

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий

(наименование института полностью)

Кафедра «Прикладная математика и информатика»

(наименование кафедры)

09.04.03 Прикладная информатика

(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления

(направленность (профиль))

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему «Инструменты и алгоритмы построения открытых информационных систем управления ИТ-инцидентами»

Студент

А.В. Луговой

(И.О. Фамилия)

(личная подпись)

Научный

руководитель

Е.А. Ерофеева

(И.О. Фамилия)

(личная подпись)

Руководитель программы д.т.н., доцент, С.В. Мкртычев

(ученая степень, звание, И.О. Фамилия)

(личная подпись)

« _____ » _____ 20 _____ г.

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А.В. Очеповский

(ученая степень, звание, И.О. Фамилия)

(личная подпись)

« _____ » _____ 20 _____ г.

Тольятти 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ ИТ- ИНЦИДЕНТАМИ	8
1.1 Обзор актуальных проблем управления в сфере информационных технологий	8
1.2 Анализ особенностей использования технологии открытых информационных систем в управлении ИТ-инцидентами.....	9
1.3 Принципы технологии открытых систем	11
1.4 Постановка задачи и определение области исследования.....	19
1.5 Алгоритм построения открытой информационной системы	20
ГЛАВА 2 АНАЛИЗ И МОДЕЛИРОВАНИЕ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ-ИНЦИДЕНТАМИ ...	27
2.1 Анализ процесса управления ИТ-инцидентами с использованием и без использования открытой информационной системы.....	27
2.2 Концептуальное моделирование открытой системы управления ИТ- инцидентами	31
2.3 Выбор модели данных и его обоснование.....	33
2.4 Моделирование базы данных.....	34
2.5 Выбор СУБД и его обоснование	43
ГЛАВА 3 РАЗРАБОТКА И РЕАЛИЗАЦИЯ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ-ИНЦИДЕНТАМИ ...	45
3.1 Диаграмма деятельности и ее спецификация.....	45
3.2 Построение базы данных открытой информационной системы управления ИТ-инцидентами.....	47
3.3 Выбор среды разработки и его обоснование	50
3.4 Разработка и реализация конструктора открытой информационной системы управления ИТ-инцидентами	53
3.5 Разработка и реализация открытой информационной системы	

управления ИТ-инцидентами.....	55
ГЛАВА 4 ВНЕДРЕНИЕ, АПРОБАЦИЯ И ОЦЕНКА ЦЕЛЕВОЙ ЭФФЕКТИВНОСТИ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ-ИНЦИДЕНТАМИ.....	69
4.1 Внедрение и апробация программного комплекса на базе ВУиТ	69
4.2 Оценка целевой и экономической эффективности применения программного инструментария	75
4.3 Проблемы и перспективы развития программного инструментария....	80
ЗАКЛЮЧЕНИЕ	84
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	87

ВВЕДЕНИЕ

В настоящем диссертационном исследовании рассматриваются инструменты и алгоритмы построения открытых информационных систем управления ИТ-инцидентами.

Выбор темы и **актуальность** проблемы диссертационного исследования обусловлены тем, что повсеместное и быстрое внедрение информационных технологий и систем, вычислительной и телекоммуникационной техники в сферы управления, а также обилие компаний-производителей компьютеров и разработчиков программного обеспечения нередко приводит к **проблеме** совместимости вычислительных, информационных и телекоммуникационных устройств [6].

Объект исследования – процесс управления ИТ-инцидентами.

Предмет исследования – использование открытых информационных систем в процессе управления ИТ-инцидентами.

Цель исследования – внедрение открытой информационной системы в процесс управления ИТ-инцидентами для обеспечения интероперабельности и мобильности программных приложений, персонала и данных.

Для достижения поставленной цели исследования необходимо выполнение следующих **задач**:

1. На основе проведенного исследования научной, нормативно-справочной и методической литературы определить алгоритм разработки открытых информационных систем для управления ИТ-инцидентами.

2. Провести анализ бизнес-процесса управления ИТ-инцидентами.

3. Исследовать вопрос существования программных инструментариев, пригодных для реализации открытых систем управления ИТ-инцидентами.

4. Выявить требования к открытым информационным системам управления ИТ-инцидентами.

5. Реализовать инструменты и алгоритмы построения открытых информационных систем управления ИТ-инцидентами.

6. Проанализировать целевую эффективность использования реализованных инструментов и алгоритмов.

Гипотеза исследования заключается в предположении о том, что внедрение открытой информационной системы в процесс управления ИТ-инцидентами позволит обеспечить интероперабельность и мобильность программных приложений, персонала и данных.

Теоретическую основу исследования составляют научные труды отечественных и зарубежных исследователей в области открытых информационных систем (Кияев В.И., Минакова Н.Н., Henze F. и др.), в области информационных систем управления предприятием (Митина О.А., Буянский С.Г., Bourgeois D. и др.).

Для решения поставленных в исследовании задач планируется использовать методологический аппарат, включающий в себя такие **методы** исследования, как:

- системный анализ;
- структурный и объектно-ориентированный анализ;
- структурное и объектно-ориентированное проектирование;
- статистический анализ;
- процессный подход;
- экономическая оценка эффективности проектов;
- и другие.

Проведение исследования было запланировано в период с 2017 по 2019 годы в три основных **этапа**:

- первый, *констатирующий*, этап исследования (2017 г.) включает в себя формулировку темы и гипотезы, проведение обзора научной и методической литературы, обусловление проблематики исследования;

- второй, *поисковый*, этап исследования (2018 г.) заключается в концептуальном и логическом моделировании открытой информационной системы управления ИТ-инцидентами, обосновании средств реализации системы, теоретической апробации результатов исследования;

- во время третьего, *экспериментального*, этапа исследования (2019 г.) выполнена практическая апробация разработанной информационной системы, проведена проверка поставленной в ходе первого этапа гипотезы на достоверность, подведены итоги проведенного исследования.

Апробация результатов исследования осуществлялась на базе ИТ-отдела – отдела информатизации и автоматизации учебного процесса учебно-методического управления Волжского университета имени В.Н. Татищева (г. Тольятти). Кроме того, результаты исследования были рассмотрены на следующих научных конференциях:

- XXXVI Международная научно-практическая конференция «Вопросы современных научных исследований», доклад на тему «Анализ процесса управления инцидентами в ИТ-компаниях с использованием и без использования открытой информационной системы» (проводилась 27.10.2018 в г. Омск);

- V Международная научно-практическая конференция (школа-семинар) молодых ученых «Прикладная математика и информатика: современные исследования в области естественных и технических наук», доклад на тему «Основные принципы применения среды открытых систем в управлении инцидентами» (проводилась в период с 22.04.2019 по 24.04.2019, г. Тольятти).

Научная новизна настоящего исследования заключается в попытке применения концепции, технологии и среды открытых информационных систем при построении открытой информационной системы управления ИТ-инцидентами.

Теоретическая значимость исследования заключается в изучении возможности и целесообразности применения концепции, технологии и среды открытых информационных систем в управлении ИТ-инцидентами.

Практическая значимость исследования заключается в направлении его результатов на улучшение качества управления ИТ-инцидентами путем внедрения в процесс управления открытой информационной системы.

На защиту выносятся следующие **положения**:

1. Концептуальная модель управления ИТ-инцидентами.
2. Программный конструктор-инструментарий, позволяющий осуществлять построение открытых информационных систем управления ИТ-инцидентами в соответствии с потребностями конечного пользователя.
3. Оценка целевой эффективности интеграции результатов работы программного инструментария в процесс управления ИТ-инцидентами.

Объем и структура диссертации: диссертационное исследование состоит из введения, четырех глав и заключения. Работа изложена на 90 страницах, содержит 28 рисунков, 24 таблицы.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ ИТ- ИНЦИДЕНТАМИ

1.1 Обзор актуальных проблем управления в сфере информационных технологий

В настоящее время наблюдается рост бизнес-услуг в сфере информационных технологий, открывается большое количество ниш и возможностей для ИТ-персонала. С ростом масштаба рынка ИТ-услуг увеличивается и потребность в оптимизации бизнес-процессов, связанных с информационными технологиями. Часто при необходимости получения экспресс-оценки состояния организации, при планировании ее развития необходима информация по состоянию процессов управления компанией. Такую информацию в современное время лучше всего получать, используя современные информационные системы управления. В условиях сложившегося рынка ИТ-услуг все большее значение приобретает применение технологии открытых информационных систем [20].

Для эффективной работы крупной организации большую роль играет автоматизация процессов управления в единой ИС, в которую может быть объединено управление персоналом, финансами, оптимизация бизнес-процессов компании, взаимодействие с клиентами и др. Основной проблемой использования такой ИС является высокая стоимость коммерческих решений, особенно это касается небольших организаций или компаний, только начинающих свою деятельность на рынке и, как следствие, еще не располагающих достаточным для приобретения подобных решений количеством денежных средств.

Во многих организациях, независимо от сферы их деятельности, не всегда имеется возможность отслеживания количества и характера инцидентов, имеющих отношение к сфере информационных технологий – отсутствует процедура управления ИТ-инцидентами.

Проблема создания информационной системы управления инцидентами существует уже длительное время. В каждой конкретной организации подход к данному вопросу осуществляется с разных точек зрения. Существует два основных подхода к решению задачи внедрения информационной системы в процесс управления инцидентами [9]:

- приобретение «монолитной» информационной системы управления ИТ-инцидентами, разработанной специализированной ИТ-компанией;
- создание «с нуля» своей информационной системы, подразумевающей использование интегрирующих модулей.

Очевидно, что каждый из этих подходов влечет за собой различные материальные и трудовые затраты. Далеко не каждая организация располагает достаточным количеством ресурсов для приобретения сторонней информационной системы управления инцидентами [22]. В то же время, не во всех организациях имеется персонал, обладающий достаточной для реализации второго подхода квалификацией.

1.2 Анализ особенностей использования технологии открытых информационных систем в управлении ИТ-инцидентами

В последнее время в ИТ-индустрии наблюдается тенденция перехода к открытым информационным системам, что позволяет значительно ускорить построение информационных систем [18, 19].

К свойствам открытых информационных систем относят:

1. Модифицируемость (или открытость).
2. Мобильность (переносимость) на разные платформы.
3. Свойство приспосабливаться к взаимодействию с другими программами (интероперабельность).
4. Дружественный интерфейс.

Под открытостью подразумевается обеспечение взаимодействия с другими системами и подсистемами. В основу создания открытых систем

положены стандартизация взаимодействия и унификация процессов. Термины «свободное программное обеспечение» и «открытое программное обеспечение» не являются синонимами. Значительная часть современного программного обеспечения является одновременно и открытым, и свободным [5].

Стандарты открытых информационных систем разрабатываются такими организациями, как IEEE, EIA, ISO другими. Большое значение при создании открытых информационных систем имеет создание интерфейса информационных систем для взаимодействия с другими подсистемами информационных систем. Открытой системой является система, состоящая из компонентов, взаимодействующих друг с другом через стандартные интерфейсы. В последнее время получила широкое распространение сертификация систем управления качеством (СМК), основным требованием стандартов которых является процессный подход к управлению (стандарты ISO 9000:2005 и др.).

Многие сервисы, такие как, система мгновенных сообщений, электронная почта, документооборот уже стандартизированы и используются многими программами [17]. В настоящее время наблюдается тенденция предоставления программного обеспечения через web-браузер.

Для обеспечения расширяемости и взаимодействия с другими информационными системами используются веб-сервисы и протоколы SOAP и WSDL, в качестве основного языка программирования серверной части программ (СПО) используется Java, для клиентской части применяются веб-технологии XHTML с использованием таблиц каскадных стилей CSS. Также при разработке приложений применяются платформенно-независимые технологии с использованием свободных библиотек Javascript, MooTools, JQuery, Prototype и прочих. Существует также множество решений с открытым исходным кодом, служащих для автоматизации управления практически всеми бизнес-процессами. Это позволяет гибко подходить к управлению бизнес-процессами, значительно увеличивать скорость внесения доработок и т.п. [4]

Компании, использующие открытые информационных технологии для разработки программ, могут существенно увеличить экономический эффект благодаря снижению расходов на внедрение и сопровождение информационных систем [30].

1.3 Принципы технологии открытых систем

Для построения открытой информационной системы управления ИТ-инцидентами необходимо знать общие принципы технологии открытых систем.

Число продуктов информационных технологий, как известно, составляет многие и многие тысячи, соответственно велико и число стандартов (международных, национальных, корпоративных и т.д.). Для облегчения взаимопонимания между группами специалистов целесообразно использовать единую модель среды открытых систем. Такой моделью служит так называемая эталонная модель среды открытых систем [31] (Open System Environment Reference Model – OSE/RM) (рисунок 1.1).

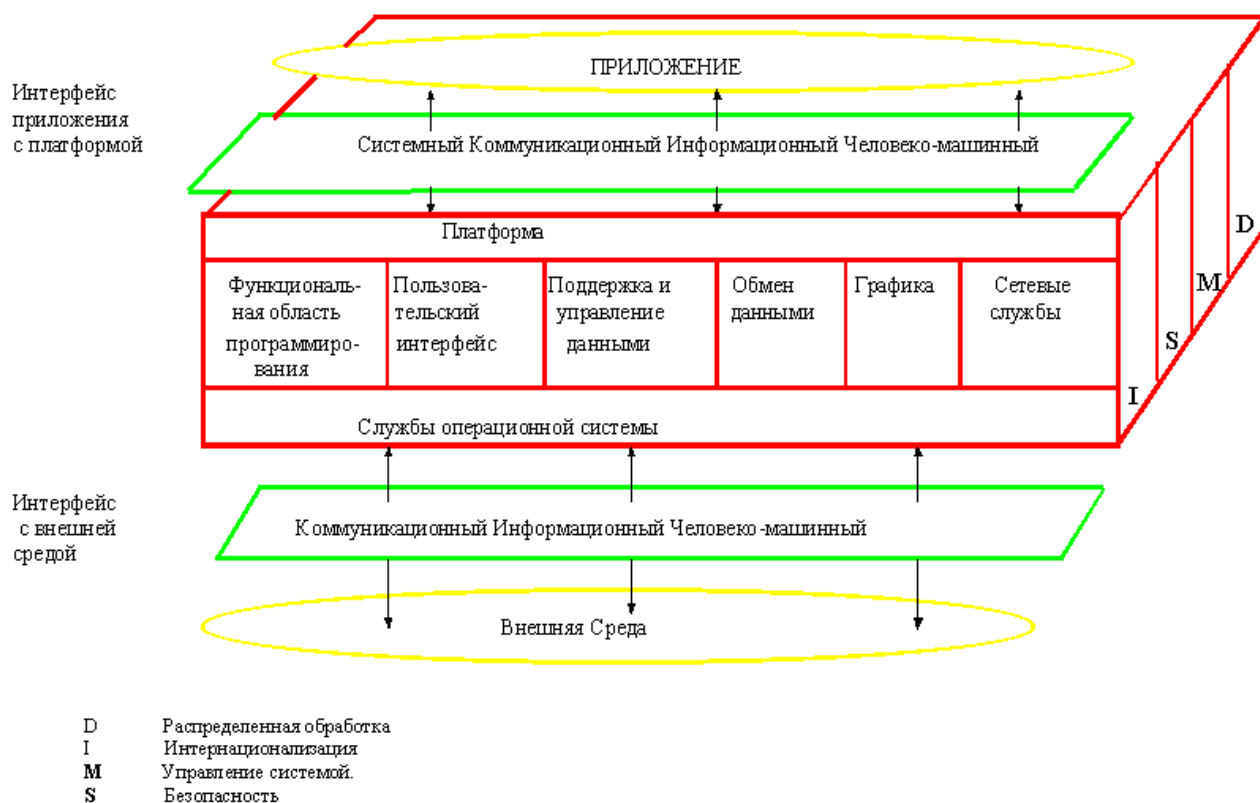


Рисунок 1.1 – Эталонная модель среды открытой системы OSE/RM

Эта модель может модернизироваться в зависимости от класса системы. Например, для телекоммуникационных систем хорошо известна 7-уровневая модель взаимосвязи открытых систем ISO/IEC 7498. Можно представить это и по-другому – модель OSE/RM выросла как расширение модели взаимосвязи открытых систем с детализацией верхнего прикладного уровня.

Как видно из рисунка 1.1, эталонная модель является трехмерной. По вертикали в ней можно выделить следующие компоненты:

- приложение;
- платформу;
- внешнюю среду;
- интерфейс приложения с платформой;
- интерфейс платформы с внешней средой.

По горизонтали имеются следующие компоненты (функциональные области):

- службы операционной системы;
- службы интерфейса "человек-машина";
- служба управления данными;
- служба обмена данными;
- служба машинной графики;
- служба сетевого обеспечения.

К третьему измерению относятся:

- службы поддержки разработки программного обеспечения;
- службы защиты информации;
- интернационализация;
- служба поддержки распределенной системы.

Следует обратить внимание, что сеть Интернет, построенная на основе протоколов TCP/IP, также является частью среды открытой системы как часть

сетевых служб, входящих в одну из функциональных областей среды, и далеко не решает всех проблем открытых систем.

Технология открытых систем (ТОС) представляет собой отечественную разработку, которую создали ученые из Центра открытых систем с целью реализации принципов открытых систем [11]. Процесс реализации принципов открытых систем в рамках ТОС состоит из следующих этапов [1, 2]:

- выбор модели среды открытой системы (СОС);
- построение профиля открытой системы;
- составление спецификаций и закупка аппаратных и программных средств;
- разработка приложений;
- аттестационное тестирование.

Основным приемом в ТОС служит функциональная стандартизация или построение функционального стандарта - профиля. Профиль – это согласованный набор базовых стандартов, предназначенный для решения какой-либо задачи или класса задач.

Построение профиля позволяет строить и развивать систему наиболее экономичным образом. Если все программно-аппаратные средства, в том числе суперкомпьютерные, поставляемые различными производителями, соответствуют профилю, т.е. выполнены в соответствии с необходимыми стандартами, они будут работать в единой среде, где будет обеспечена переносимость приложений, взаимодействие и функциональная расширяемость. В соответствии с этим существует определенная классификация профилей. Ее упрощенный вид представлен на рисунке 1.2.

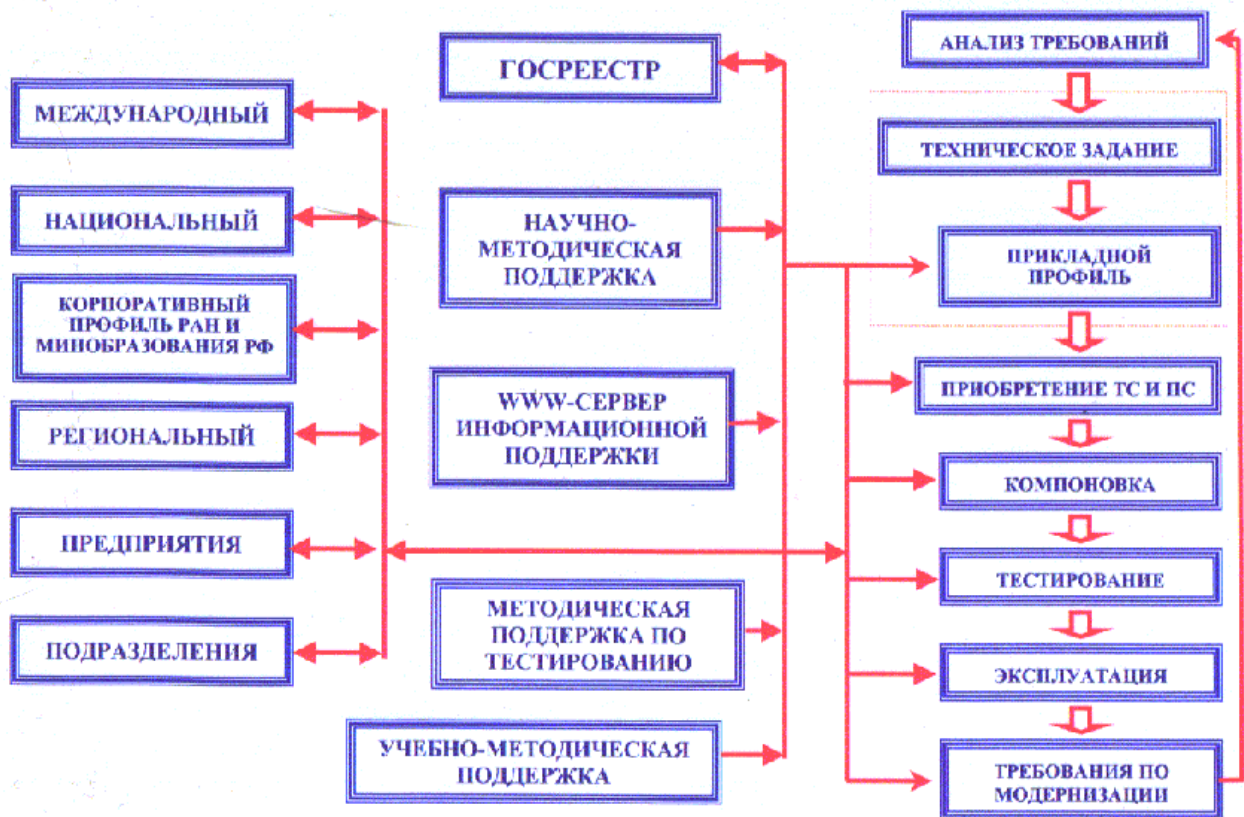


Рисунок 1.2 – Реализация принципов открытых систем

На верхнем уровне находятся международные стандартизованные профили (International Standardized Profiles – IPS), признанные комитетом ICO. ISP имеют в международном сообществе такой же статус, что и международные базовые стандарты и направлены на широкую область применения. Сюда относятся профили, описывающие конкретную программно-аппаратную среду, независимо от области применения. Именно к таким профилям относится профиль суперкомпьютерной среды (Supercomputer Application Environment Profile IEEE Std.1003.10 – 1995).

Ниже следуют национальные профили, в соответствии с которыми должна строиться Национальная информационная инфраструктура. Примерами национальных профилей могут служить Профиль Переносимости Приложений Правительства США (Application Portability Profile – APP), а также входящий в него Государственный профиль взаимосвязи открытых систем

(Government Open System Interconnection Profile – GOSIP). Подготовлен отечественный аналог Госпрофиля, который в настоящее время находится на стадии утверждения Госстандартом России.

Профили следующего уровня - отраслевые или корпоративные профили. Для каждой отрасли может и должен быть построен свой профиль, например, профиль банковской деятельности, профиль военного назначения, профиль научных исследований и т.д. Применительно к данной Концепции речь должна идти о корпоративном профиле РАН-Минобразования РФ.

Ниже следуют профили уровня предприятия и подразделения.

Все описанные профили не должны противоречить профилю более высокого уровня, а составлять их подмножество.

Общие правила построения профилей – Таксономия профилей описаны в трехчастевом стандарте ISO/IEC TR-10000-1-2-3, но реальное построение профиля – достаточно сложная научно-техническая задача. Разработкой профилей занимаются аккредитованные организации по стандартизации, производители, пользователи.

Внутри каждой из этих трех категорий организации объединяются между собой, в том числе, в различные ассоциации и консорциумы, организации всех этих категорий участвуют в сложном и дорогостоящем процессе выработки стандартов по принципам Workshop (рисунок 1.3). Workshop дословно переводится как мастерская, что очень верно передает смысл весьма точно регламентированного процесса, аналога в русском языке пока нет, и поэтому будем пользоваться этим термином. Следует подчеркнуть, что в условиях рыночной экономики стандарты играют несколько другую роль, чем они играют при централизованно распределительной экономике. Их живучесть и эффективность достигаются за счет согласительного, сбалансированного процесса их создания с участием пользователей, производителей и разработчиков.

К аккредитованным организациям в нашей стране относится Госстандарт.

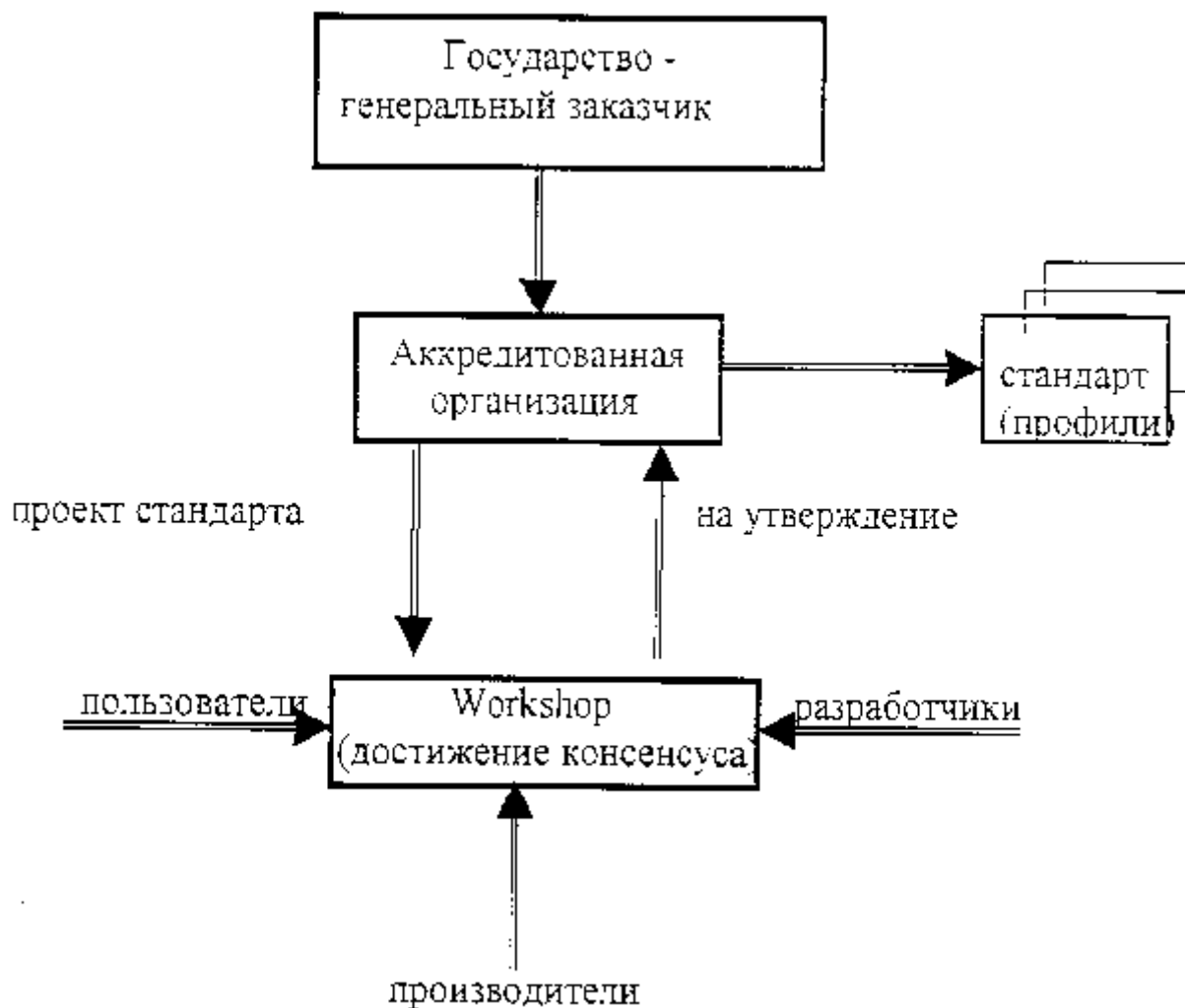


Рисунок 1.3 – Процесс принятия стандарта (профиля) методом достижения консенсуса

Подчеркнем еще раз роль профилей в реализации принципов открытых систем. Построение профиля на самых ранних стадиях создания информационной системы и следование ему на всех дальнейших стадиях жизненного цикла дает пользователю (заказчику) возможность составлять спецификацию на приобретаемые и разрабатываемые аппаратные и программные средства, как системные, так и прикладные, независимость от конкретного поставщика при создании и модернизации системы.

Разработчики приложений, в свою очередь, следуя профилю, обеспечивают возможность повторного применения разработанных приложений при смене платформ.

Поставщики средств вычислительной техники обеспечивают себе расширение рынка сбыта.

Наконец, разработчики стандартов могут оценить отсутствие необходимых стандартов и сосредоточить внимание на их разработке.

Как известно, говорить о соответствии стандартам невозможно без проведения соответствующего тестирования и сертификационных испытаний. Поэтому стадия тестирования является обязательным этапом ТОС. На основе профиля должно проводиться тестирование и сертификация приложений на соответствие требованиям открытости. Основу любого профиля, в том числе и суперкомпьютерного профиля, составляют стандарты серии POSIX. Общий перечень стандартов POSIX составляет более 45 наименований.

Следует подчеркнуть, что и базовые стандарты, и профиль имеют свой срок жизни, но срок жизни профиля должен быть больше срока жизни системы.

Так как основой технологии и принципов открытых систем является функциональная стандартизация, этап, на котором происходит построение профилей, является ключевым в ТОС. Данный этап включает в себя конкретный технологический цикл. Построение профилей предполагает применение методов хронологической декомпозиции, началом которой является выбор области применения профиля, а концом – выбор нужных стандартов. Последующие этапы таковы:

1. Анализ предметной области: выявляются направления деятельности, которые следует учесть в профиле.

2. Формулирование требований: определяются требования пользователя к функциональным возможностям и качеству служб на всех направлениях деятельности.

3. Логическое проектирование: на данном этапе выявляются информационные технологии и строятся модели служб информационных технологий, описывается технологическая структура и вычислительная среда открытой системы.

4. Физическое проектирование: модели служб и технологические компоненты заполняются стандартами.

5. Выбор продуктов информационных технологий.

6. Эксплуатация и тестирование полученного программного продукта.

Исходя из концепции использования принципов открытых систем в разрезе интеграционной основы построения информационной инфраструктуры, ТОС характеризуется двумя главными достоинствами [15]:

1. Высокая экономическая эффективность, которая обусловлена тем, что ТОС дает возможность построения и модернизации системы наиболее экономичным способом [27], так как не нужно дополнительно разрабатывать различного рода интерфейсы к аппаратным и программным средствам, а также появляется возможность реинжиниринга.

2. Эта технология – совершенно новая. Общеизвестно, что выпуск конкурентоспособной продукции требует использования инновационных технологий [26].

На основе вышесказанного были сделаны следующие выводы. Основные механизмы первых двух подходов в построении интегрированной корпоративной информационной среды являются неотъемлемыми технологическими компонентами на этапе выбора продуктов информационных технологий и разработки необходимых приложений, но уже согласно разработанному профилю. Таким образом, может быть выделен еще один, третий, подход к решению задачи внедрения информационной системы в процесс управления компанией, который включает в себя достоинства первых двух. Действительно, исходя уже из четко сформулированного набора стандартов, гораздо быстрее и эффективнее можно определиться и с выбором ERP-системы или ее модулей, покупкой новых программных продуктов, в том числе интернет-порталов, и с разработкой необходимых web-приложений [29].

К работам, развивающим общую методологию открытых систем в РФ можно отнести [25]. По применению концепции принципов открытых систем в

прикладных областях следует отнести работу [21].

1.4 Постановка задачи и определение области исследования

Эффективное управления ресурсами, методы и средства поддержки экономического и стратегического управления постепенно превращаются в необходимые атрибуты современного управления ИТ-инцидентами [10]. Информационная система, в этой связи, обязана обеспечить компании поддержку управления финансовыми, материальными кадровыми ресурсами на всех уровнях управления, обеспечивать руководство актуальной информацией, необходимой для принятия стратегических и оперативных решений. Таким образом, задача создания открытой информационной системы управления ИТ-инцидентами является очень важной, при этом важно корректно выбрать инструмент ее построения.

На текущий момент каждая ИС обязана в той или иной степени отвечать требованиям открытости. В этой связи актуально применение технологии открытых систем (ТОС), однако в то же время возникают следующие проблемы:

- не существует алгоритма применения принципов и технологии ОС для создания открытой информационной системы для управления ИТ-инцидентами;
- ТОС базируется на функциональной стандартизации, а, как общеизвестно, каждая стандартизация нацелена на экономию средств, при этом на данный момент нет никакой методики оценки экономической эффективности функциональной стандартизации, которая сама по себе могла бы послужить еще одним веским доводом в пользу необходимости применения принципов и идей ТОС;
- технология и принципы ОС предполагают модульное построение прикладного программного обеспечения [23], что позволяет начать автоматизацию с достаточно важного аспекта деятельности любой

организации, использующей информационные технологии для обеспечения своей деятельности.

Таким образом, для решения всех перечисленных проблем и достижения цели диссертационной работы необходимо решение следующих задач:

1. На основе проведенного исследования научной, нормативно-справочной и методической литературы определить алгоритм разработки открытых информационных систем для управления ИТ-инцидентами.

2. Провести анализ бизнес-процесса управления ИТ-инцидентами.

3. Исследовать вопрос существования программных инструментариев, пригодных для реализации открытых систем управления ИТ-инцидентами.

4. Выявить требования к открытым информационным системам управления ИТ-инцидентами.

5. Реализовать инструменты и алгоритмы построения открытых информационных систем управления ИТ-инцидентами.

6. Проанализировать целевую эффективность использования реализованных инструментов и алгоритмов.

Только при выполнении всех перечисленных задач диссертационное исследование может считаться успешно завершенным.

Перейдем к определению стандартного алгоритма построения открытой информационной системы.

1.5 Алгоритм построения открытой информационной системы

Информационная система управления ИТ-инцидентами представляет собой ИС масштаба предприятия, главной задачей которой является информационная поддержка производственных, административных и управленческих процессов (бизнес-процессов), направленных на скорейшее разрешение инцидентов, возникающих в ИТ-сфере [13].

Каждая система имеет жизненный цикл (ЖЦ). ЖЦ может быть описан с помощью абстрактной функциональной модели, которая отображает

концепцию потребности в системе, ее реализацию, применение, развитие и уничтожение. Система проходит через свой ЖЦ в соответствии с действиями, предпринятыми и управляемыми людьми в организациях, с использованием процессов для их исполнения.

Межгосударственный стандарт ГОСТ Р ИСО/МЭК 12207-2010 [3] выделяет несколько процессов, имеющих отношение к процессам ЖЦ, при помощи которых возможно построение модели ЖЦ системы. В течение своего ЖЦ система проходит несколько этапов. Каждый такой этап имеет свою цель, внося свой вклад в ЖЦ. Его разработка происходит в ходе планирования и выполнения ЖЦ системы. Этапы отображают главные периоды в ЖЦ, связанные с системой и относятся либо ко всей системе, либо к ее части. Этапы описывают основной прогресс и целедостижение системы, проходящей через ЖЦ, поддерживая принятие тех или иных решений.

Согласно ГОСТ Р ИСО/МЭК 12207-2010 возможно выделение следующих этапов ЖЦ ИС:

1. Выработка концепции системы.
2. Проектирование системы.
3. Реализация системы.
4. Тестирование.
5. Сопровождение и эксплуатация.

Процессы ЖЦ, происходящие на каждом из перечисленных этапов, представлены в таблице 1.1.

Таблица 1.1 – Этапы и процессы жизненного цикла

Этапы ЖЦ	Процессы ЖЦ
Выработка концепции системы	Определение требований заинтересованных лиц Анализ требований
Проектирование системы	Проектирования архитектуры
Реализация системы	Техническое обеспечение (практическая реализация) Интеграция
Тестирование	Проверка Настройка

	Тестирование
Эксплуатация и сопровождение	Ввод в эксплуатацию Сопровождение

Процессы определения требований заинтересованных лиц, анализа требований и проектирования архитектуры рекурсивно прикладываются к соответствующим уровням детализации до тех пор, пока элементы не станут пригодными к закупке, созданию, построению и повторному использованию [14].

Согласно требования стандарта ГОСТ Р ИСО/МЭК 12207-2010, разработка любого программного средства в виде элемента включает в себя следующие этапы:

1. Анализ требований.
2. Проектирование архитектуры.
3. Детальное проектирование.
4. Тестирование и кодирование.
5. Интеграцию.
6. Квалификационное тестирование.
7. Установку.

Опираясь на вышесказанное, можно описать алгоритм разработки любой обычной информационной системы, в том числе предназначенной для управления ИТ-инцидентами. Алгоритм разработки обычной ИС представлен на рисунке 1.4.

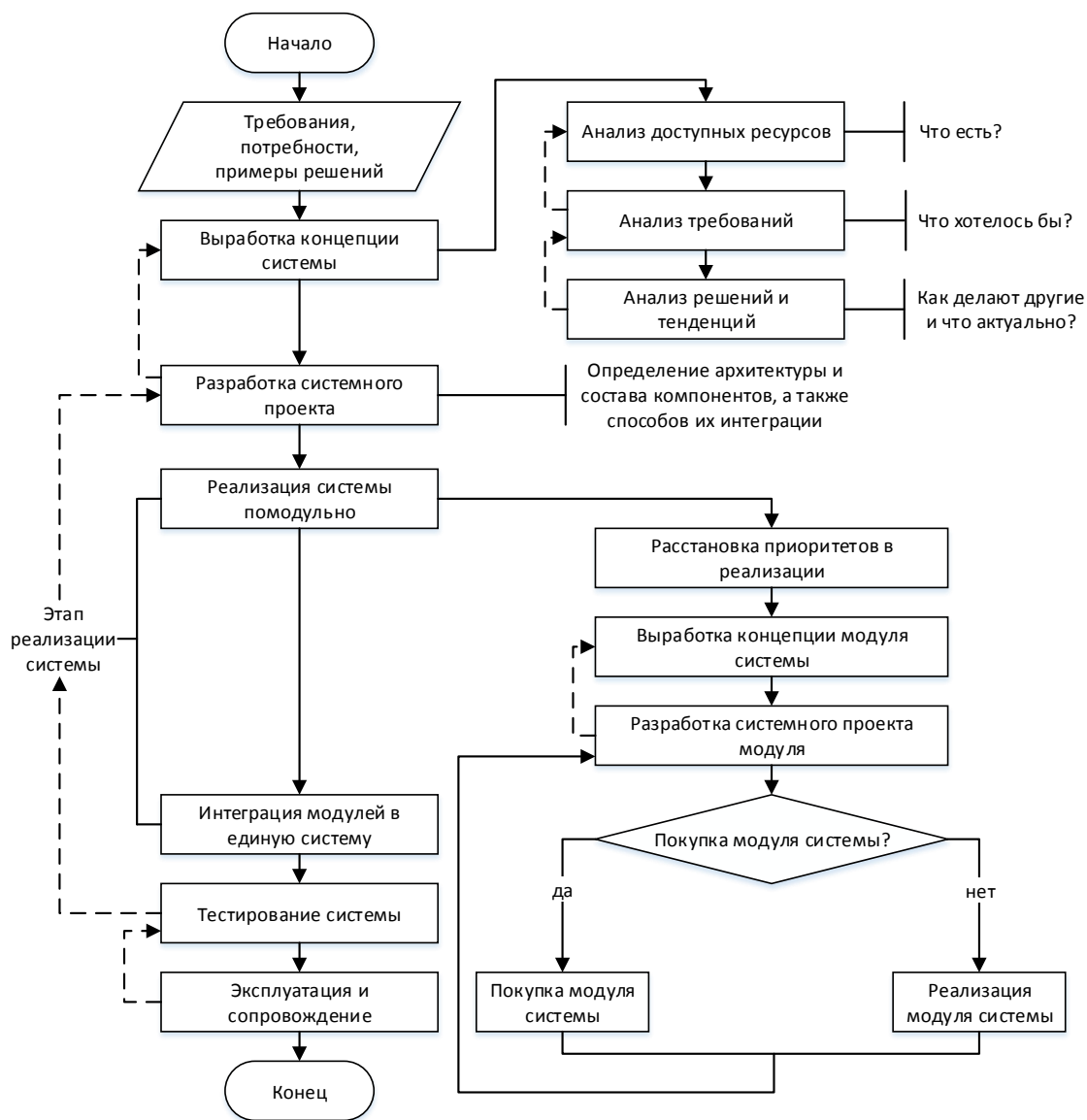


Рисунок 1.4 – Алгоритм разработки обычной информационной системы

Теперь изучим процесс построения ОС, для чего вернемся к ТОС, описанной в параграфе 1.3.

В соответствии с [12], ОС представляет собой систему, реализующую открытые стандарты и (или) спецификации на службы, форматы данных и интерфейсы, которых достаточно, чтобы приложение, построенное подобным образом, располагало:

- возможностью переноса с минимальным количеством изменений или без таковых на широкий диапазон операционных систем (кроссплатформенность);

- взаимодействием с пользователем в стиле, упрощающем ему переход от одной системы к другой (мобильность пользователя);

- взаимодействием с другими прикладными системами на локальных или удаленных платформах.

Таким образом, можно выделить дополнительный набор требований к открытой информационной системе управления ИТ-инцидентами, подлежащей построению.

Технология открытых систем требует на входе сделать выбор в пользу одного из вариантов решения требуемой системы, а, чтобы сделать выбор, соответствующий ситуации, необходимо произвести анализ непосредственно предметной области и информационной инфраструктуры (ИИ) этой предметной области [16].

После анализа предметной области и ее ИИ следует добавить в рассмотренный ранее ЖЦ ИС этап построения профиля и предшествующий ему этап выбора моделей. Исходя из ТОС, очевидно, что перечисленные этапы надлежит пройти еще в период проектирования системы, не доходя до ее реализации.

Если обобщить все вышеперечисленное в единое целое, то алгоритм построения открытой ИС станет выглядеть несколько иным образом (представлен на рисунке 1.5).

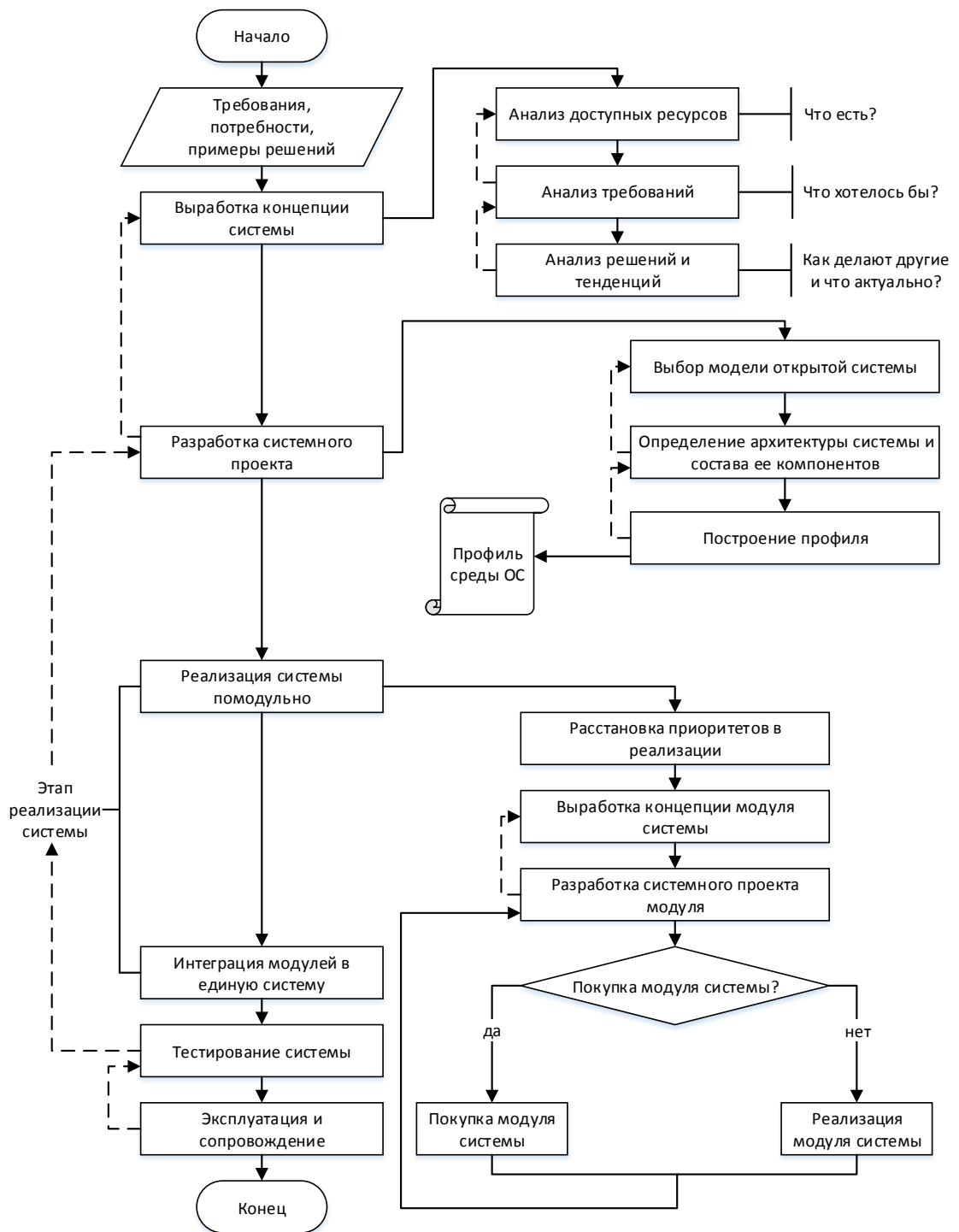


Рисунок 1.5 – Алгоритм создания ИС на основе принципов и технологии открытых систем

Опираясь на полученный алгоритм, можно описать процесс построения открытой ИС для управления ИТ-инцидентами. Для этого первым этапом доработаем концепцию системы, то есть в общих чертах опишем предметную область в форме моделей и рисунков; охарактеризуем информационную

инфраструктуру среднестатистической компании, таким образом, подготовим все необходимые сведения для реализации технологии открытых систем. На следующем этапе разработаем архитектуру ОИС, опираясь на эталонную модель СОС и профиль СОС. В результате станет возможной реализация инструментов и алгоритмов построения открытой информационной системы управления ИТ-инцидентами.

ГЛАВА 2 АНАЛИЗ И МОДЕЛИРОВАНИЕ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ- ИНЦИДЕНТАМИ

2.1 Анализ процесса управления ИТ-инцидентами с использованием и без использования открытой информационной системы

Современные компании используют в своей работе открытые информационные системы, решающие различные задачи: от оперативного управления компанией до помощи в принятии управленческих решений.

В современных условиях эффективное управление является ценным ресурсом любой организации, вместе с финансовыми, материальными, человеческими и другими ресурсами. Наиболее действенным способом повышения эффективности протекания трудового процесса является его автоматизация. Бурное развитие информационных компьютерных технологий, совершенствование технической платформы и появление принципиально новых классов программных продуктов привело к изменению подходов к автоматизации управления компанией.

В современных условиях хозяйствования одной из основных задач управления инцидентами является обеспечение его устойчивого развития. В связи с этим существует необходимость своевременной и всесторонней оценки результатов работы, за счет осуществления анализа параметров функционирования такого хозяйствующего субъекта.

Эффективным направлением совершенствования управления инцидентами является внедрение современных открытых информационных систем, что позволяет повысить скорость, качество и надежность процессов сбора, хранения и обработки информации; значительно сократить управленческий персонал, который занимается подготовкой информации для формирования и принятия управленческих решений по возникающим инцидентам; обеспечить в нужные сроки руководство и управленческий персонал компании качественной информацией; своевременно и качественно

вести анализ и прогнозирование хозяйственной деятельности компании; быстро и качественно принимать решения по всем уровням управления инцидентами.

Вопросами внедрения открытых информационных систем занимаются многие исследователи информационного менеджмента и ИТ-технологий.

Мировая практика свидетельствует, что открытые информационные системы – мощный инструмент повышения производительности труда и эффективности производства компании. На мировом рынке открытых информационных систем доминируют Северная Америка и Европа. Значимыми сегментами рынка остаются Азиатско-Тихоокеанский регион и Латинская Америка, где наблюдается быстрый рост.

Всемирным экономическим форумом для анализа стран мира по использованию информационных технологий используется балльная шкала оценивания: страна, в которой компании только начинают осваивать открытые информационные системы, имеют оценку 1 балл; страны, где принято широко осваивать открытые информационные системы – 7 баллов. Анализ стран мира по освоению открытых информационных систем и использования их в управлении компанией в 2016 году позволил сделать вывод, что лидером внедрения информационных систем является Исландия (6,2 балла), Япония, США и Норвегия – по 6,18 баллов (рисунок 2.1) [23].

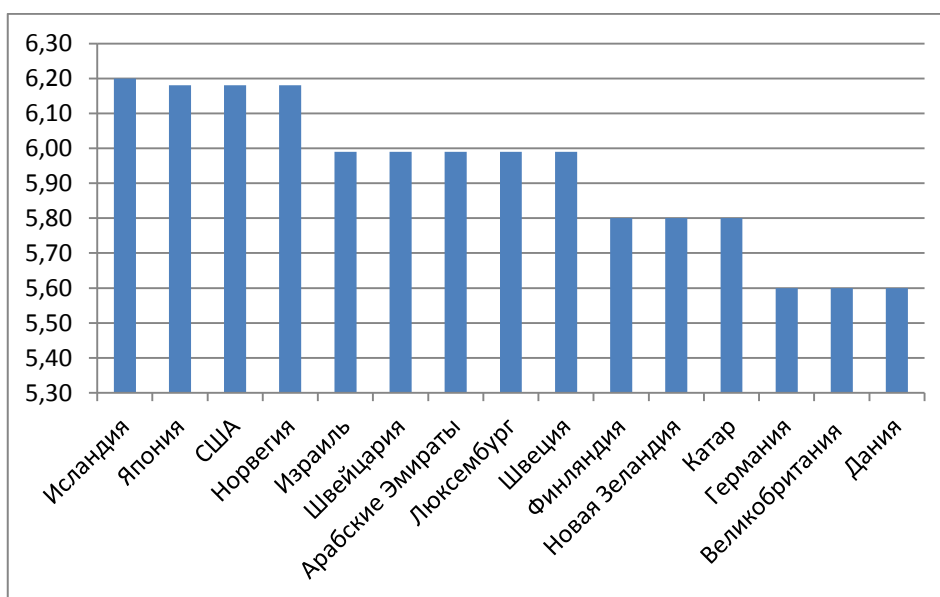


Рисунок 2.1 – Рейтинг использования открытых информационных систем

Открытые информационные системы, предназначенные для автоматизации различных видов хозяйственного учета, в том числе и управления ИТ-инцидентами можно условно разделить на три класса (таблица 2.1): локальные системы, средние интегрированные системы, крупные интегрированные системы.

Таблица 2.1 – Виды открытых информационных систем

№ п/п	Вид открытой информационной системы	Характеристика
1	Локальная	Успешно справляются с решением отдельных задач учета на предприятии, но, как правило, не предоставляют целостной информации для автоматизации управления. Преимуществом этих систем является сравнительно невысокая цена и относительная простота внедрения.
2	Средняя интегрированная	Примером средних интегрированных систем могут быть системы «AVACOSOFT», «ABACUS Financial», широко используемые в отечественной практике «Галактика», «Парус», «1С: Предприятие», «Регистры».
3	Большая интегрированная	Большие интегрированные системы - это функционально развитые, сложные дорогие системы. В них, как правило, реализуются западные стандарты управления уровня MRP II и ERP [9].

За последний десяток лет открытые информационные системы, в том числе и системы управления инцидентами, стали одним из самых популярных программных решений. Полнофункциональная система управления инцидентами становится единственным фундаментом для решения важных стратегических и управленческих задач, а не только инструментом автоматизации типичных для среднестатистической компании процессов.

Именно внедрение компанией системы управления инцидентами (в идеале – открытой) означает переход на более высокую стадию развития, потому что они позволяют наиболее эффективно реализовывать возможности компании. Количество компаний, которые используют такие системы, составляет несколько десятков тысяч по всему миру.

Современные открытые информационные системы должны удовлетворять определенным требованиям:

- использование клиент-серверной архитектуры с возможностью применения более промышленных СУБД;
- организация безопасности с помощью различных методов контроля и разграничения доступа к информационным ресурсам;
- поддержка распределенной обработки информации;
- модульный принцип построения с программно-независимыми функциональными блоками;
- возможность расширения за счет открытых стандартов.

Примеры наиболее известных зарубежных производителей открытых информационных систем (ОИС) приведены на рисунке 2.2.

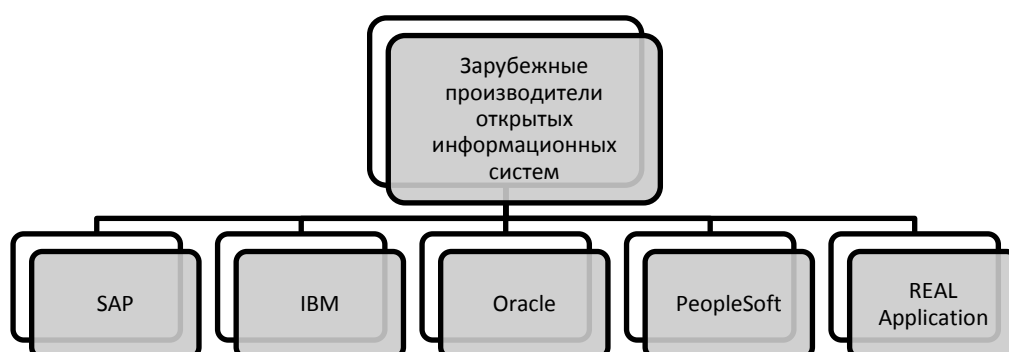


Рисунок 2.2 – Примеры известных зарубежных производителей ОИС

Примерами наиболее распространенных открытых информационных систем могут служить: Scala, Baan IV, «Галактика», SAP R/3.

Использование открытых информационных систем в управлении инцидентами будет способствовать решению следующих проблем:

- сложность управления при необходимости выбора управленческого решения из множества возможных решений;

- необходимость обработки больших объемов информации;
- необходимость принятия решения за короткий временной промежуток;
- проблема координации (решения необходимо координировать с другими звеньями процесса или объекта);
- необходимость сохранения и распространения знаний, накопленных в процессе многолетней работы и большого практического опыта.

Внедрение открытых информационных систем и технологий является обязательным условием деятельности любого современного предприятия, поскольку способствует принятию обоснованных управленческих решений, направленных на рост конкурентоспособности и усиление экономической безопасности.

Основываясь на проведенном в настоящем параграфе анализе, можно перейти к проектированию открытой информационной системы управления ИТ-инцидентами. Предварительно для этого необходимо также произвести моделирование такой системы.

2.2 Концептуальное моделирование открытой системы управления ИТ-инцидентами

Система управления в общем виде выглядит представленным на рисунке 2.3 образом [11].

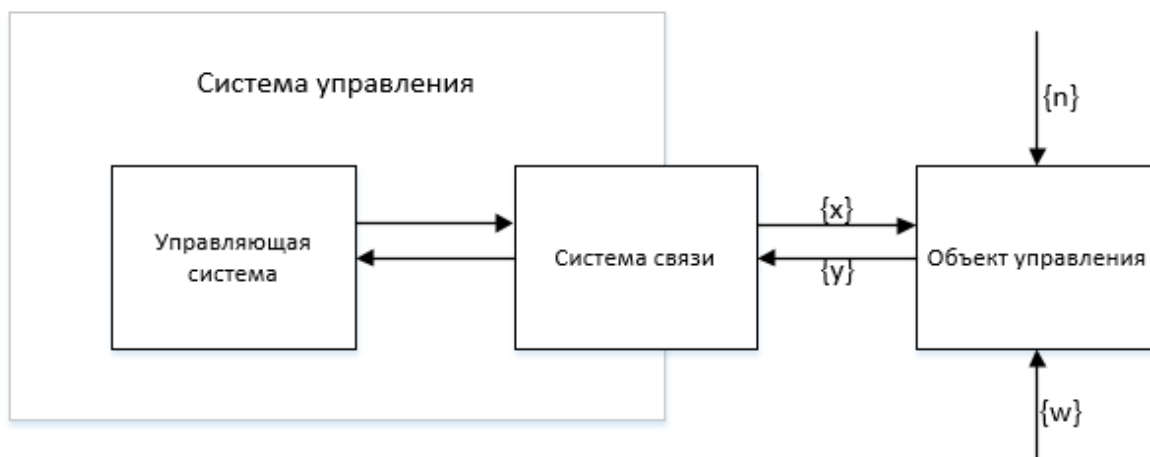


Рисунок 2.3 – Модель системы управления в общем виде

Под $\{x\}$ следует понимать множество входной информации, а под $\{y\}$ – множество выходной информации.

Множество воздействий окружающей среды (таких как помехи или коллизии) обозначается $\{n\}$.

Показатели, которые характеризуют эффективность управления, являются собой множество $\{w\}$.

Основываясь на модели системы управления в общем виде, построим концептуальную модель управления ИТ-инцидентами (рисунок 2.4).

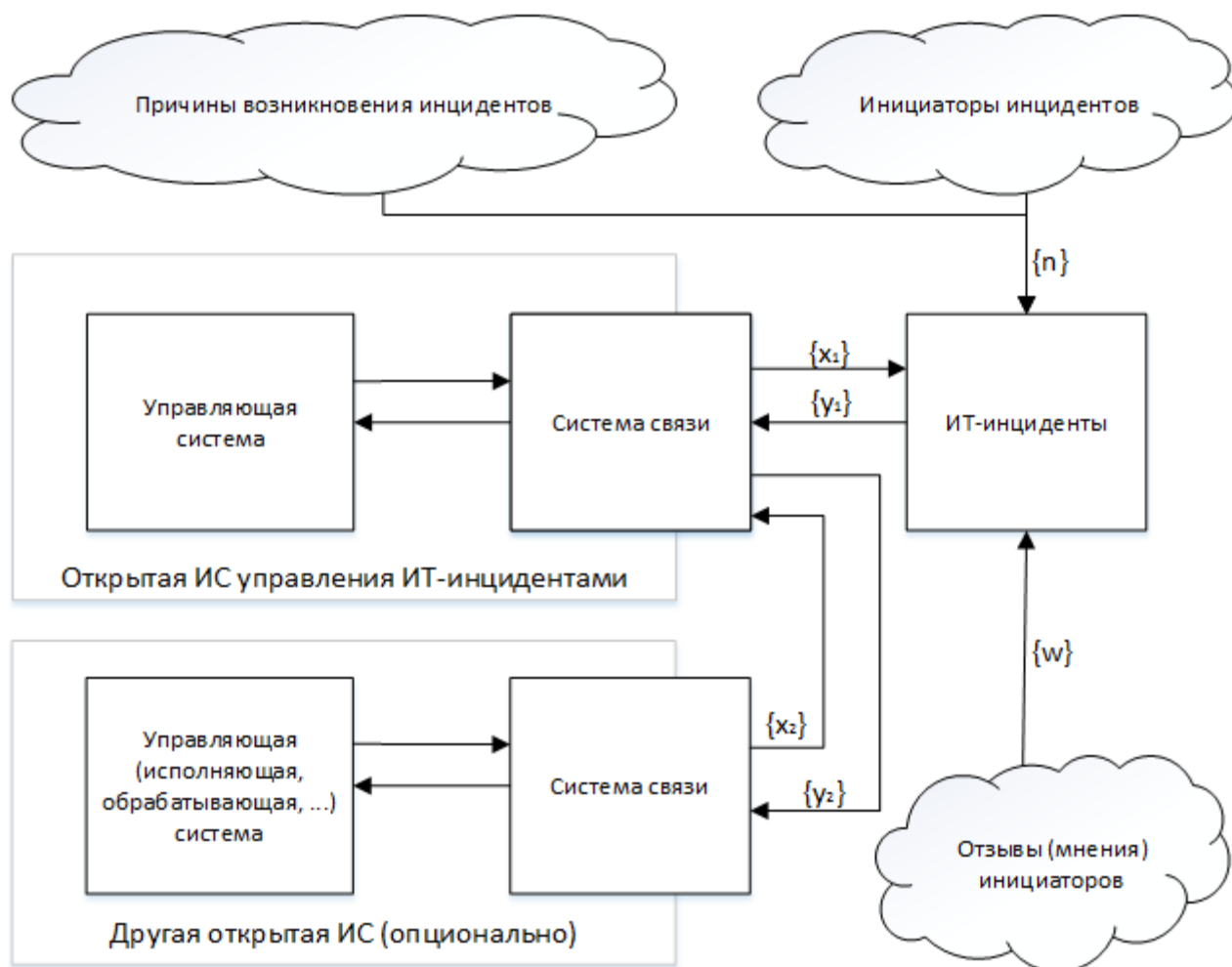


Рисунок 2.4 – Концептуальная модель управления ИТ-инцидентами

Поскольку проектируемая информационная система является открытой, то, согласно своему определению, она должна иметь возможность взаимодействия с другими ИС в случае возникновения такой необходимости,

что и было отражено в модели. Подобного рода взаимодействие с наименьшими трудовыми затратами может быть реализовано через специальные поля базы данных [12]. Таким образом, следует перейти к моделированию БД. Однако для этого необходимо вначале выбрать модель данных, которая будет использоваться.

2.3 Выбор модели данных и его обоснование

Существует три типа моделей данных: иерархическая, сетевая и реляционная. Кратко рассмотрим каждый тип, чтобы затем сделать выбор.

Иерархическая модель данных – представление базы данных в виде древовидной структуры, состоящей из объектов – данных различных уровней. Между объектами существуют связи, каждый объект может включать в себя несколько объектов более низкого уровня. Такие объекты находятся в отношении предка (объект более близкий к корню) к потомку (объект более низкого уровня), при этом возможна ситуация, когда объект-предок не имеет потомков или имеет их несколько, тогда как у объекта-потомка обязательно только один предок. Объекты, имеющие общего предка, называются близнецами (в программировании применительно к структуре данных дерево устоялось название «братья»).

В сетевой модели связи описываются с помощью графа, поэтому все элементы связаны друг с другом. Основным недостатком сетевой модели данных является: сложность и тяжелая наглядность схемы (данная схема наглядно не показывает это, так как содержит достаточно малое количество объектов), ослаблен контроль целостности связей вследствие допустимости установления произвольных связей между записями, любое изменение в схеме ведет к изменению всей базы. К основным достоинствам относятся: экономия памяти, быстрое действие, возможность обрабатывать произвольные связи.

Реляционная модель – это набор отношений нескольких двумерных таблиц, в каждой из которых хранится определенная информация. Основными

достоинствами этой модели является удобство использования, наглядность, возможность реализации связи «многие-ко-многим», порядок строк и столбцов не существенен. Учитывая вышеперечисленное, для предметной области настоящего диссертационного исследования эта модель наиболее приемлема.

Самым важным недостатком реляционной модели является то, что проектирование надежной реляционной базы требует определенных навыков и опыта, поэтому для несложных заданий лучше выбирать другую модель. Однако построение информационной системы управления (в особенности – открытой) в любом случае не является простой задачей.

Перейдем к моделированию реляционной базы данных.

2.4 Моделирование базы данных

Моделирование баз данных начинается, как правило, с построения UML-диаграммы классов [28]. Такого рода модель позволяет определить значимость одних данных в разрезе их взаимосвязи с другими данными. Конечный вид диаграммы классов будет зависеть от масштаба применения открытой информационной системы (ИТ-компания или же ИТ-отдел/служба).

В ходе построения диаграммы классов базы данных для ИТ-компании было выделено десять основных классов: «Сотрудник», «Отдел», «Должность», «Домен», «РабочееВремя», «Инцидент», «Заказчик», «Продукт», «СтатусСотрудника», «СтатусИнцидента», а также установлены соответствующие связи между ними и заданы ограничения. Получившаяся диаграмма классов базы данных представлена на рисунке 2.5.

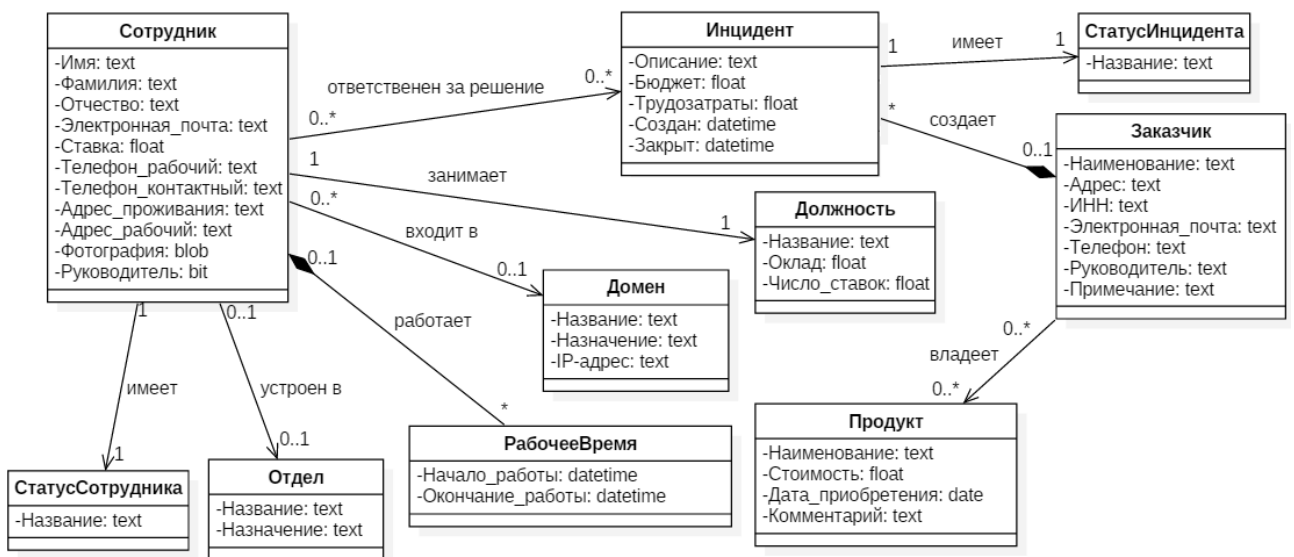


Рисунок 2.5 – Диаграмма классов базы данных (ИТ-компания)

Между классами «Заказчик» и «Продукт», а также «Сотрудник» и «Инцидент» установлена связь типа «многие-ко-многим», поскольку один и тот же клиент компании (заказчик) может приобрести сразу несколько продуктов компании, равно как и один и тот же продукт может быть приобретен множеством разных клиентов; аналогично один сотрудник может быть назначен для решения сразу нескольких инцидентов, и на решение каждого инцидента могут быть назначены сразу несколько сотрудников. Для реализации такого типа связи возникает необходимость в создании так называемых «промежуточных сущностей» (от англ. «transitional entity»). Дадим этим сущностям условные названия – «Заказчики-Продукты» и «Сотрудники-Инциденты» соответственно.

В ходе построения диаграммы классов базы данных для ИТ-отдела/службы было выделено восемь основных классов: «Сотрудник», «Отдел», «Должность», «Домен», «РабочееВремя», «Инцидент», «СтатусСотрудника», «СтатусИнцидента», а также установлены соответствующие связи между ними и заданы ограничения. Получившаяся диаграмма классов базы данных представлена на рисунке 2.6.

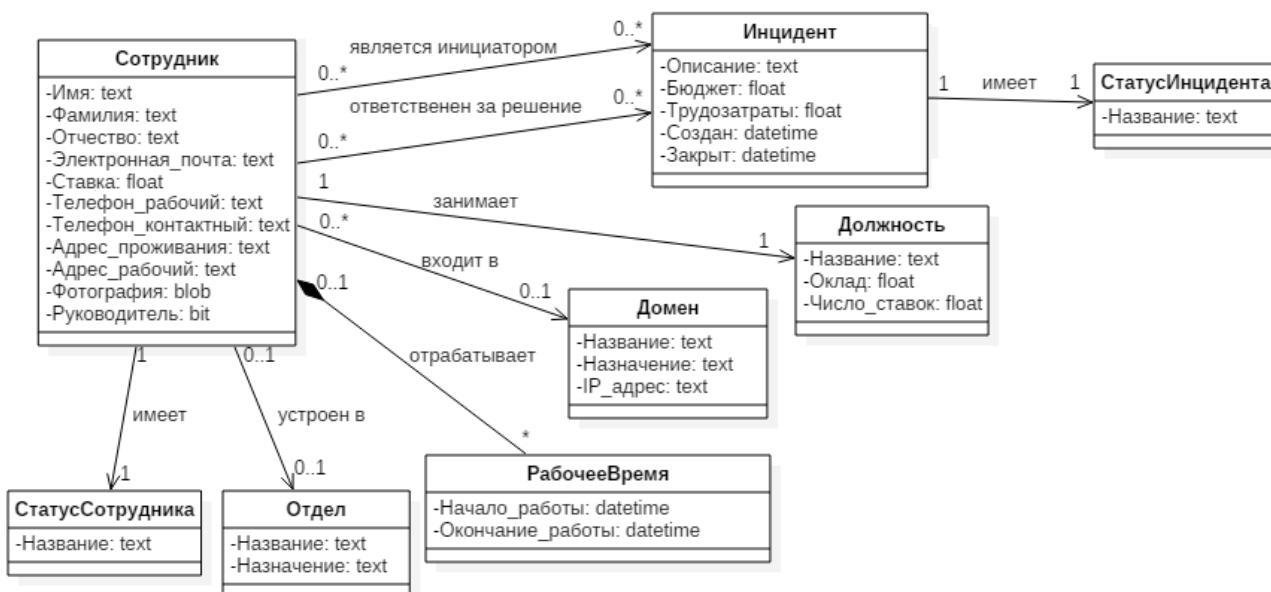


Рисунок 2.6 – Диаграмма классов базы данных (ИТ-отдел/служба)

Аналогично варианту для ИТ-компании, между классами «Сотрудник» и «Инцидент» установлена связь типа «многие-ко-многим», поскольку один и тот же сотрудник может быть назначен для решения сразу нескольких инцидентов, и на решение каждого инцидента могут быть назначены сразу несколько сотрудников. Промежуточная сущность «Сотрудники-Инциденты» необходима и в данном случае.

Следующим этапом моделирования базы данных является построение даталогической модели. Такая модель данных будет являться основой для создания будущей БД. Логическая модель данных строится без привязки к какой-либо СУБД, поэтому на данном этапе нет необходимости в ее выборе.

На рисунке 2.7 представлена даталогическая модель открытой информационной системы управления инцидентами, которая могла бы использоваться в деятельности некоторой абстрактной ИТ-компании при оказании технической поддержки клиентам. Данная модель построена с использованием бесплатной версии программы ERwin Data Modeler.

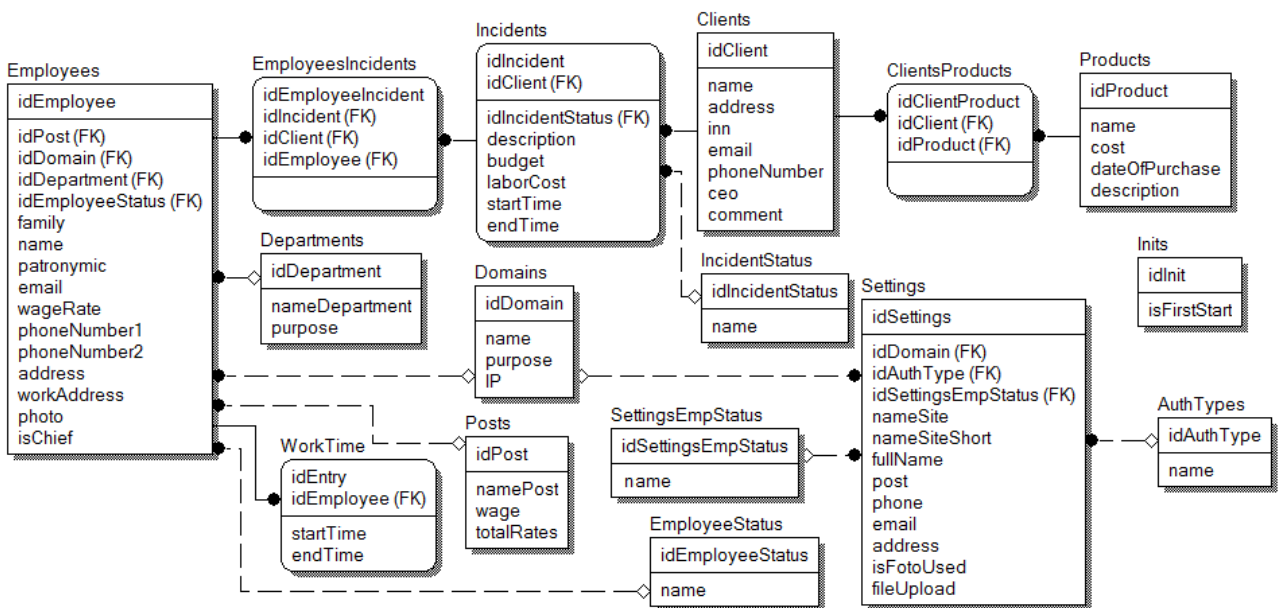


Рисунок 2.7 – Даталогическая модель базы данных (ИТ-компания)

Разработанная модель включает в себя следующие сущности:

- Employees («Сотрудники»);
- Incidents («Инциденты»);
- EmployeesIncidents («Сотрудники-Инциденты»);
- Clients («Заказчики»);
- Products («Продукты»);
- Departments («Отделы»);
- ClientsProducts («Заказчики-Продукты»);
- Worktime («Рабочее время»);
- Posts («Должности»);
- Domains («Домены»);
- Inits («Инициализации»);
- AuthTypes («Типы аутентификации»);
- EmployeeStatus («Статус сотрудника»);
- Settings («Параметры»);
- SettingsEmpStatus («Параметры статусов сотрудников»);
- IncidentStatus («Статус инцидента»).

Краткие спецификации полей сущностей приведены в таблицах 2.2 – 2.17. Буквой (O) обозначены те поля, значения которых могут быть получены из других открытых информационных систем.

Таблица 2.2 – Сущность «Employees» («Сотрудники»)

№ п/п	Название поля	Описание поля
1	idEmployee	Идентификационный номер сотрудника (первичный ключ)
2	idDepartment	Идентификационный номер отдела, в котором работает сотрудник (внешний ключ)
3	idPost	Идентификационный номер должности сотрудника (внешний ключ)
4	idDomain (O)	Идентификационный номер домена сотрудника (внешний ключ)
5	idEmployeeStatus (O)	Идентификационный номер статуса сотрудника (внешний ключ)
6	family (O)	Фамилия сотрудника
7	name (O)	Имя сотрудника
8	patronymic (O)	Отчество сотрудника (может отсутствовать – допустимо значение NULL)
9	email (O)	Электронная почта сотрудника (допустимо значение NULL)
10	wage_rate (O)	Тарифная ставка, на которую устроен сотрудник
11	phoneNumber1 (O)	Рабочий телефон сотрудника – внутренний либо городской (допустимо значение NULL)
12	phoneNumber2 (O)	Личный телефон сотрудника – мобильный либо городской (допустимо значение NULL)
13	address (O)	Адрес регистрации либо фактического проживания (при отсутствии регистрации) сотрудника (допустимо значение NULL)
14	workAddress (O)	Адрес рабочего места сотрудника
15	authType (O)	Вариант аутентификации сотрудника в системе – встроенная либо на основе LDAP
16	photo	Фотография сотрудника
17	isChief	Логическая переменная, показывающая, является ли сотрудник руководителем своего отдела

Таблица 2.3 – Сущность «Incidents» («Инциденты»)

№ п/п	Название поля	Описание поля
1	2	3
1	idIncident	Идентификационный номер инцидента (первичный ключ)
2	idClient (O)	Идентификационный номер заказчика, инициировавшего инцидент (первичный внешний ключ)
3	idEmployee	Идентификационный номер сотрудника, назначенного

		на решение инцидента (внешний ключ)
--	--	-------------------------------------

Продолжение таблицы 2.3

1	2	3
4	description (O)	Описание проблемы (заполняется инициатором инцидента)
5	budget	Бюджет, отведенный на исчерпание инцидента – за исключением оплаты труда (допустимо значение NULL)
6	laborCost	Временные затраты назначенного сотрудника
7	startTime	Время регистрации инцидента
8	endTime	Время закрытия инцидента

Таблица 2.4 – Сущность «EmployeesIncidents» («Сотрудники-Инциденты»)

№ п/п	Название поля	Описание поля
1	idEmployeeIncident	Идентификационный номер записи соответствия (первичный ключ)
2	idEmployee	Идентификационный номер сотрудника (внешний ключ)
3	idIncident	Идентификационный номер инцидента (внешний ключ)
4	idClient	Идентификационный номер заказчика (внешний ключ)

Таблица 2.5 – Сущность «Clients» («Заказчики»)

№ п/п	Название поля	Описание поля
1	idClient	Идентификационный номер заказчика (первичный ключ)
2	name	Полное наименование юридического лица заказчика
3	address	Юридический адрес заказчика
4	inn	Индивидуальный налоговый номер (ИНН) заказчика
5	email	Адрес электронной почты заказчика
6	phoneNumber	Контактный телефон заказчика
7	ceo	Руководитель юридического лица заказчика
8	comment	Комментарий по заказчику (допустимо значение NULL)

Таблица 2.6 – Сущность «Products» («Продукты»)

№ п/п	Название поля	Описание поля
1	idProduct	Идентификационный номер продукта (первичный ключ)
2	name	Наименование продукта
3	cost	Стоимость продукта
4	dateOfPurchase	Дата приобретения продукта
5	description	Комментарий к продукту (допустимо значение NULL)

Таблица 2.7 – Сущность «ClientsProducts» («Заказчики-Продукты»)

№ п/п	Название поля	Описание поля
1	idClientProduct	Идентификационный номер записи соответствия (первичный ключ)
2	idClient	Идентификационный номер заказчика (внешний ключ)
3	idProduct	Идентификационный номер продукта (внешний ключ)

Таблица 2.8 – Сущность «Departments» («Отделы»)

№ п/п	Название поля	Описание поля
1	idDepartment	Идентификационный номер отдела (первичный ключ)
2	nameDepartment	Название отдела
3	purpose	Назначение отдела

Таблица 2.9 – Сущность «Worktime» («Рабочее время»)

№ п/п	Название поля	Описание поля
1	idEntry	Идентификационный номер записи (первичный ключ)
2	idEmployee (O)	Идентификационный номер сотрудника (первичный внешний ключ)
5	startTime (O)	Время начала работы (фиксируется ежедневно)
6	endTime (O)	Время окончания работы (фиксируется ежедневно)

Таблица 2.10 – Сущность «Posts» («Должности»)

№ п/п	Название поля	Описание поля
1	idPost	Идентификационный номер должности (первичный ключ)
2	namePost	Название должности в штатном расписании
3	wage	Оклад за 1,0 ставки
4	totalRates	Общее количество ставок, отведенных штатным расписанием на данную должность

Таблица 2.11 – Сущность «Domains» («Домены»)

№ п/п	Название поля	Описание поля
1	idDomain	Идентификационный номер домена (первичный ключ)
2	name	Основной DNS-суффикс домена
3	purpose	Предназначение (описание) домена
4	IP	IP-адрес контроллера домена

Таблица 2.12 – Сущность «Inits» («Инициализации»)

№ п/п	Название поля	Описание поля
1	idInit	Идентификационный номер инициализации системы (первичный ключ)
2	isFirstStart	Значение поля показывает, была ли инициализация системы (если система запускается впервые, то инициализация не произведена)

Таблица 2.13 – Сущность «AuthTypes» («Типы аутентификации»)

№ п/п	Название поля	Описание поля
1	idAuthType	Порядковый номер типа аутентификации (первичный ключ)
2	name	Название типа аутентификации («встроенная», «доменная», «смешанная»)

Таблица 2.14 – Сущность «EmployeeStatus» («Статус сотрудника»)

№ п/п	Название поля	Описание поля
1	idEmployeeStatus	Порядковый номер возможного статуса сотрудника (первичный ключ)
2	name	Названия возможных статусов сотрудника («онлайн», «офлайн», «занят» и т.д.)

Таблица 2.15 – Сущность «Settings» («Параметры»)

№ п/п	Название поля	Описание поля
1	idSettings	Порядковый номер совокупности параметров (первичный ключ)
2	idDomain	Порядковый номер домена, для которого актуальна данная совокупность параметров (внешний ключ)
3	idAuthType	Порядковый номер типа аутентификации (внешний ключ)
4	idSettingsEmpStatus	Порядковый номер способа фиксации статуса сотрудника (внешний ключ)
5	nameSite	Полное название информационной системы
6	nameSiteShort	Краткое название информационной системы
7	fullName	Полное ФИО контактного лица, производившего инициализацию системы (суперадминистратора)
8	post	Должность суперадминистратора
9	phone	Контактный телефон суперадминистратора
10	email	Адрес электронной почты суперадминистратора
11	address	Почтовый адрес суперадминистратора
12	isFotoUsed	Использовать ли реальные аватары ИТ-сотрудников
13	fileUpload	ВЛОБ-файл конфигурации для взаимодействия со СКУД (при наличии таковой)

Таблица 2.16 – Сущность «SettingsEmpStatus» («Параметры Статусов сотрудников»)

№ п/п	Название поля	Описание поля
1	idSettingsEmpStatus	Порядковый номер параметра статуса сотрудников (первичный ключ)
2	name	Параметр, характеризующий способ фиксации статусов сотрудников (вручную или же при помощи СКУД)

Таблица 2.17 – Сущность «IncidentStatus» («Статус инцидента»)

№ п/п	Название поля	Описание поля
1	idIncidentStatus	Порядковый номер статуса инцидента (первичный ключ)
2	name	Статус инцидента

На рисунке 2.8 представлена даталогическая модель открытой информационной системы управления инцидентами, которая могла бы использоваться в деятельности некоторой абстрактной ИТ-службы (или ИТ-отдела) при решении ИТ-инцидентов, возникающих в организации. Данная модель также была построена с использованием бесплатной версии программы ERwin Data Modeler.

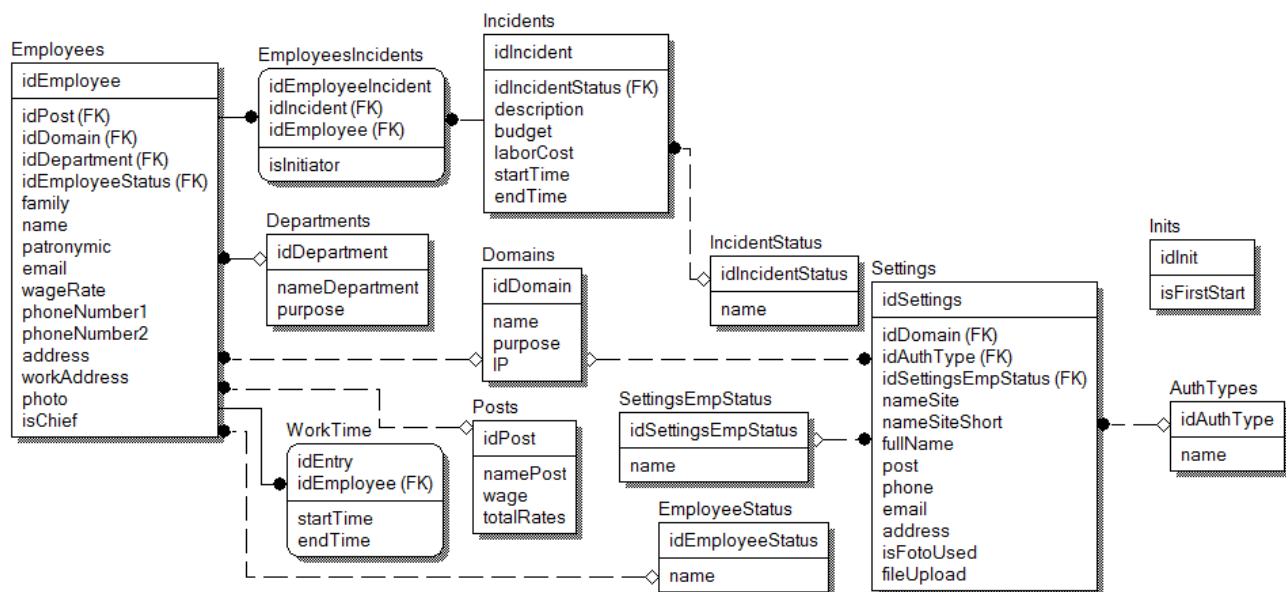


Рисунок 2.8 – Даталогическая модель базы данных (ИТ-служба/отдел)

Разработанная даталогическая модель включает в себя те же сущности, что и предыдущая, за исключением «Clients», «Products» и «ClientsProducts». Спецификации полей сущностей не имеют отличий, за исключением вновь появившегося поля «isInitiator» сущности «EmployeesIncidents». Данное поле является логической переменной, показывающей, является ли сотрудник инициатором инцидента, или же он является лицом, ответственным за разрешение инцидента. Кроме того, по очевидным причинам поле «idClient» в указанной сущности будет отсутствовать.

Итак, моделирование информационной системы практически завершено. Прежде, чем переходить к непосредственному проектированию базы данных, необходимо также выбрать СУБД, которая будет использоваться.

2.5 Выбор СУБД и его обоснование

В качестве доступных конечному пользователю СУБД предполагается использовать MySQL и Microsoft SQL Server (версий 2005 и выше). Такой выбор обусловлен несколькими причинами, речь о которых пойдет далее.

Во-первых, перечисленные СУБД являются одними из самых распространенных полноценных серверных СУБД – входят в первую тройку рейтинга согласно [26].

Во-вторых, стандартизация упомянутых СУБД находится на достаточно высоком уровне [13], что позволит сократить временные и умственные затраты на их освоение.

В-третьих, выбранные СУБД достаточно легко подлежат освоению. Здесь можно отметить наличие большого числа обучающих курсов, видеоуроков, мастер-классов. Кроме того, существует достаточное количество информатиков, обладающих внушительными знаниями по данным СУБД и способных дать консультацию по возникающим при освоении вопросам.

Опираясь на полученные в данной главе модели, можно осуществить проектирование и построение открытой информационной системы управления

ИТ-инцидентами. А в перспективе, осуществить ее внедрение в деятельности одной или нескольких ИТ-компаний, ИТ-отделов или ИТ-служб и исследовать положительный эффект от использования открытых информационных систем в процессе управления ИТ-инцидентами.

ГЛАВА 3 РАЗРАБОТКА И РЕАЛИЗАЦИЯ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ- ИНЦИДЕНТАМИ

3.1 Диаграмма деятельности и ее спецификация

Диаграмма деятельности (также встречается название «диаграмма активности») представляет собой диаграмму в нотации UML, на которой представлены какие-либо деятельности. Под деятельностями понимают координированное последовательное и параллельное выполнение подчиненных элементов – вложенных деятельностей и отдельных действий, которые соединяются между собой при помощи так называемых «потоков». Построение диаграммы деятельности – важный этап проектирования любой ИС [14].

Построим диаграмму деятельности открытой информационной системы управления ИТ-инцидентами. Построенная диаграмма приведена на рисунке 3.1.

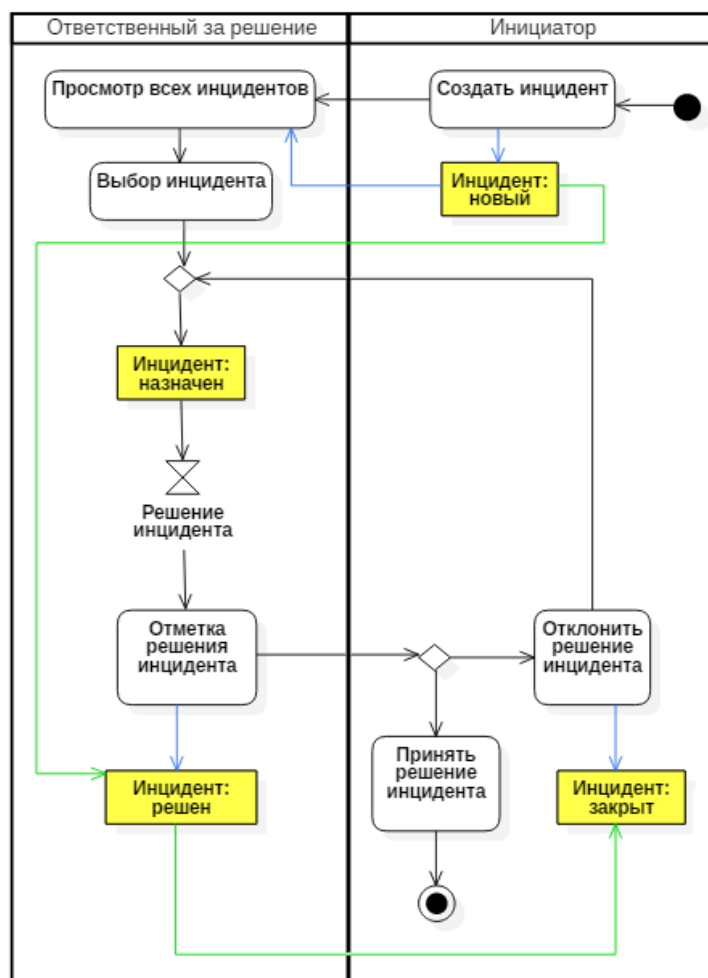


Рисунок 3.1 – Диаграмма деятельности

Составим спецификацию диаграммы деятельности.

Действия (активности):

«Создать инцидент» – инициатор регистрирует в единой системе новый инцидент в соответствии с возникшим событием состояния ИТ-инфраструктуры.

«Просмотр всех инцидентов» – сотрудник, ответственный за решение инцидентов, просматривает список активных в системе инцидентов, созданных заказчиками.

«Выбор инцидента» – сотрудник выбирает инцидент из списка.

«Решение инцидента» – комплекс действий (вне системы), направленных на анализ инцидента, поиск средств для его решения и непосредственное решение инцидента.

«Отметка решения инцидента» – сотрудник помечает решенный

инцидент в системе, присваивая ему статус «решен», о чем приходит уведомление заказчику.

«Принять решение инцидента» – инициатор анализирует результат решения инцидента и принимает его.

«Отклонить решение инцидента» – инициатор анализирует результат решения инцидента и не принимает его, обосновывая свое решение заказчику – инцидент возвращается в систему как нерешенный.

Возможные состояния инцидента:

«Новый» – новый, только что созданный инцидент, поступивший в систему от инициатора.

«Назначен» – инциденту был назначен исполнитель.

«Решен» – инцидент, помеченный сотрудником как выполненный. Подлежит закрытию либо не закрытию инициатором.

«Закрыт» – инцидент, прошедший полный цикл обработки в системе и помеченный инициатором как закрытый (выполненный).

3.2 Построение базы данных открытой информационной системы управления ИТ-инцидентами

Построим унифицированный (т.е. подходящий как для ИТ-отдела/ИТ-службы, так и для ИТ-компании) шаблон базы данных открытой информационной системы управления ИТ-инцидентами в соответствии с составленными во второй главе настоящего диссертационного исследования моделями базы данных. Дополним данный шаблон стандартным набором таблиц, необходимым для работы встроенной аутентификации пользователей – ASP.NET Identity (рисунок 3.2).

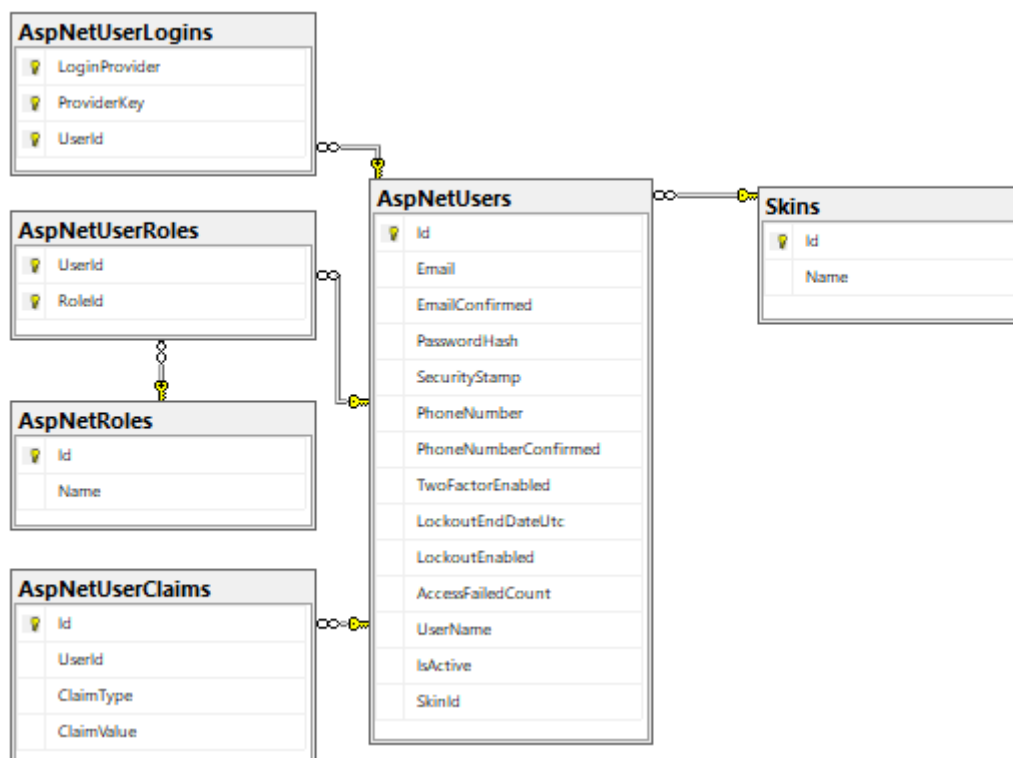


Рисунок 3.2 – Таблицы ASP.NET Identity

В качестве пользователей информационной системы могут выступать только Сотрудники и Заказчики. Следовательно, необходимо дополнительно создать следующие связи:

- между таблицей «AspNetUsers» и таблицей «Employees»;
- между таблицей «AspNetUsers» и таблицей «Clients»;

Диаграмма построенного шаблона БД представлена на рисунке 3.3.

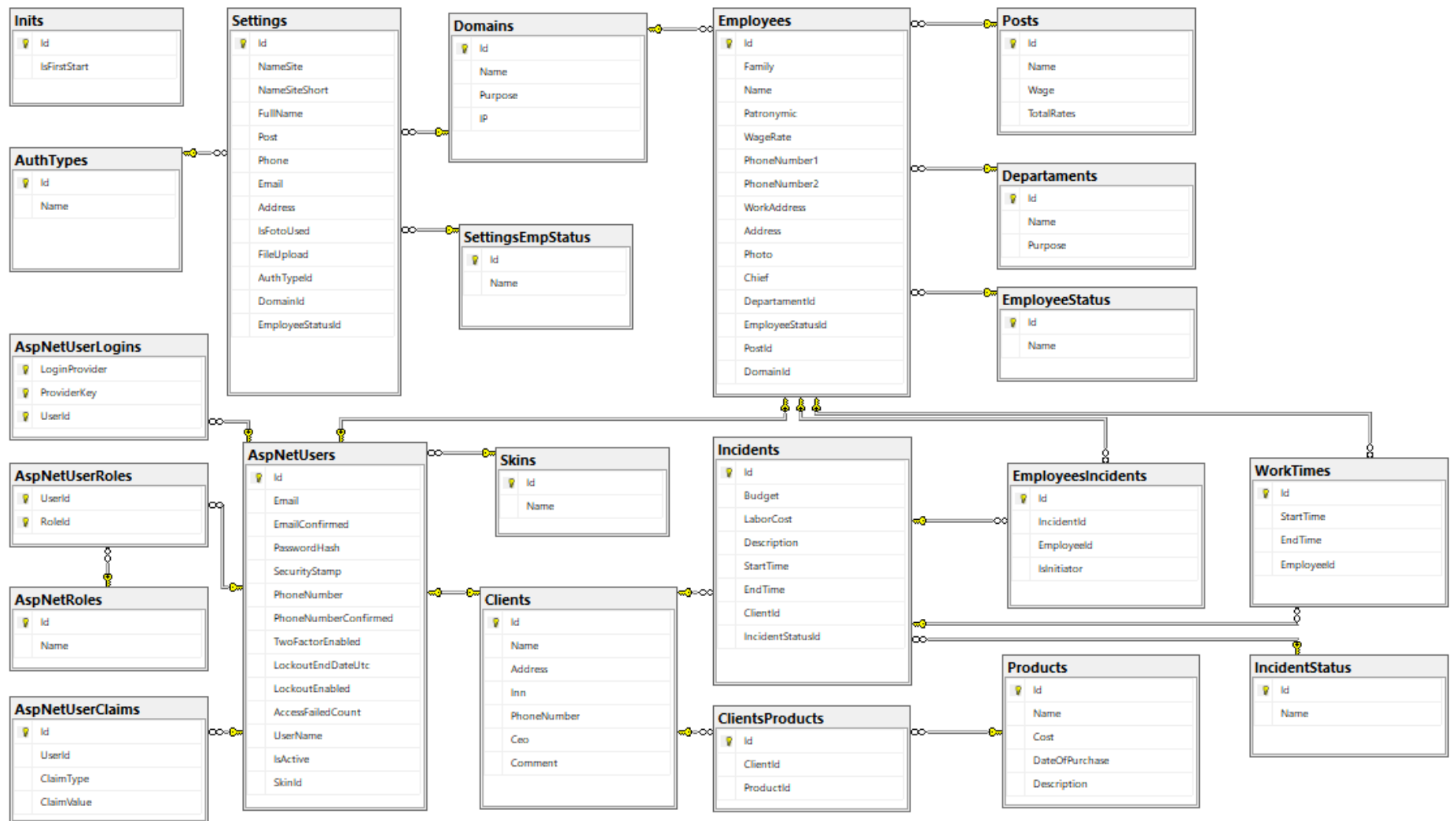


Рисунок 3.3 – Диаграмма шаблона базы данных

Диаграммы шаблонов были составлены с использованием средств утилиты Microsoft SQL Server Management Studio 2008, однако сами шаблоны могут быть также построены в средах Microsoft SQL Server 2005 (или выше) или MySQL в зависимости от предпочтений конечного пользователя.

Данные шаблоны могут быть до определенной степени кастомизированы в ходе процесса построения информационной системы при помощи конструктора, речь о котором пойдет далее.

3.3 Выбор среды разработки и его обоснование

На этапе проектирования любого программного продукта важным вопросом является выбор программных средств для его реализации. Средства разработки должны не только обеспечивать возможность полноценно реализовать функциональную часть программного продукта, но и обеспечивать максимально простой и эффективный процесс разработки, соответствовать масштабу проекта и перспективам его развития.

Основными параметрами, повлиявшими на выбор платформы для реализации продукта, стали следующие:

- производительность;
- удобство средств разработки;
- компонентная ориентированность;
- открытость;
- расширяемость архитектуры.

После анализа инструментальных средств для создания проектируемого продукта (системы автоматизации процессов эксплуатации ИТ-услуг), был сделан выбор в пользу платформы ASP.NET с реализацией шаблона Model-View-Controller (ASP.NET MVC).

Архитектурный шаблон MVC подразумевает схему разделения на три отдельных компонента данных приложения, пользовательского интерфейса и управляющей логики. Таким образом, каждый из компонентов может

модифицироваться независимо от других. Преимуществами такой структуры являются:

- широкие возможности для масштабирования проекта по мере его развития;
- разделение логики от представления данных;
- возможности эффективного тестирования разрабатываемого программного продукта;
- четкая структурированность кода и простота повторного применения решений.

Платформа ASP.NET, в свою очередь, обладает следующими характеристиками:

- бесплатная среда разработки с полной поддержкой;
- основываясь на платформе программирования .NET, ASP.NET имеет развитую и развивающуюся архитектуру, благодаря чему имеется возможность использования широкого спектра готовых инструментов (классов, фреймворков, встроенных элементов управления и др.);
- широкий выбор поддерживаемых языков программирования;
- быстрая компиляция и исполнение кода.

По сравнению с распространенным языком веб-программирования PHP, ASP.NET имеет следующие преимущества:

- в среде ASP.NET приложение реализуется на строго типизированных компилируемых .NET языках, таким образом значительно упрощается отладка приложения по сравнению PHP;
- ASP.NET включает большое количество встроенных стандартных библиотек, что облегчает процесс разработки;
- ASP.NET предоставляет больше возможностей для создания веб-приложений со сложной логикой, без потери четкости структуры программного кода, а также больше возможностей для масштабирования готового приложения в дальнейшем.

Основной недостаток ASP.NET по сравнению с PHP – производительность и объем используемого трафика – достаточно успешно разрешен в ASP.NET MVC за счет отказа от компонентной архитектуры в пользу серверных вставок и выделения Master-страниц.

Сравнение популярных фреймворков ASP.NET MVC и Java Spring позволяет сделать следующие выводы:

- ASP.NET MVC проще в использовании за счет более простого кода конфигурации. Фреймворк Spring требует написания большего объема кода конфигурации xml/java, помимо этого, иногда требуется использование сторонних инструментов;

- большое количество документации и активное сообщество ASP.NET MVC упрощает работу с данной платформой, позволяя легче находить готовые решения для имеющихся задач.

Таким образом, на основании проведенного анализа средств разработки, был сделан вывод о целесообразности использования для разработки данного проекта платформы ASP.NET и фреймворка MVC. Решающими характеристиками стали следующие:

- открытый код;
- простота масштабирования проекта;
- обилие готовых решений частных задач;
- высокая производительность и скорость компиляции;
- возможности эффективного тестирования.

Также следует отметить, что выбранная среда разработки на сегодняшний день имеет достаточно широкий набор инструментов для разработки мобильных приложений, что, хотя и не рассматривается на данном этапе разработки программного инструментария, но может стать актуальным по мере его дальнейшего развития.

3.4 Разработка и реализация конструктора открытой информационной системы управления ИТ-инцидентами

При помощи инструмента «Проволочная диаграмма» [26] векторного графического редактора Microsoft Visio спроектируем экранные формы конструктора открытой информационной системы управления ИТ-инцидентами. Будем исходить из того, что построение системы происходит в два шага:

- на первом шаге происходит выбор основных параметров информационной системы;
- на втором шаге производится тонкая настройка информационной системы в соответствии с потребностями, предпочтениями и техническими возможностями конечного пользователя.

Макеты экранных форм шагов 1 и 2 представлены на рисунках 3.4 и 3.5 соответственно.

Инструментарий построения открытой информационной системы управления ИТ-инцидентами

Шаг 1. Выбор основных параметров ИС

Выберите масштаб использования ИС: ИТ-отдел/служба ИТ-компания

Используются ли домены для авторизации пользователей? Да, Active Directory Да, Samba Домены не используются

Используется ли система контроля и управления доступом (СКУД)? Да Нет

Использовать аватары (фотографии) ИТ-персонала?

Укажите СКУД

ФАНТОМ

РусГард

Старк

Далее > Отмена

Рисунок 3.4 – Шаг 1

Инструментарий построения открытой информационной системы управления ИТ-инцидентами

Шаг 2. Тонкая настройка ИС

Укажите сетевой адрес *либо* DNS-имя основного контроллера домена:

Укажите путь к аватарам (фотографиям) ИТ-персонала:

Укажите сетевой адрес *либо* имя сервера базы данных:

Укажите имя пользователя базы данных: Пароль:

Укажите название базы данных:

Необходимо построение базы данных* Путь к выходному файлу:

Необходимо построение программного обеспечения* Путь к выходной папке:

** - как минимум один флажок должен быть выбран для продолжения*

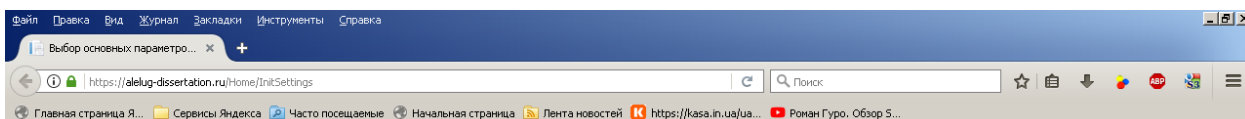
Рисунок 3.5 – Шаг 2

В соответствии со спроектированными макетами был разработан программный комплекс (конструктор) для построения информационной системы управления инцидентами в сфере информационных технологий с использованием следующих программных средств:

- платформа разработки – ASP.NET, язык программирования C#;
- поддерживаемые СУБД: MS SQL 2005 и выше, MySQL;
- регистрация/авторизация пользователей: ASP.NET Identity.

Система реализуется в виде web-приложения.

Конструктор появляется при первом запуске системы, являясь стартовой страницей (рисунок 3.6).



Выбор основных параметров ИС

Масштаб применения ИС	<input type="text" value="ИТ-компания"/>
Название ИС	<input type="text"/>
Краткое название ИС	<input type="text"/>
Мое ФИО	<input type="text"/>
Должность	<input type="text"/>
Номер телефона	<input type="text"/>
Почтовый адрес	<input type="text"/>
Адрес	<input type="text"/>
Способ Аутентификации	<input type="text" value="Встроенная"/>
Фиксация статуса	<input type="text" value="Вручную сотрудником"/>
Использовать аватары	<input type="checkbox"/>
	<input type="button" value="Сохранить"/>

Рисунок 3.6 – Интерфейс стартовой страницы (конструктора)

Далее необходимо получить представление о том, какая информационная система может быть построена при помощи данного конструктора.

3.5 Разработка и реализация открытой информационной системы управления ИТ-инцидентами

Пользовательский интерфейс информационной системы управления ИТ-инцидентами может быть рассмотрен со следующих точек зрения:

1. Заказчик – инициатор инцидента. В роли заказчика может выступать любой сотрудник предприятия, в структуру которого входит ИТ-отдел (ИТ-служба), либо клиент ИТ-компании. Заказчик имеет право создавать инциденты в системе и отслеживать ход их разрешения.

2. Администратор системы. Имеет полный доступ к системе: может просматривать все поступившие в систему инциденты, назначать любых исполнителей ответственными за решение инцидентов, менять исполнителей после назначения, изменять статус решения инцидентов, вносить изменения в тонкие настройки системы и т.д.

3. Исполнитель. Имеет ограниченный доступ к системе: может просматривать только назначенные ему инциденты или не назначенные никому, а также может назначать самого себя ответственным за решение поступивших в систему инцидентов, но не может менять исполнителей после назначения.

Экранная форма пользовательского интерфейса заказчика представлена на рисунке 3.7.

ОИС управления ИТ-инцидентами. Имя сервера - 'localhost', имя базы - 'IncidentsManagement'

Новый инцидент Мои инциденты Помощь

Пользователь: Адамов И.В. (Выход)

Пожалуйста, опишите проблему/инцидент.

Информировать о ходе решения по электронной почте: Нет

Описание:

Зарегистрировать инцидент

Рисунок 3.7 – Интерфейс заказчика

Экранная форма пользовательского интерфейса администратора представлена на рисунке 3.8.

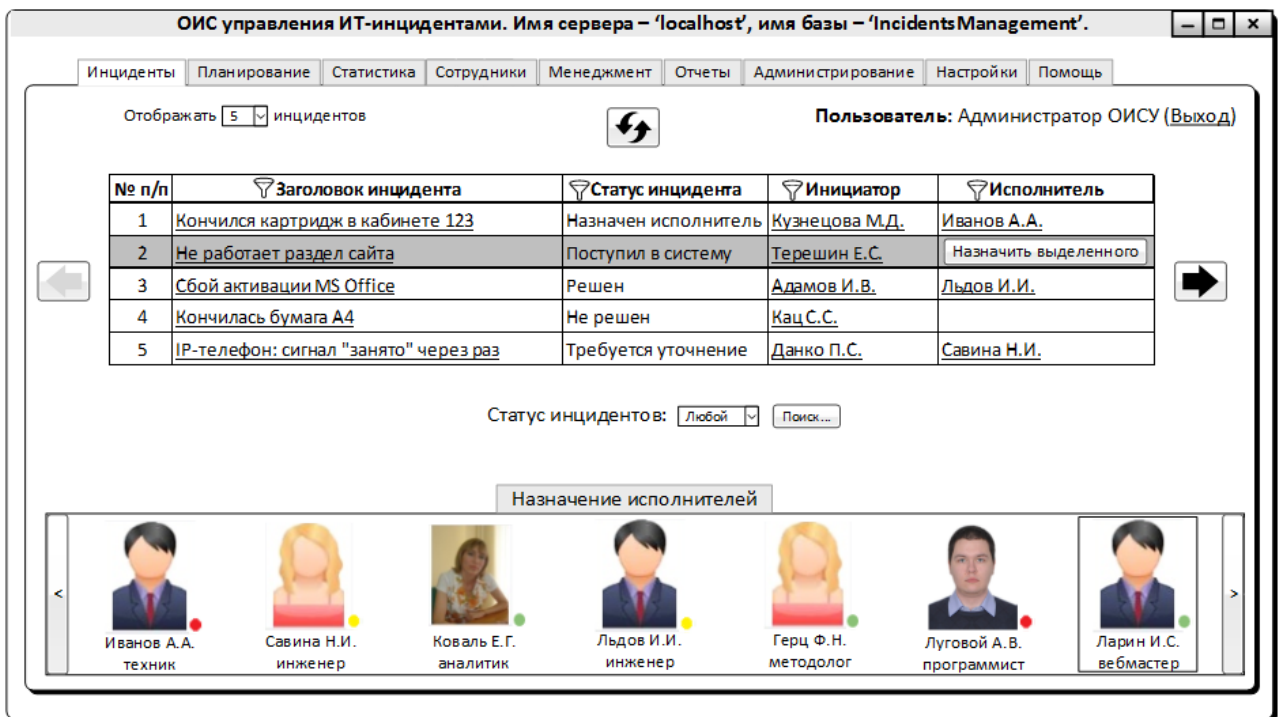


Рисунок 3.8 – Интерфейс администратора

Экранная форма пользовательского интерфейса исполнителя представлена на рисунке 3.9.

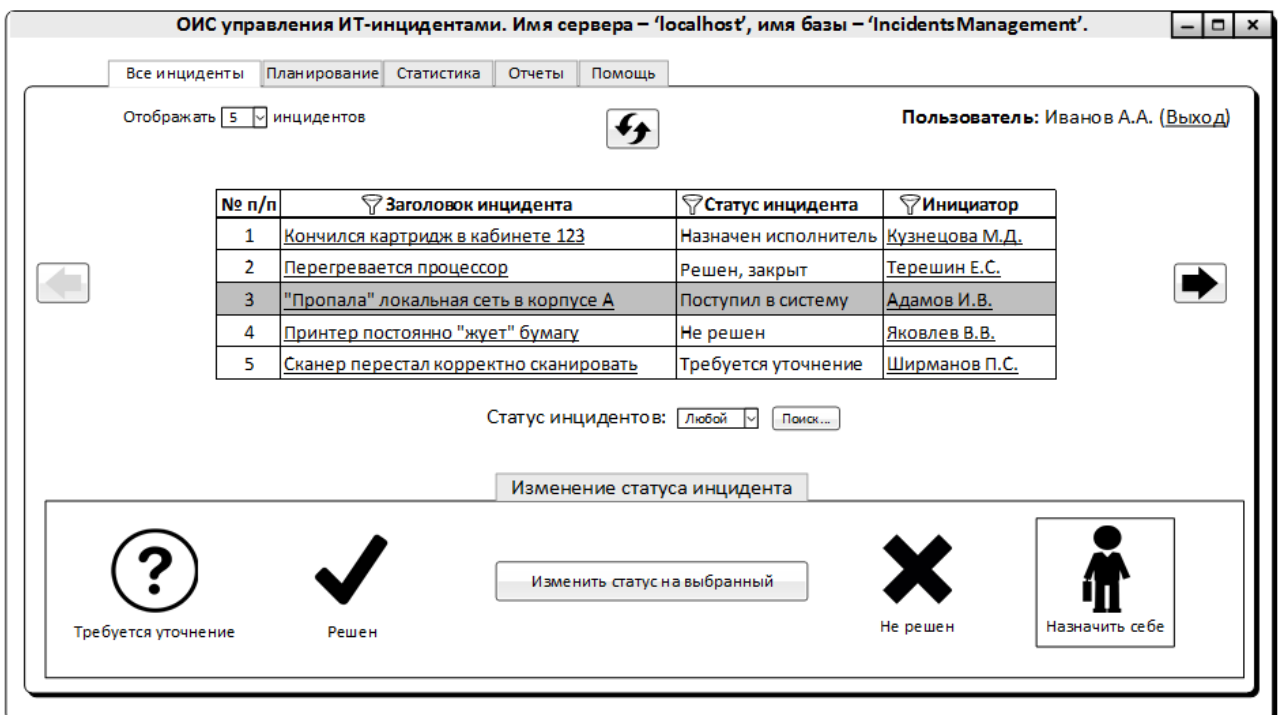



Рисунок 3.9 – Интерфейс исполнителя

Серым цветом на рисунках 3.8-3.9 выделен выбранный в текущий момент времени инцидент. Выбор происходит однократным нажатием левой кнопки мыши. Повторное нажатие отменяет выбор. Не допускается выбор более чем одного инцидента – в случае выбора другого инцидента при уже выбранном отменяется выбор более раннего.

В нижней панели на рисунках 3.8-3.9 («Назначение исполнителей» или «Изменение статуса инцидента») прямоугольной рамкой обозначается выбранный в текущий момент времени элемент панели. Повторное нажатие отменяет выбор. Не допускается выбор более чем одного элемента – в случае выбора другого инцидента при уже выбранном отменяется выбор более раннего.

Значком  обозначается фильтр по текущему столбцу. Первое нажатие по значку приводит к сортировке инцидентов по выбранному критерию в прямом порядке, второе нажатие – в обратном порядке, третье нажатие отменяет фильтр. По умолчанию производится сортировка по возрастанию порядкового номера (ID) инцидентов.

Форма авторизации пользователей выглядит одинаково для всех трех уровней доступа пользователей. При запуске информационной системы пользователь видит эту форму первой. Макет ее внешнего вида представлен на рисунке 3.10.

ОИС управления ИТ-инцидентами. Имя сервера – 'localhost', имя базы – 'IncidentsManagement'

Авторизация пользователя в системе

Вход в открытую информационную систему управления ИТ-инцидентами компании ООО «Вектор».

Пожалуйста, введите выданные Вам реквизиты доступа к системе.

Домен:

Логин:

Пароль:

Внимание! В случае ввода некорректных учетных данных более трех раз подряд, Ваша учетная запись будет заблокирована на 15 минут.

Рисунок 3.10 – Форма авторизации пользователей

В построенной системе обеспечена криптографическая защита аутентификационных данных, хранимых и передаваемых по сети в рамках процедур идентификации и аутентификации (ASP.NET Identity).

В целях безопасности исключается возможность ввода некорректных реквизитов доступа к системе более трех раз. После четвертой неудачной попытки входа учетная запись данного пользователя будет заблокирована на 15 минут (при использовании доменов блокировка произойдет также на уровне контроллера домена на заданный доменной политикой промежуток времени). Досрочная разблокировка учетной записи может быть произведена администратором информационной системы либо администратором домена, если при построении системы была отмечена необходимость интеграции с контроллером домена.

Приложение не требует использования в штатном режиме работы пользователей съемных носителей информации. Место расположения объекта

для выгрузки/загрузки является настраиваемым и позволяет загружать/выгружать файлы с ресурса сети, идентифицируемого IP-адресом или DNS-именем.

В структуре построенной информационной системы можно выделить следующие модули:

- управление инцидентами;
- управление конфигурациями;
- управление пользователями;
- анализ и отчетность;
- база знаний.

Основная задача сформированной системы – служить точкой связи, контакта между клиентами (пользователями), информационной инфраструктурой и техническими специалистами для оказания квалифицированной технической поддержки. Ключевые операции системы для реализации данной цели приведены в таблице 3.1.

Таблица 3.1 – Основные операции

№ п/п	Наименование операций
1	Прием, регистрация обращений пользователей по вопросам ИТ-инцидентов
2	Идентификация и обработка Инцидентов и запросов на обслуживание
3	Накопление базы знаний по решенным инцидентам
4	Управление жизненным циклом Инцидента
5	Информирование пользователей о текущем статусе обращений
6	Контроль сроков решения инцидентов
7	Диспетчеризация инцидентов специалистам соответствующей квалификации

Функциональные возможности открытой информационной системы таковы:

- регистрация пользователей (новых заказчиков и исполнителей);
- доступ пользователей к данным согласно разрешениям;
- открытие (регистрация в системе) инцидента;
- учет и отображение статусов исполнителей (не в сети/занят/свободен);
- назначение исполнителя для открытого инцидента;

- изменение статуса инцидента;
- ведение статистики работы системы;
- формирование отчетов по работе системы.

В общем случае работа открытой информационной системы управления ИТ-инцидентами может быть представлена в виде пяти основных этапов:

1. Пользователь обращается в Службу с заявкой о Проблеме (Инциденте).
2. Поступившая заявка получает уникальный номер и отображается в списке инцидентов. Назначение Исполнителя выполняется либо Администратором, либо непосредственно Исполнителем (самоназначение).
3. Исполнитель решает проблему, либо запрашивает уточнение, либо отказывается от решения (изменение статуса на «не решен»).
4. Фиксируется закрытие инцидента.
5. Выполняются работы по извещению пользователя.

Работа с системой со стороны пользователя предполагает, что данной системой будут пользоваться неспециалисты, соответственно, ставилась задача разработки максимально простого интуитивно понятного интерфейса. Разработанный интерфейс отвечает всем требованиям, а именно:

- интерфейс готового программного продукта соответствует разработанным прототипам;
- стиль интерфейса соответствует задачам программного продукта (минималистичный стиль с простой навигацией, с малым использованием графических элементов и максимально стандартизованными элементами управления);
- соответствие интерфейса основным правилам дизайна, что облегчает визуальное восприятие и работу с системой;
- респонсивность интерфейса, что позволяет использовать ПО не только на стационарных компьютерах, но и на мобильных устройствах (планшет, смартфон).

Рассмотрим подробнее функциональные возможности, предоставляемые

сервисом для пользователей, обладающих разными уровнями доступа.

Разработанная открытая информационная система управления ИТ-инцидентами предоставляет возможность для работы трех групп пользователей:

- пользователи, которые обращаются к помощи службы технической поддержки;
- операторы, реагируют на заявки пользователей;
- админруководство, которые берет на себя полный контроль над функционированием системы и осуществляет управление задачами пользователей.

Соответственно, в системе выделено три роли:

- Заказчик – инициатор инцидента. Заказчик имеет право только создавать инциденты в системе и отслеживать ход их разрешения.

- Администратор системы. Имеет полный доступ к системе: может просматривать все поступившие в систему инциденты, назначать любых исполнителей ответственными за решение инцидентов, менять исполнителей после назначения, изменять статус решения инцидентов, вносить изменения в настройки системы, регистрировать новых пользователей и исполнителей и т.д.

- Исполнитель. Имеет ограниченный доступ к системе: может просматривать только назначенные ему инциденты или не назначенные никому, а также может назначать самого себя ответственным за решение поступивших в систему инцидентов, но не может менять исполнителей после назначения.

Работа с разработанным программным инструментарием начинается с определения настроек формирования.

При построении информационной системы определяются (выбираются) следующие основные параметры:

- масштаб применения ИС;
- название ИС;

- краткое название ИС;
- ФИО контактного лица, ответственного за эксплуатацию ИС;
- должность контактного лица;
- номер телефона;
- почтовый адрес;
- адрес;
- способ Аутентификации;
- домен;
- способ фиксации статуса;
- использовать или не использовать аватары.

Внешний вид интерфейсов для пользователя, исполнителя и администратора соответствует макетам, разработанным на этапе проектирования (рис. 3.11, 3.12 и 3.13 соответственно).

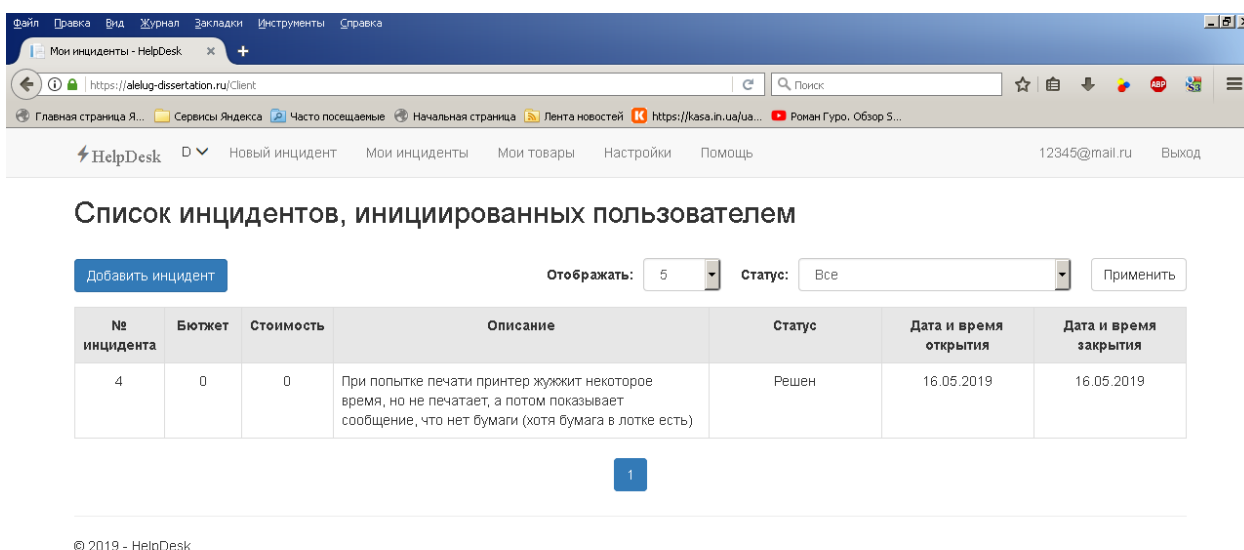


Рисунок 3.11 – Интерфейс системы для пользователя

Для уровня доступа «Пользователь» доступны следующие функции:

1. Новый инцидент: Пользователь имеет возможность ввести информацию об инциденте и определить, необходимо ли информирование о ходе решения по электронной почте.

2. Мои инциденты: в данной вкладке представлен список инцидентов, инициированных пользователем, отображение которого происходит в виде таблицы. Пользователю предоставлена возможность выбрать, отображать ли весь список инцидентов или только с определенным, конкретно заданным статусом.

3. Помощь: на вкладке размещается инструкция пользователя и контактная информация службы поддержки.

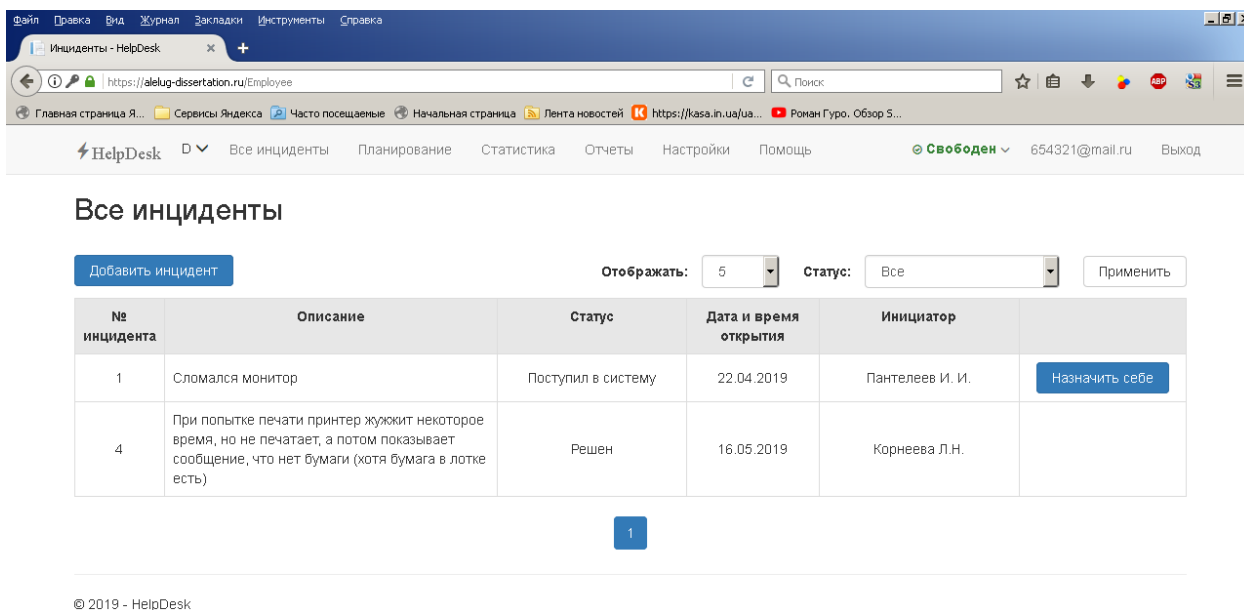


Рисунок 3.12 – Интерфейс системы для исполнителя

Для уровня доступа «Исполнитель» доступны следующие функциональные возможности:

1. Все инциденты: Все инициированные всеми пользователями инциденты отображаются в таблице. Выбранный в текущий момент времени инцидент подсвечивается серым фоном. Выбор происходит однократным нажатием левой кнопки мыши. Повторное нажатие отменяет выбор. Не допускается выбор более чем одного инцидента – в случае выбора другого инцидента при уже выбранном отменяется выбор более раннего.

Исполнитель имеет возможность выбрать статус отображаемого инцидента (выпадающий список со значениями «Все» и возможными статусами

инцидентов).

Для выбранного в текущий момент времени инцидента Исполнитель может изменить статус только в том случае, если исполнитель не назначен (поле «Исполнитель» пустое), либо если на решение инцидента назначен данный исполнитель (поле «Исполнитель» совпадает с ФИО пользователя). Для изменения статуса необходимо произвести выбор визуального элемента на поле в нижней части вкладки и осуществить нажатие кнопки «Изменить статус на выбранный».

2. Планирование: Исполнитель имеет возможность планировать свое рабочее время, фиксируя время начала и окончания работы над каждым инцидентом.

3. Статистика: на данной вкладке отображается статистика назначенных, находящихся в работе и закрытых Исполнителем инцидентов за выбранный период.

4. Отчеты: Исполнитель также имеет возможность на данной вкладке выбрать период отображения отчетных данных (Поля «с» и «по» - выбор календарной даты) и выбрать необходимые поля из списка для формирования отчета.

5. Помощь: на данной вкладке размещены инструкция по работе с системой, список часто задаваемых вопросов и контактные данные Администратора.

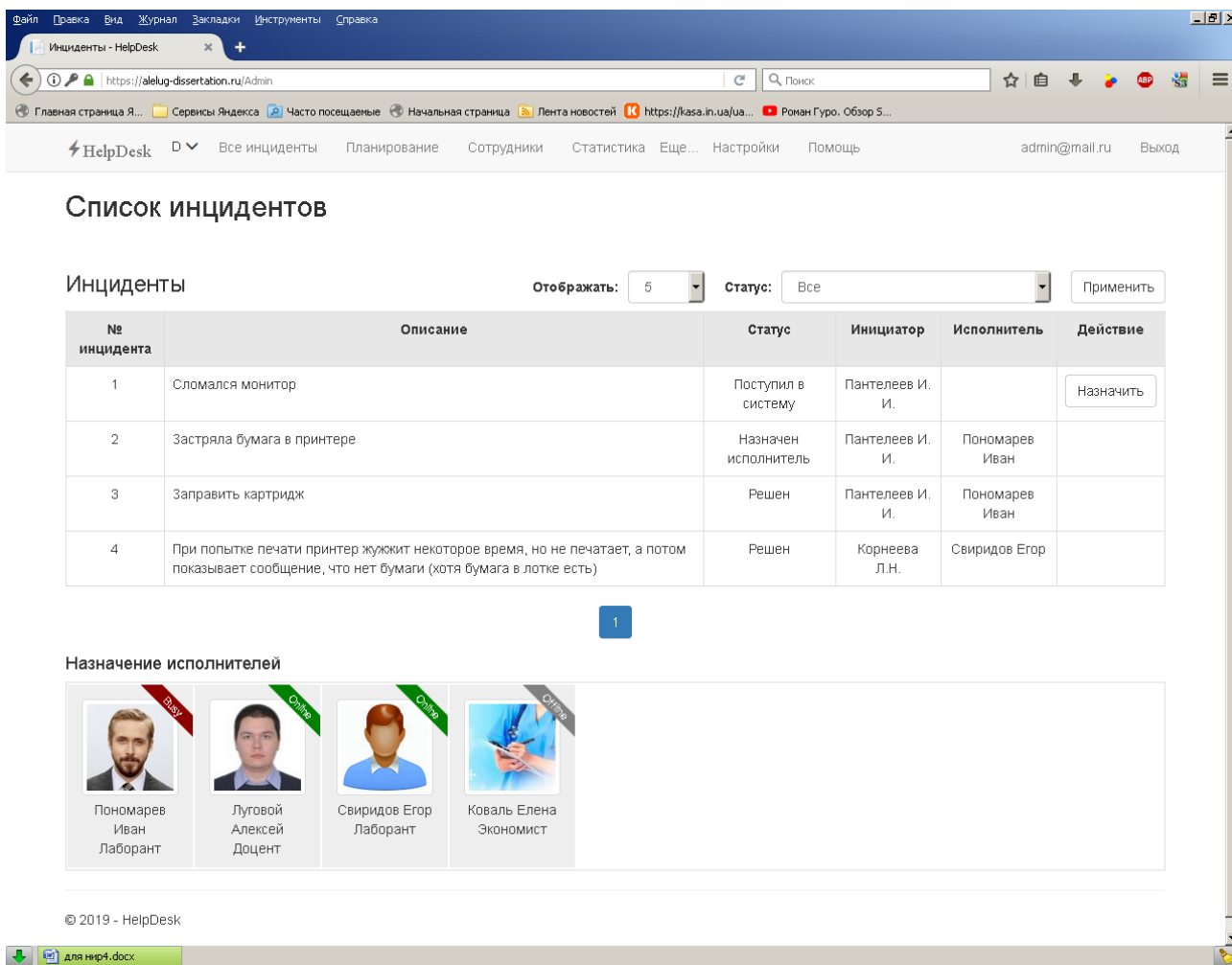


Рисунок 3.13 – Интерфейс системы для администратора

Для уровня доступа «Администратор» доступны следующие функциональные возможности:

1. Инциденты: Все инциденты отображаются в таблице. Выбранный текущий момент времени инцидент подсвечивается серым фоном. Выбор происходит однократным нажатием левой кнопки мыши. Повторное нажатие отменяет выбор. Не допускается выбор более чем одного инцидента – в случае выбора другого инцидента при уже выбранном отменяется выбор более раннего. Администратор имеет возможность выбрать статус отображаемых инцидентов (выпадающий список со значениями «Все» и возможными статусами инцидентов). Администратор имеет возможность назначить на инцидент любого исполнителя. Назначение происходит нажатием кнопки

«Назначить выбранного» после выбора (однократным нажатием левой кнопки мыши) инцидента из списка и исполнителя в нижнем поле.

2. Планирование: в данной вкладке Администратор имеет возможность просматривать страницу планирования выбранного Исполнителя. В верхней части экрана отображается календарь с возможностью выбора даты и поле «Сотрудник» с возможностью выбора из выпадающего списка одного из сотрудников.

3. Статистика: на данной вкладке Администратор имеет возможность выбрать период отображения статистических данных, а также выбрать отображение данных по всем Исполнителям либо по одному из них.

4. Сотрудники, Отделы, Должности: в данных вкладках Администратор имеет возможность управлять (добавлять, редактировать, удалять), соответственно, списками Исполнителей и Пользователей, Отделов организации и Должностей исполнителей.

6. Отчеты: Администратор имеет возможность на данной вкладке выбрать период отображения отчетных данных; выбрать отображение данных по всем Исполнителям либо по одному из них для формирования отчетности по работе отдела.

7. Настройки: На данной вкладке Администратор имеет возможность сменить пароль (своего аккаунта).

8. Помощь: на данной вкладке размещены инструкция по работе с системой, список часто задаваемых вопросов и контактные данные Службы поддержки Программного комплекса по созданию системы.

В ходе написания третьей главы диссертационного исследования была доработана концепция информационной системы, то есть в общих чертах описаны проектирование и разработка информационной системы в форме моделей, диаграмм и рисунков, и, таким образом, подготовлены все необходимые сведения для реализации технологии открытых систем.

В следующей главе будет произведена практическая апробация

получившейся информационной системы, оценена целевая и экономическая эффективность применения программного инструментария, проанализированы проблемы и перспективы развития программного инструментария.

ГЛАВА 4 ВНЕДРЕНИЕ, АПРОБАЦИЯ И ОЦЕНКА ЦЕЛЕВОЙ ЭФФЕКТИВНОСТИ ОТКРЫТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИТ-ИНЦИДЕНТАМИ

4.1 Внедрение и апробация программного комплекса на базе ВУиТ

Апробация результатов исследования была осуществлена на базе ИТ-отдела – отдела информатизации и автоматизации учебного процесса учебно-методического управления ВУиТ (Волжского университета имени В.Н. Татищева, г. Тольятти).

ИТ-инфраструктура университета включает в себя 26 компьютерных классов, больше 600 стационарных компьютеров, более 300 периферийных устройств (принтеры, сканеры и др.). Сетевое взаимодействие обеспечено единой гигабитной сетью (IaaS), а также гигабитными аплинками внутри корпусов, для абонентов предоставляется 100-мбитный доступ. Кроме того, следует отметить, что наблюдается устойчивая тенденция увеличения количества некомпьютерных абонентских IP-устройств: IP-телефоны, IP-камеры видеонаблюдения и др. Организована беспроводная сеть Wi-Fi, защищенная паролем.

Информационные технологии (ИТ) глубоко интегрированы во все процессы вуза – учебный, административно-хозяйственный, деловой. Соответственно, бесперебойная работа ИТ является критично важной для непрерывности работы учреждения, что обуславливает необходимость внедрения системы управления ИТ-инцидентами в современном вузе.

Цель создания службы управления ИТ-инцидентами в университете – повышение качества обслуживания конечных абонентов путем оперативного разрешения возникающих проблем за счет автоматизации процесса регистрации и распределения заявок. Таким образом, необходимо не только развертывание автоматизированного центра технической поддержки, но и стандартизация процедуры подачи заявки и правил ее оформления.

На момент проведения апробации разработанного программного

продукта для управления ИТ-инцидентами в университете не использовалась никакая система автоматизации, документирования инцидентов, их причин и методов решения, а также хода устранения велось частично, исключительно в ручном режиме.

На момент внедрения открытой информационной системы управления ИТ-инцидентами в учреждении для регистрации инцидентов пользователи имели возможность воспользоваться следующими каналами:

- телефонный звонок в службу поддержки;
- обращение по электронной почте;
- служебная записка.

Кроме того, достаточно часто пользователи обращались напрямую лично к работникам службы поддержки.

Документирование обращений пользователей производилось в специальном журнале в ручном режиме, однако, в журнал вносились не все инциденты.

Очевидными недостатками такой системы являлись следующие:

- скорость поступления заявок от пользователя в службу поддержки была низкой, из-за чего многие инциденты решались со значительными задержками;
- часть инцидентов не решалась (из-за отсутствия системы регистрации обращений о них просто забывали);
- сотрудникам ИТ-отдела необходимо было просматривать несколько источников (почта, журнал, поступившие служебные записки) для определения фронта работ;
- в связи с отсутствием учета не было возможности контролировать периодичность и тенденции возникновения инцидентов для дальнейшего анализа и возможности превентивного их устранения.

Кроме того, такая организация работы ИТ-отдела с пользователями не давала возможности оценить эффективность работы сотрудников отдела.

Внедрение открытой информационной системы управления ИТ-инцидентами состояло из нескольких этапов (таблица 4.1).

Таблица 4.1 – Этапы внедрения системы

Выполняемые работы	Результат	Срок, дней
Построение, установка и настройка системы на сервере университета	Система установлена, настроена и готова к работе	1
Формализация требований к пользователям и разработка типовых инструкций	Разработаны инструкции для пользователей и специалистов ИТ-отдела	3
Регистрация пользователей	Все специалисты ИТ-отдела и пользователи имеют личные аккаунты в системе	7
Обучение пользователей	Пользователи понимают принцип работы системы и могут самостоятельно оформить заявку в системе	14

При построении открытой информационной системы управления ИТ-инцидентами были применены следующие параметры (рисунок 4.1):

- масштаб применения ИС: ИТ-отдел/служба;
- название ИС: «Управление ИТ-инцидентами Волжского университета имени В.Н. Татищева»;
- краткое название ИС: «Управление ИТ-инцидентами ВУиТ»;
- мое ФИО (здесь подразумевается ФИО контактного лица, ответственного за эксплуатацию информационной системы): «Луговой Алексей Васильевич»;
- должность: «Начальник отдела ИКТ»;
- номер телефона: «62-48-61»;
- почтовый адрес: «alelug@vuit.ru»;
- адрес: «ул. Ленинградская 16, каб. 204»;
- способ Аутентификации: Доменная;
- домен (здесь подразумевается порядковый № контроллера домена): 1;
- фиксация статуса: Вручную сотрудником;
- использовать аватары: выбрано.

Выбор основных параметров ИС

Масштаб применения ИС	ИТ-отдел/служба
Название ИС	Управление ИТ-инцидентами Волжско
Краткое название ИС	Управление ИТ-инцидентами ВУиТ
Мое ФИО	Луговой Алексей Васильевич
Должность	Начальник отдела ИКТ
Номер телефона	62-48-61
Почтовый адрес	alelug@vuit.ru
Адрес	ул. Ленинградская 16, каб. 204
Способ Аутентификации	Доменная
Домен	1
Фиксация статуса	Вручную сотрудником
Использовать аватары	<input checked="" type="checkbox"/>

Сохранить

Рисунок 4.1 – Параметры построения

Разработка инструкций для пользователей проводилась совместно с сотрудниками ИТ-отдела университета. Учитывая максимально удобную и интуитивно понятную работу системы, проводить обучение сотрудников ИТ-отдела не потребовалось, достаточно было изучения ими технической документации по работе с системой.

Обучение пользователей проводилось в два этапа: на первом этапе было проведено обучение для ответственных сотрудников (назначенных от каждой кафедры и подразделения), а далее каждый из них проводил обучение для других пользователей на своей кафедре либо подразделении университета.

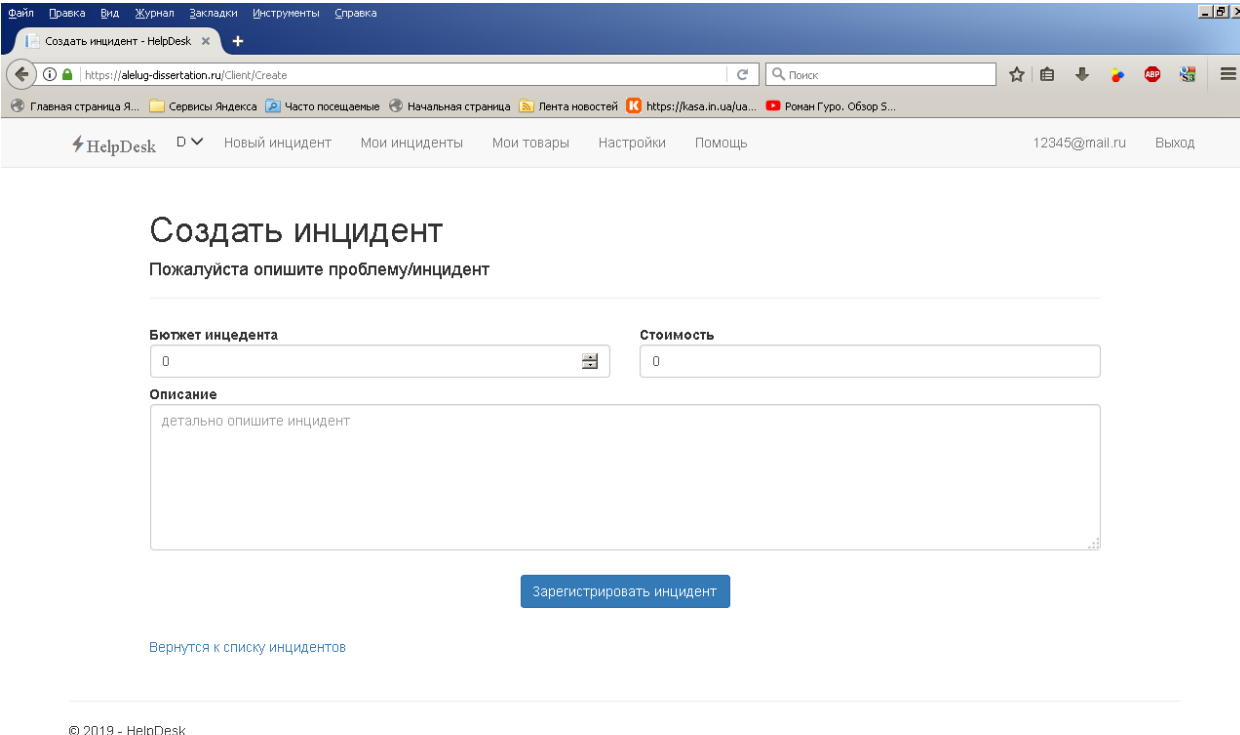
При внедрении открытой информационной системы управления ИТ-инцидентами возникли некоторые сложности, связанные с нежеланием части пользователей переходить на новую систему решения ИТ-инцидентов, решение этого вопроса возможно исключительно при безоговорочной поддержке руководства учреждения.

Для пользователей системы были разработаны простые и четкие инструкции, максимально формализующие работу с системой.

Инструкция для пользователя по составлению заявок в системе:

1. Зайти на страницу авторизации системы в браузере.
2. Авторизоваться в системе (ввести свой логин и пароль).
3. Нажать кнопку «Добавить инцидент» (рисунок 4.2).
4. Заполнить описание инцидента, обязательно указав номер кабинета и инвентарный номер оборудования, с которым возникла проблема.
5. Указать ориентировочные трудозатраты и бюджет инцидента (либо не заполнять данные поля в случае отсутствия информации).
6. Нажать кнопку «Зарегистрировать инцидент» и заявка будет отправлена в службу поддержки.

Для упрощения работы пользователей, страницы авторизации (пункт 1 инструкции) были сохранены в «закладках» браузеров пользователей при помощи доменной политики.



The screenshot shows a web browser window with the URL <https://alekug-dissertation.ru/Client/Create>. The page title is "Создать инцидент - HelpDesk". The main heading is "Создать инцидент" with the instruction "Пожалуйста опишите проблему/инцидент". Below this are two input fields: "Бюджет инцидента" (Budget of the incident) and "Стоимость" (Cost), both containing the value "0". A large text area labeled "Описание" (Description) contains the placeholder text "детально опишите инцидент". At the bottom of the form is a blue button labeled "Зарегистрировать инцидент". A link "Вернуться к списку инцидентов" is located below the button. The footer of the page reads "© 2019 - HelpDesk".

Рисунок 4.2. Форма создания заявки пользователем

После внедрения открытой информационной системы управления ИТ-инцидентами обращение в службу ИТ-поддержки для пользователей значительно упростилось, так как создание заявки занимает не более пяти минут, при этом она гарантированно передается работникам ИТ-отдела. В свою очередь, сотрудники ИТ-отдела получили возможность моментально получать информацию о новых заявках без необходимости регистрировать их вручную и собирать из различных источников. Также внедрение системы стало важным источником информации о степени загруженности и эффективности работы сотрудников для руководителя ИТ-отдела. Количественные показатели, определяющие эффективность внедрения системы в учреждении, будут рассмотрены далее.

В то же время в ходе апробации системы были выявлены некоторые сложности и недочеты в ее работе, а именно:

1. Отображение инцидента в системе единым полем, отсутствие заголовка.

2. Отсутствие системы классификации и назначения исполнителей инцидентов. Достаточно большую долю заявок составляют инциденты, связанные с простыми техническими неполадками (застряла бумага в принтере) или поточным обслуживанием компьютеров и периферийных устройств. Большую часть таких инцидентов способны решить лаборанты. Однако, подключение лаборантов в систему в качестве исполнителей нецелесообразно, так как они не являются непосредственно сотрудниками ИТ-отдела, при этом общее их число значительно превышает количество сотрудников отдела. Таким образом, добавив лаборантов в качестве исполнителей, мы бы значительно затруднили процесс отслеживания эффективности работы сотрудников ИТ-отдела.

3. Отсутствие системы приоритетов, позволяющей определить степень критичности инцидента для рабочего процесса. Каждая сформированная заявка рассматривается в порядке очереди, однако, очевидно, что некоторые заявки

являются более срочными, так как некоторые инциденты непосредственно влияют на ход рабочего процесса, в то время как другие могут быть устранены в течении более длительного срока без нарушения рабочего процесса.

4. Отсутствие системы оповещения о решении инцидента. Пользователь не получает информации о том, что инцидент решен, до тех пор, пока самостоятельно заново не зайдут на страницу со списком инцидентов. Это приводит к тому, что пользователь все еще ожидает решения инцидента в то время, когда сотрудник ИТ-отдела уже выполнил все работы.

Следует отметить, что, ввиду достаточно короткого срока апробации, не все функции и механизмы открытой информационной системы управления ИТ-инцидентами были задействованы в полной мере. Например, практически не был задействован контроль эффективности работы сотрудников ИТ-отдела путем анализа планирования дня и контроля статистики назначенных, не решенных и выполненных инцидентов. В целом же, внедренная система может являться источником разнообразной управленческой информации о доступности, эффективности, уровне подготовленности персонала, степени загруженности службы и т.д. Данная информация с помощью встроенных средств оформляется в виде структурированных отчетов, что для эффективной работы должно производиться на регулярной основе. Такие отчеты могут быть применены в качестве основы для детального и глубокого анализа возникающих проблем, выявления их причин, а также для определения необходимости внесения изменений в системы.

4.2 Оценка целевой и экономической эффективности применения программного инструментария

Эффективность работы системы управления инцидентами можно оценивать с точки зрения различных параметров:

- технические параметры;
- экономическая эффективность;

- степень удовлетворенности пользователей работой службы поддержки.

Для оценки производительности процесса технической поддержки университета необходимо четко определить контрольные параметры и показатели эффективности.

Таковыми параметрами могут быть:

- общее количество инцидентов;
- количество «потерянных» (незарегистрированных и нерешенных) инцидентов;
- среднее время закрытия инцидентов;
- количество решенных инцидентов на одно рабочее место или на одного ИТ-сотрудника;
- инциденты, решенные без посещения пользователя (удаленно).

В таблице 4.2 приведена оценка вышеуказанных показателей за период два месяца до внедрения открытой информационной системы управления ИТ-инцидентами и за аналогичный период после внедрения системы.

Таблица 4.2 – Оценка показателей производительности процесса технической поддержки

Наименование показателя	Значение показателя		Изменение показателя	
	до внедрения системы	после внедрения системы	абсолютное	относительное, %
Общее количество инцидентов	167	186	19	11
Количество «потерянных» (незарегистрированных и нерешенных) инцидентов	26	0	-26	-100
Среднее время закрытия инцидентов, мин.	45	32	-13	-29
Количество решенных инцидентов на одно рабочее место или на одного ИТ-сотрудника	17	19	2	12
Инциденты, решенные без посещения пользователя (удаленно)	32	58	26	81

Отметим, что поскольку до внедрения открытой информационной

системы управления ИТ-инцидентами учет инцидентов велся не в полном объеме, некоторые показатели имеют приблизительное значение

Из таблицы 4.2 следует, что внедрение открытой информационной системы управления ИТ-инцидентами, прежде всего, исключило возможность «утери» обращения, за счет автоматической регистрации каждого инцидента в системе. Увеличение числа инцидентов может быть связано с двумя причинами:

- отсутствие «потерянных» обращений;
- упрощение обращения в службу поддержки стимулирует пользователей обращаться к ИТ-специалистам, вместо того, чтобы тратить время на решение проблемы самим либо работать в условиях неоптимальной работы компьютерной техники (примером таких случаев являются обращения с жалобами на «зависающий», либо медленно работающий компьютер).

Отметим, что время закрытия инцидентов сократилось, прежде всего, за счет моментального отображения их в системе, а, следовательно, появилась возможность для специалистов поддержки быстро увидеть и отреагировать на проблему.

Увеличение числа инцидентов, решенных без участия пользователей, связано с уже упоминаемыми ранее простыми техническими проблемами. Специалисты службы поддержки, имея достаточно полное описание инцидента, часть из них решают в телефонном режиме, помогая пользователю либо лаборанту решить возникшую проблему.

Что касается экономической эффективности внедрения открытой информационной системы управления ИТ-инцидентами, то она может быть оценена по следующим параметрам:

- средняя стоимость поддержки на инцидент;
- эффективное время работы сотрудников ИТ-отдела;
- сокращения времени простоя сотрудников (пользователей) в связи с техническими неполадками.

Эффективное время работы сотрудников службы поддержки увеличилось после внедрения открытой информационной системы управления ИТ-инцидентами за счет сокращения затрат на регистрацию инцидентов и их обработку (сбор инцидентов из трех различных источников обращений, приведенных ранее), а также за счет сокращения времени на уточнение деталей по ним.

Расчет и анализ проведенных показателей экономической эффективности приведен в таблице 4.3.

Таблица 4.3 – Показатели экономической эффективности внедрения открытой системы управления ИТ-инцидентами

Наименование показателя	Формула	Значение
1	2	3
Средняя зарплата специалиста ИТ-отдела, руб.	-	38000
Количество сотрудников ИТ-отдела, чел.	-	5
Стоимость часа работы специалиста ИТ-отдела, руб.	Средняя зарплата специалиста ИТ-отдела / Месячный фонд рабочего времени на одного человека	190
Средняя стоимость поддержки на инцидент до внедрения системы	Среднее время закрытия инцидента до внедрения * Стоимость часа работы специалиста ИТ-отдела	142,5
Средняя стоимость поддержки на инцидент после внедрения системы	Среднее время закрытия инцидента до внедрения * Стоимость часа работы специалиста ИТ-отдела	101,3
Увеличение эффективного времени работы сотрудников ИТ-отдела, часов в месяц на одного сотрудника	-	12
Сокращение времени простоя сотрудников (пользователей) в связи с техническими неполадками, всего в месяц	-	34
Средняя стоимость часа простоя сотрудников (пользователей), руб.	-	480
Экономия за счет сокращения стоимости поддержки на инцидент, руб.	К-во инцидентов в месяц * Снижение средней стоимости поддержки на инцидент	3831,6
Экономия за счет увеличения эффективного времени работы сотрудников ИТ-отдела, руб.	Стоимость часа работы специалиста ИТ-отдела * Увеличение эффективного времени работы сотрудников ИТ-отдела * Количество сотрудников	11400
Экономия за счет сокращения времени простоя сотрудников (пользователей) в связи с техническими неполадками, руб.	Сокращение времени простоя сотрудников (пользователей) в связи с техническими неполадками * Средняя стоимость часа простоя сотрудников (пользователей)	16320

Продолжение таблицы 4.3

1	2	3
Суммарная экономия от внедрения информационной системы	Экономия за счет сокращения стоимости поддержки на инцидент + Экономия за счет увеличения эффективного времени работы сотрудников ИТ-отдела + Экономия за счет сокращения времени простоя сотрудников (пользователей) в связи с техническими неполадками	31551,6

Средняя стоимость часа простоя сотрудников (пользователей) определена эмпирически, исходя из средней зарплаты преподавателей и научных работников, а также примерной стоимости обучения студентов в вузе.

Таким образом, даже на первоначальном этапе внедрения открытой информационной системы управления ИТ-инцидентами экономический эффект составил 31551,6 рублей в месяц. Дальнейшее развитие и совершенствование работы системы может еще более повысить показатели экономической эффективности от ее внедрения.

Оценка степени удовлетворенности пользователей работой службы поддержки может быть произведена путем опроса пользователей. Для этого был определен список параметров и с помощью группы экспертов из числа пользователей определен вес каждого параметра. Пользователям было предложено заполнить анкету из пяти вопросов.

1. Оцените, насколько легко обратиться (зафиксировать заявку) в службу поддержки (по шкале от 1 – очень сложно, до 5 – очень просто).

2. Оцените, насколько быстро ИТ-служба реагирует на заявки (по шкале от 1 – очень долго, до 5 – очень быстро).

3. Оцените, насколько часто Ваша заявка остается без ответа (по шкале от 1 – очень часто, до 5 – никогда).

4. Оцените, насколько часто Вам приходится повторно обращаться в ИТ-службу с одной той же проблемой (по шкале от 1 – очень часто, до 5 – никогда).

5. Оцените, насколько быстро решаются возникающие инциденты (по шкале от 1 – очень долго, до 5 – очень быстро).

Вопросы и шкала для их оценки сформированы таким образом, что рост

общей суммы баллов соответствует росту показателя удовлетворенности пользователей работой службы поддержки

Среднее значение параметров, полученное при заполнении анкет 108 пользователями до и после внедрения открытой информационной системы управления ИТ-инцидентами, а также интегральная оценка степени удовлетворенности пользователей работой службы поддержки, приведены в таблице 4.4

Таблица 4.4 – Интегральная оценка степени удовлетворенности пользователей

Номер вопроса	Среднее значение		Вес показателя	Итоговый балл	
	до внедрения системы	после внедрения системы		до внедрения системы	после внедрения системы
1	3,6	4,8	3	10,8	14,4
2	2,9	3,9	4	11,6	15,6
3	4,2	4,9	5	21	24,5
4	4,0	4,7	4	16	18,8
5	4,0	4,6	4	16	18,4
Общая сумма баллов				75,4	91,7

Таблица 4.4 позволяет сделать вывод, что интегральный показатель удовлетворенности пользователей работой службы поддержки вырос на 16,3 балла или на 21,6%.

Таким образом, можно сделать вывод об эффективности проведенного в рамках апробации программного проекта внедрения открытой информационной системы управления ИТ-инцидентами на базе Волжского университета имени В.Н. Татищева (г. Тольятти).

4.3 Проблемы и перспективы развития программного инструментария

Апробация работы разработанной системы управления инцидентами продемонстрировала эффективность применения данного программного инструментария для построения информационных систем, однако, вместе с тем, выявила и некоторые проблемы и «узкие места» в работе системы, нуждающиеся в дальнейшей доработке. Однако, рассматривая возникшие в

ходе апробации нюансы работы следует учитывать, что в ходе проектирования и разработки ставилась задача по созданию универсальной системы для реализации функционала открытой информационной системы управления ИТ-инцидентами для любого предприятия или ИТ-отдела. А, следовательно, и решения не должны отражать специфику работы одного учреждения, а должны обеспечивать достаточно гибкие настройки для реализации различных задач.

Рассмотрим основные перспективные направления развития и усовершенствования разработанного программного продукта.

1. Реализация системы определения приоритета инцидентов. Инциденты, возникающие в процессе работы организации могут иметь разную степень приоритетности в зависимости от того, насколько критичным является инцидент для бесперебойной работы организации. Соответственно, более критичные инциденты должны быть отработаны службой поддержки в первую очередь. Таким образом, реализация системы определения приоритета инцидентов может значительно повысить эффективность работы службы технической поддержки пользователей.

2. Возможность классификации инцидентов. Классификация инцидентов облегчает процесс идентификации и распределение инцидентов между исполнителями. Также, в зависимости от структуры ИТ-службы, в организации может быть распределена ответственность за решение определенных типов инцидентов между сотрудниками (т.е., решение определенных типов инцидентов может быть однозначно зафиксировано за конкретными сотрудниками либо группой исполнителей). В этом случае также возможна реализация функции автоматического назначения исполнителей для решения инцидентов. Однако, следует учитывать, что и классификация инцидентов, и определение типов приоритетов сильно зависят от специфики работы организации, соответственно, данные функциональные возможности не должны быть жестко унифицированы. Возможность гибкой настройки данных параметров должна быть реализована при настройке и формировании открытой

информационной системы управления ИТ-инцидентами.

3. Ведение Базы знаний. Решение типовых инцидентов может быть ускорено за счет фиксации способов решения в Базе знаний. При правильной организации таковой, часть инцидентов может быть решена путем автоматической отправки пользователю инструкций по решению инцидента.

4. Аналитический учет частоты типовых инцидентов. Данный пункт является своеобразным «расширением» пунктов 2 и 3. Анализ частоты и периодичности возникновения определенных типов инцидентов может стать основой для превентивных действий, позволяющих выявить и локализовать проблемные ситуации до возникновения инцидента.

5. Усовершенствование интерфейса системы. Для более комфортной работы с информационной системой следует добавить такие элементы:

5.1 Поле «Заголовок» для инцидента;

5.2 Механизмы оповещения (как для пользователя – о решении открытого им инцидента, так и для ИТ-отдела – о регистрации нового инцидента). Механизм оповещения может быть реализован визуальным сигналом (например, мигающий символ во вкладке браузера), звуковым сигналом, а также возможно оповещение по электронной почте.

6. Реализация возможности многоуровневой системы поддержки. Для крупных организаций в условиях большого количества и разнообразия возникающих инцидентов может быть полезна возможность реализации нескольких уровней исполнителей в системе. Например, все инциденты видит только диспетчер, они распределяются им между исполнителями, а эскалация на следующий уровень (запрос к специалистам более высокой квалификации) происходит только в случае невозможности решения инцидента на данном уровне.

Таким образом, разработанный программный инструмент для построения информационной системы управления инцидентами в сфере информационных технологий хотя и реализует все необходимые для

управления ИТ-инцидентами функции, однако имеет достаточно широкие возможности для совершенствования и развития.

ЗАКЛЮЧЕНИЕ

В процессе работы над выпускной квалификационной работе в виде магистерской диссертации был проведен анализ литературы, имеющей отношение к открытым информационным системам и управлению ИТ-инцидентами. По итогам анализа научной литературы было установлено, что применение технологии открытых информационных систем в процессе управления ИТ-инцидентами имеет определенные перспективы. Также в процессе анализа был сделан вывод о том, что до сих пор учеными-информатиками не проводились серьезные исследования в области методов и подходов построения открытых информационных систем управления ИТ-инцидентами. Более того, не проводилась оценка экономической эффективности применения упомянутых подходов.

Для достижения поставленной цели исследования (внедрение открытой информационной системы в процесс управления ИТ-инцидентами для обеспечения интероперабельности и мобильности программных приложений, персонала и данных) были решены все поставленные задачи, а именно:

1. На основе проведенного исследования научной, нормативно-справочной и методической литературы был определен алгоритм разработки открытых информационных систем для управления ИТ-инцидентами.

2. Проведен анализ бизнес-процесса управления ИТ-инцидентами.

3. Исследован вопрос существования программных инструментариев, пригодных для реализации открытых систем управления ИТ-инцидентами.

4. Выявлены требования к открытым информационным системам управления ИТ-инцидентами.

5. Реализованы инструменты и алгоритмы построения открытых информационных систем управления ИТ-инцидентами.

6. Проанализирована целевая эффективность использования реализованных инструментов и алгоритмов на примере ИТ-отдела – отдела

информатизации и автоматизации учебного процесса учебно-методического управления ВУиТ (Волжского университета имени В.Н. Татищева, г. Тольятти).

Таким образом, можно сделать вывод о том, что цель исследования была достигнута.

Была эмпирически подтверждена гипотеза о том, что внедрение открытой информационной системы в процесс управления ИТ-инцидентами позволит обеспечить интероперабельность и мобильность программных приложений, персонала и данных.

Основной научный результат магистерской диссертации заключается в том, что реализованный в ходе исследования программный инструментарий даст возможность широкому кругу конечных пользователей построить собственную открытую информационную систему управления ИТ-инцидентами в соответствии с необходимыми потребностями. Применение такой системы дает следующие преимущества:

- отсутствие «потерянных» инцидентов;
- более быстрое и более эффективное разрешение возникающих инцидентов, снижающее затраты на материальные активы и сокращающее расходы на поддержание ИТ-инфраструктуры;
- уменьшение времени простоя пользователей;
- уменьшение трудозатрат ИТ-персонала;
- возможность быстрого получения различного рода статистических отчетов;
- возможность контроля за процессом управления ИТ-инцидентами;
- возможность интеграции с другими информационными системами организации (предприятия, учреждения, сообщества);
- возможность сбора обратной связи от пользователя для улучшения качества обслуживания.

Кроме того, определенным научным успехом можно считать тот факт, что впервые были успешно применены концепции, технологии и среда

открытых информационных систем при построении открытой информационной системы управления ИТ-инцидентами. Результаты настоящего исследования могут послужить опорой для дальнейших научных разработок в данной области.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. ГОСТ Р ИСО/МЭК ТО 10000-2-99 Информационная технология (ИТ). Основы и таксономия международных функциональных стандартов. Часть 2. Принципы и таксономия профилей взаимосвязи открытых систем (дата введения 1 июля 2000 года). [Электронный ресурс]: электронный фонд правовой и нормативно-технической документации: <http://docs.cntd.ru/document/1200027469>

2. ГОСТ Р ИСО/МЭК ТО 10000-3-99 Информационная технология (ИТ). Основы и таксономия международных функциональных стандартов. Часть 3. Принципы и таксономия профилей среды открытых систем (дата введения 1 июля 2000 года). [Электронный ресурс]: электронный фонд правовой и нормативно-технической документации: <http://docs.cntd.ru/document/1200027470>

3. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств (дата введения 1 марта 2012 года). [Электронный ресурс]: электронный фонд правовой и нормативно-технической документации: <http://docs.cntd.ru/document/gost-r-iso-mek-12207-2010>

4. ГОСТ 7.82-2001. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления. – введ. 2002-07-01. – Минск: Издательство стандартов, 2001. – 35 с. – (Система стандартов по информации, библиотечному и издательскому делу).

Научная и методическая литература

5. Бачило И.Л. Актуальные проблемы информационного права (для магистров): учебник / И.Л. Бачило, М.А. Лапина – М.: Юстиция, 2016. – 532 с.

6. Бирюков А.Н. Процессы управления информационными технологиями: курс лекций / А.Н. Бирюков. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 264 с.

7. Буянский С.Г. Корпоративное управление, комплаенс и риск-менеджмент: учебное пособие / С.Г. Буянский, Ю.В. Трунцевский – М.: Русайнс, 2016. – 342 с.
8. Варфоломеева, А.О. Информационные системы предприятия: учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. – М.: НИЦ Инфра-М, 2013. – 283 с.
9. Гухман В.Б. Философия информации: курс лекций / В.Б. Гухман. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 249 с.
10. Данилин А.В. Архитектура предприятия: курс лекций / А.В. Данилин, А.И. Слюсаренко. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 450 с.
11. Кияев В.И. Информатизация предприятия: курс лекций / В.И. Кияев, О.Н. Граничин. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 235 с.
12. Кияев В.И. Информационные технологии в управлении предприятием: курс лекций / В.И. Кияев, О.Н. Граничин. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 506 с.
13. Кияев В.И. Открытые системы и интеллектуальная собственность в ИТ: курс лекций / В.И. Кияев, О.Н. Граничин. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 153 с.
14. Коноплева И.А. Информационные технологии. 2-е издание. Учебное пособие: учебное пособие / И.А. Коноплева, О.А. Хохлова, А.В. Денисов. – М.: Проспект, 2014. – 328 с.
15. Парамонов Ф.И., Колесниченко О.В. Основы проектирования АСУП: Учебное пособие. – М.: Изд-во МАИ, 2015. – 92 с.
16. Чистов, Д.В. Проектирование информационных систем. Учебник и практикум / Д.В. Чистов, П.П. Мельников, А.В. Золотарюк, Н.Б. Ничепорук. – М.: Юрайт, 2016. – 260 с.

17. Черняк В.З. Принципы управления инновационными рисками на разных стадиях проекта: монография / В.З. Черняк – М.: Русайнс, 2016. – 202 с.

Электронные ресурсы

18. Agarwal H. Managing the demand for IT infrastructure, 2014 // McKinsey&Company [Электронный ресурс]: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/managing-the-demand-for-it-infrastructure>

19. Baaziz A. Patents used by NPE as an Open Information System in Web 2.0, 2014 // A. Baaziz, L. Quoniam [Электронный ресурс]: сайт Публичного Хранилища Знаний: <https://ojs.hh.se/index.php/JISIB/article/view/97>

20. Chaudhary P. Sensing Attributes of an Agile Information System. 2013 // P. Chaudhary, M. Hyde, A. Ramaprasad [Электронный ресурс]: сайт, предоставляющий открытый доступ к научным журналам: <http://www.scirp.org/journal/PaperInformation.aspx?PaperID=37192>

21. Chaudhary P. Exploring the Benefits of an Agile Information System, 2017 // P. Chaudhary, M. Hyde, J.A. Rodger [Электронный ресурс]: сайт, предоставляющий открытый доступ к научным журналам: <http://www.scirp.org/journal/PaperInformation.aspx?PaperID=78662>

22. Fisher C. New Techniques in Project Management, 2014 // C. Fisher [Электронный ресурс]: сайт, предоставляющий открытый доступ к научным журналам: <http://www.scirp.org/journal/PaperInformation.aspx?PaperID=52183>

23. Henze F. Concepts and Technologies for a Comprehensive Information System for Historical Research and Heritage Documentation, 2013 // The SAO/NASA Astrophysics Data System [Электронный ресурс]: сайт, содержащий научные статьи об исследованиях в области физики и астрономии: <http://adsabs.harvard.edu/abs/2013ISPAr.XL5b.325H>

24. Iakovidis D.K. Open-Access Framework for Efficient Object-Oriented Development of Video Analysis Software, 2014 // D.K. Iakovidis, D. Diamantis [Электронный ресурс]: сайт, предоставляющий открытый доступ к научным журналам: <http://www.scirp.org/journal/PaperInformation.aspx?PaperID=48124>

25. Tsolakidis A. Institutional Research Management using an Integrated Information System, 2013 // A. Tsolakidis, C. Sgouropoulou, E. Papageorgiou, O. Terraz, G. Miaoulis [Электронный ресурс]: сайт, предоставляющий преимущественно платный доступ к научным публикациям: <http://www.sciencedirect.com/science/article/pii/S1877042813003789>

26. Vukšić V.B. Social Business Process Management: Croatian IT Company Case Study, 2017 // V.B. Vukšić, D.S. Vugec, A. Lovrić [Электронный ресурс]: сайт немецкого научного издательства, специализирующегося на издании академической литературы: <https://www.degruyter.com/view/j/bsrj.2017.8.issue-1/bsrj-2017-0006/bsrj-2017-0006.xml>

27. Минакова Н.Н., Петров И.В. Открытая информационная система для минимизации ошибок доступа при идентификации личности по радужной оболочке глаза, 2015 // Научный журнал «Известия Алтайского государственного университета» [Электронный ресурс]: <http://izvestia.asu.ru/ru/article/547/>

28. Митина О.А. Информационные системы поддержки принятия управленческих решений крупных предприятий, 2015 // Альманах современной науки и образования [Электронный ресурс]: научная электронная библиотека eLIBRARY.ru: <https://elibrary.ru/item.asp?id=24918315>

Литература на иностранном языке

29. Afsarmanesh H. Collaboration in a Hyperconnected World – IFIP Press, 2016.

30. Bailis, P. Readings in Database Systems – 5th edition, MIT Press, 2015.

31. Bourgeois D. Information systems for business and beyond – The Saylor Foundation's Open Textbook Challenge, 2014.

32. Esposito, D. Architecting Applications for the Enterprise – 2nd edition, Microsoft Press, 2014.

33. Haridi, S. Concepts, Techniques, and Models of Computer Programming – 3rd edition, MIT Press, 2014.

34. Kalloniatis C. Innovative Information Systems Modelling Techniques – InTech Press, 2016.

35. McKean D. Excellent IT Management – CreateSpace Independent Publishing Platform, 2014.