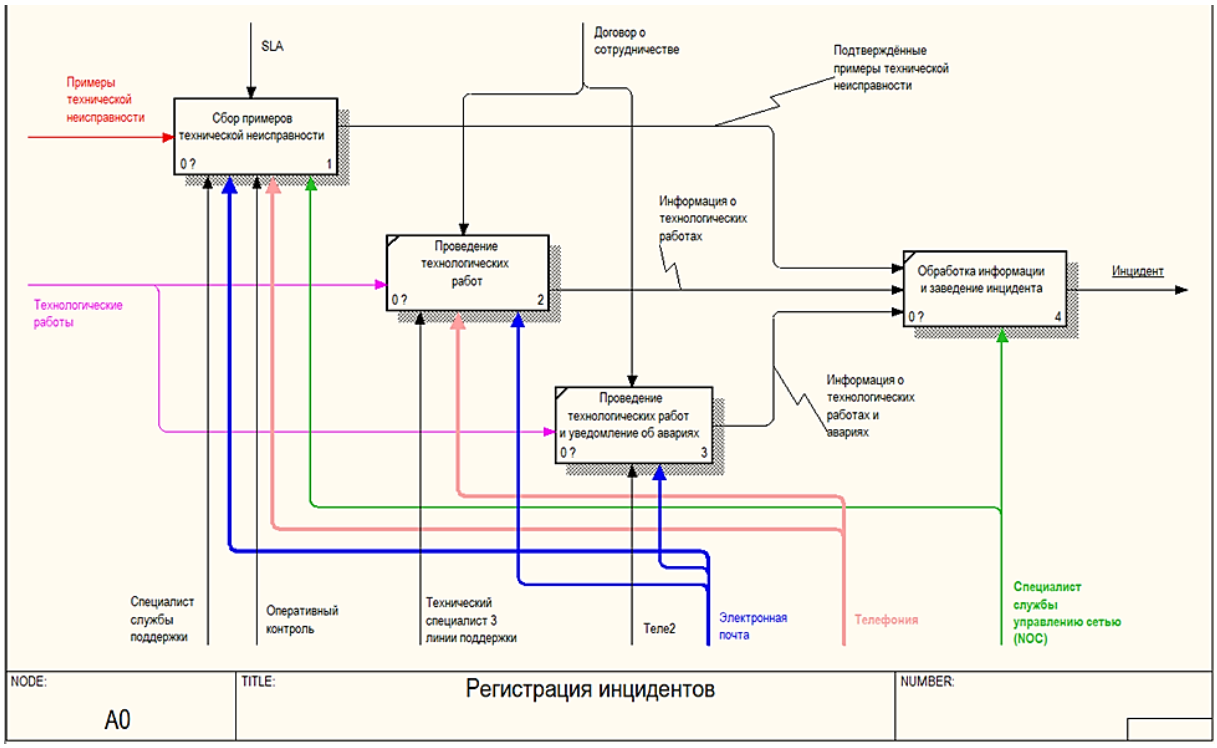

Рисунок 3 – Функциональная декомпозиция процесса регистрации инцидентов
Figure 3 – Functional decomposition of incident logging process

В настоящее время решение вопросов управления инцидентами осуществляется с использованием средств автоматизации, что порождает специфические проблемы, связанные с передачей информации между участниками процесса, с дублированием ряда функций и задержкой сведений в системе. Последнее наблюдается, когда представители службы оперативного контроля, осуществляющие мониторинг событий, испытывают затруднения при их регистрации, несвоевременно информируя вышестоящие органы управления, что влечет потери времени, значимые для бизнеса. По этой причине возникает потребность в рамках существующей ИС банка исключить вмешательство сотрудников подразделения оперативного контроля из процесса регистрации инцидента без ущерба для качества обслуживания. Данное исключение позволит:

– уменьшить время на передачу примеров о потенциальном инциденте специалистам службы управления сетью NOC, являющейся важным структурным звеном информационной системы;

– снизить расход денежных средств, идущих на содержание специалистов оперативного контроля;

– уменьшить шанс повторения ошибки в транслировании информации о текущих инцидентах.

После исключения участия сотрудников службы оперативного контроля, указанные сотрудники могут быть задействованы на других направлениях деятельности организации.

Следует отметить необходимость автоматизации процесса отправки примеров о потенциальном инциденте от специалистов службы поддержки. Данные примеры необходимы для быстрой категоризации инцидента и оперативного выбора возможных методов реагирования. Обычно отправка примеров происходит посредством использования почтового сервиса (например, Microsoft Outlook) и телефонии. При этом информирование о действующем инциденте осуществляется через электронную почту. Специалист службы поддержки вручную составляет письмо о проблеме, включающее номер абонента, суть проблемы (выбирая из шаблона), подробное ее описание, номер обращения клиента, дату и время воспроизведения неисправности у абонента, ФИО специалиста и т. д. Письмо направляется руководителю службы поддержки и на оперативный контроль. При сборе определенного числа (обычно – не менее трех) корректных примеров оперативный контроль обращается к специалистам службы управления сетью. Если с их стороны проблема подтверждена, специалисты службы оперативного контроля получают соответствующие рекомендации и направляют почтой их в службу поддержки. Описанный процесс влечет временные и человеческие затраты, что сказывается на качестве работы организации и взаимодействии ее с клиентами. Предлагается модификация ИС управления инцидентами, затрагивающая подпроцесс их регистрации, в которой реализованы приложения, выполняющие ряд операций:

1) оформление инцидента в базе данных службы управления сетью, а также отслеживание текущих и закрытых инцидентов;

2) прием инцидента «в работу», исполнение и отслеживание его с регистрацией заявителя;

3) возможность экспорта данных по инцидентам в MS Excel (или другую электронную таблицу, используемую сторонними специалистами для анализа).

Немаловажным является отслеживание статуса инцидента, указывающего на его состояние в процессе обработки (примеры статусов: «новый», «принят в работу», «активен», «отложен», «закрыт»). В процессе разрешения инцидента регистрационная запись о нем обновляется с изменением статуса, указанием выполненных действий и кода работавшего с инцидентом сотрудника. Также модифицированная подсистема передачи инцидентов должна поддерживать стандартные функции – идентификацию пользователей, хранение поступивших примеров инцидентов, формирование отчетов. ИС должна обладать понятным и удобным интерфейсом, обеспечивать быстрое отображение экранных форм, но решение этих технических вопросов реализуемо на стадии проектирования и не представляет трудности для специалистов в области ИТ. В обновленный процесс регистрации инцидентов к механизмам реализации добавится автоматизированная передача инцидентов, а служба оперативного контроля не будет задействована в обеспечении процесса. Выходная информация будет включать отчеты по зарегистрированным и направленным примерам инцидентов, поступающие в базу знаний, способствуя поддержанию ее актуальности. Декомпозиция обновленного процесса представлена на Рисунке 4. Примеры технической неисправности фиксируются сразу по мере их передачи, после чего направляются непосредственно специалистам службы управления сетью, чьи сотрудники получают прямой доступ к специализированному ПО для проверки, имеются ли ошибки или неисправности по направленному примеру. Иногда достаточно одного примера, что немаловажно в случае,

когда требуется редкий кейс с описанием нестандартной технической проблемы. Наконец, при выявлении сложных системных недоработок обновленная модель позволит специалисту службы поддержки передать проблему комплексно на разработчика (так называемая третья линия), чтобы решать вопрос не по отдельным обращениям, а сразу у всех абонентов с аналогичной проблемой.

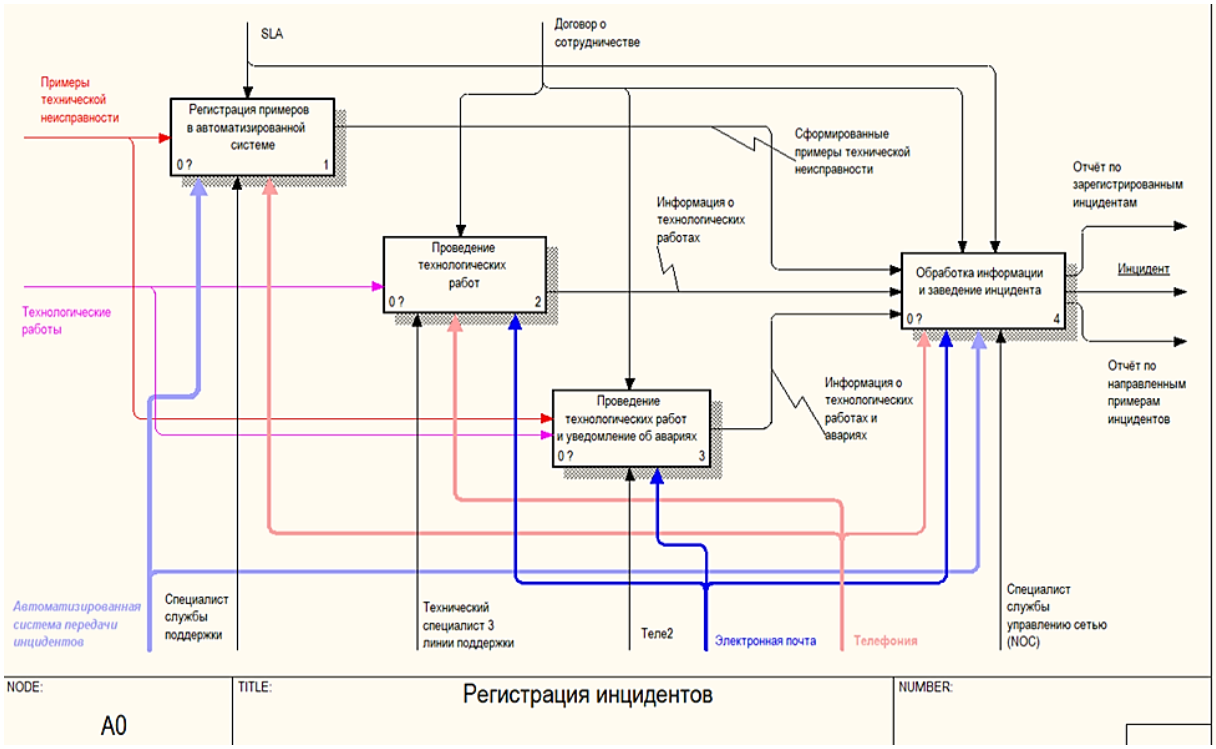

Рисунок 4 – Функциональная декомпозиция процесса регистрации инцидентов в системе после доработки

Figure 4 – Functional decomposition of incident logging process in the system after completion

Заключение

В настоящей работе предложена усовершенствованная модель бизнес-процесса управления инцидентами, затрагивающая подпроцессы их регистрации и категоризации. Построена соответствующая концептуальная модель, сделана ее декомпозиция и предложены изменения, позволяющие оперативно обновлять информацию о потенциальных инцидентах и оповещать сотрудников службы поддержки о неисправностях. Обоснована необходимость модифицирования информационной системы банка с включением в нее базы данных примеров инцидентов и методов реагирования на них, составлен список функциональных требований к новой ИС. Особенностью предлагаемого механизма управления инцидентами является то, что уже на начальном этапе их обнаружения и регистрации возможно оперативное реагирование благодаря использованию постоянно обновляющейся базы данных примеров.

Дальнейшее развитие модели видится в усовершенствовании подпроцессов, связанных с разрешением и закрытием инцидента. В условиях, когда полное разрешение инцидента представляется недостижимым, его негативное влияние может быть снижено применением обходного или временного решения, выработка которого требует внимательного анализа. Аналогичным образом, но с учетом специфики возникновения проблемы, можно осуществить анализ инцидентов, вызванных другими причинами – действиями провайдера или пользователя. Ведение истории реагирования на

проблемные ситуации с включением в базу знаний моделей инцидентов и соответствующих способов их обработки, указанием ответственности участников процесса, временных ограничений, сервисов, подвергшихся воздействию инцидента – все это потребует определенных усилий в плане автоматизации. В качестве вывода также можно отметить, что представленная модель является частью более комплексного процесса оптимизации управления инцидентами в контексте подхода ITISM. Ее использование способствует экономии временных и человеческих ресурсов организации, тем самым снижая финансовые и репутационные риски и повышая качество работы банка в целом.

СПИСОК ИСТОЧНИКОВ

1. Смирнов А.В. ITSM – подход к управлению и организации ИТ-услуг как фактор повышения конкурентоспособности предприятия. *Аллея науки*. 2018;1(11):16–20.
2. Буренин А.Н., Легков К.Е., Оркин В.В. Управление инцидентами при обеспечении безопасности информационных подсистем автоматизированных систем управления сложными организационно-техническими объектами. *Инфокоммуникационные технологии*. 2018;16(1):122–131.
3. Дмитриева Н.Г. Методологические модели управления информационным обеспечением. *Труды НГТУ им. Р.Е. Алексеева*. 2017;1(116):11–22.
4. Зефиров С.Л., Щербакова А.Ю. Оценка инцидентов информационной безопасности. *Доклады ТУСУР. Управление, вычислительная техника и информатика*. 2014;2(32):77–81.
5. Костомаров В.А. Анализ существующих процессных подходов к управлению инцидентами информационной безопасности. *Интеллектуальный потенциал XXI века: ступени познания*. 2014;23:131–135.
6. Ashraf M.U., Arif S., Basit A., Khan M.Sh. Provisioning quality of service for multimedia applications in cloud computing. *International Journal of Information Technology and Computer Science*. 2018;10(5):40–47.
7. Бубненкова А.О., Власюк Е.А., Сплендер Л.В., Трандофиров Д.А., Азаров В.Н. Моделирование основных бизнес-процессов управления IT-сервисами. *Качество. Инновации. Образование*. 2016;5(132):47–61.
8. Блинникова А.В., Нестерова Ю.О. Управление инцидентами в ITSM с использованием искусственного интеллекта. *Вестник университета*. 2020;6:36–40.
9. Сазанова Л.А. Применение современных СППР для решения управленческих задач. *Наука и бизнес: пути развития*. 2022;5(131):60–63.
10. Аншина М.Л. Архитектурные модели, управляемые сервисными соглашениями. *Современные информационные технологии и ИТ-образование*. 2021;17(2):334–344.
11. Зарубин С.В., Оболонская А.В., Мелузов Г.В. Специфика функционирования систем управления инцидентами безопасности. *Охрана, безопасность, связь*. 2022;7–2:17–23.

REFERENCES

1. Smirnov A.V. ITSM – an approach to the management and organization of IT services as a factor in increasing the competitiveness of an enterprise. *Alleya nauki = Alley of Science.* 2018; 1(11):16–20. (In Russ.).
2. Burenin A.N., Legkov K.Ye., Orkin V.V. Incident management in ensuring the security of information subsystems of automated control systems for complex organizational and

technical objects. *Infokommunikatsionnyye tekhnologii = Infocommunication technologies*. 2018;16(1):122–131. (In Russ.).
3. Dmitriyeva N.G. Methodological models of information management. *Trudy NGTU im. R.Ye. Alekseyeva = Proceedings of NNSTU im. R.E. Alekseev*. 2017; 1(116):11–22. (In Russ.).
4. Zefirov S.L., Shcherbakova A.Y. Information security incidents assessment. *Doklady TUSUR. Upravleniye, vychislitel'naya tekhnika i informatika = Proceedings of TUSUR University. Management, Computer Engineering and Informatics.* 2014;2(32):77–81. (In Russ.).
5. Kostomarov V.A. Analysis of existing process approaches to managing information security incidents. *Intellektual'nyy potentsial XXI veka: stupeni poznaniya = Intellectual potential of the XXI century: stages of knowledge*. 2014;23:131–135. (In Russ.).
6. Ashraf M.U., Arif S., Basit A., Khan M.Sh. Provisioning quality of service for multimedia applications in cloud computing. *International Journal of Information Technology and Computer Science*. 2018;10(5):40–47.
7. Bubnenkova A.O., Vlasyuk Ye.A., Splender L.V., Trandofirov D.A., Azarov V.N. Modeling of business IT service management processes. *Kachestvo. Innovatsii. Obrazovaniye = Quality. Innovation. Education*. 2016;5(132):47–61. (In Russ.).
8. Blinnikova A.V., Nesterova YU.O. Incident management in ITSM using artificial intelligence. *Vestnik universiteta = Bulletin of the University*. 2020;6:36–40. (In Russ.).
9. Sazanova L.A. Application of modern DSS for solving managerial problems. *Nauka i biznes: puti razvitiya = Science and business: development ways*. 2022; 5(131):60–63. (In Russ.).
10. Anshina M.L. Architectural Models Managed by Service Agreements. *Sovremennyye informatsionnyye tekhnologii i IT-obrazovaniye = Modern Information Technologies and IT Education*. 2021;17(2):334–344. (In Russ.).
11. Zarubin S.V., Obolonskaya A.V., Meluzov G.V. The specifics of the functioning of security incident management systems. *Okhrana, bezopasnost', svyaz' = Security, safety, communication*. 2022;7–2:17–23. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Сазанова Лариса Анатольевна, кандидат физико-математических наук, доцент Уральского государственного экономического университета, Екатеринбург, Российская Федерация.
e-mail: sazanovalarisa@rambler.ru

Larisa Anatolievna Sazanova, Candidate of Physical and Mathematical Sciences, Associate Professor at Ural State Economic University, Ekaterinburg, the Russian Federation.

Статья поступила в редакцию 14.03.2023; одобрена после рецензирования 26.06.2023; принята к публикации 06.07.2023.

The article was submitted 14.03.2023; approved after reviewing 26.06.2023; accepted for publication 06.07.2023.