НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»

Институт Информационных технологий

Направление подготовки 09.03.02 Информационные системы и технологии
(шифр и наименование)

Департамент Цифровой экономики
(аббревиатура)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ работа

На тему: Внедрение средства управления ITSM для ПАО «Московский Кредитный Банк»

Обучающийся _____
(ФИО полностью) (подпись)

Руководитель _____ _____
(ФИО полностью) (подпись)

Директор Департамента _____ _____
(ФИО полностью) (подпись)

МОСКВА 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....6

I АНАЛИТИЧЕСКАЯ ЧАСТЬ.....9

1.1. Технико-экономическая характеристика предметной области банка. Анализ деятельности «КАК ЕСТЬ».....9

1.1.1. Характеристика банка и его деятельности.....9

1.1.2. Организационная структура управления банка.....11

1.2. Анализ деятельности ПАО «Московский кредитный банк».....16

1.2.1. SWOT-анализ ПАО «Московский кредитный Банк».....17

1.2.2. Стратегия внедрения ITSM в ПАО «Московский кредитный банк».....19

1.2.3. Способ приобретения ИС для внедрения ITSM в ПАО «Московский кредитный банк».....21

1.3. Обоснование проектных решений.....23

1.3.1. Обоснование проектных решений по информационному обеспечению.....23

1.3.2. Обоснование проектных решений по программному обеспечению.....26

1.3.3. Обоснование проектных решений по техническому обеспечению.....27

II ПРОЕКТНАЯ ЧАСТЬ.....29

2.1. Понятие и сущность ITSM.....29

2.1.1. Ошибки на этапах внедрения ITSM и их описание.....37

2.1.2. Организационно-правовые и программно-аппаратные средства обеспечения информационной безопасности и защиты информации.....41

2.2. Описание существующих ITSM-систем управления IT сервисов.....48

2.3. Этапы внедрения ITSM.....52

2.4. «OMNITRACKER ITSM Center» как оптимальный программный продукт для внедрения в организацию.....62

III ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА.....71

ЗАКЛЮЧЕНИЕ.....73

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....75

ВВЕДЕНИЕ

В условиях современного мира банки чрезвычайно зависимая от информационных технологий (ИТ) структура. Абсолютное большинство банковских услуг использует ИТ в той или иной форме. Происходит расширение ИТ- сервиса за счёт внедрения клиентских услуг на базе информационных решений и в первую очередь, систем дистанционного банковского обслуживания.

Для покрытия бизнес-потребностей в том числе и банков широко используют систему управления ИТ-сервисом — ITSM (Information Technology Service Management). Основой идеологической составляющей данной системы является сочетаний процессов, технологий и людей.

Постоянно возрастает влияние ИТ-деятельности на бизнес-процессы в банках, их управление и контроль, повышение безопасности операций и, как следствие в целом, имидж финансовой организации. Поэтому совершенствование и развитие системы управления IT-сервисом в банковской сфере является весьма актуальной задачей.

Предпосылок для начала внедрения ITSM, в ПАО «Московский кредитный Банк», было несколько. Прежде всего в банке планировался запуск ряда крупных ИТ-проектов, и это требовало адекватных методик поддержки внедрения и последующего обслуживания, что, конечно же, предполагает непосредственное участие департамента ИТ. Данное подразделение по численности является одним из крупных среди аналогичных коммерческих структур, а профессиональная квалификация большинства его сотрудников не вызывает у руководства сомнений. Качество работы этого коллектива в целом, по словам его руководителей, во многом зависит от того, как эта работа организована, каким образом она отслеживается и как анализируются ее результаты.

Приоритетными направлениями в управлении ИТ в банке, являются поддержка критично важных для него бизнес-процессов, обеспечиваемых средствами ИТ; оптимизация и повышение эффективности банковской ИТ-

инфраструктуры; разумные инвестиции в технологии и решения, непосредственно ориентированные на получение прибыли от клиентов и развитие бизнеса в среднесрочной перспективе.

Именно проблема организации работы ИТ-департаментов в контексте деятельности всего банка как правило, выходит на первый план в ходе стратегических проектов автоматизации в большинстве крупных российских банков. Подобные организации часто оснащены внушительными по размерам отделами ИТ с высоким уровнем профессиональной подготовки специалистов. Повседневные и отработанные на долгом практическом опыте задачи решаются вполне удовлетворительно. В то же время при попытке развернуть полномасштабное взаимодействие ИТ-подразделения с ключевыми департаментами, отвечающими за развитие бизнеса, в ходе решения комплексных вопросов автоматизации, как правило, возникают проблемы.

Тактику управления ИТ в ПАО «Московский кредитный Банк» можно описать так:

- сокращение (часто — до нуля) капитальных затрат на ИТ;
- сохранение информатизации и автоматизации основной деятельности;
- оптимизация операционных затрат;
- поддержка приоритетных видов банковских работ на базе имеющейся инфраструктуры и базовых средств автоматизации;
- обеспечение соответствия внешним требованиям (таким, как закон о персональных данных).

В целом роль ИТ в деятельности банка трудно переоценить. Тесную и постоянную связь с ИТ-департаментом поддерживают практически все бизнес-подразделения организации, а с развитием Интернет-технологий даже сторонние предприятия в принципе могут оказаться вовлеченными в непосредственное взаимодействие с ним. Уровень, стабильность и качество сервиса, предоставляемого ИТ-подразделением банка, — это в определенной степени ключевой фактор в деятельности ПАО «Московский кредитный Банк» в целом. Поэтому для повышения эффективности использования ресурсов подразделений ИТ

руководством банка было принято решение взять на вооружение методологию ITSM.

Цель данной работы: провести исследование, на что повлияло внедрение средства управления ITSM в ПАО «Московский кредитный банк».

Задачами выпускной квалификационной работы являются:

- Провести организационно-экономический анализ деятельности ПАО «Московский кредитный Банк».
- Проанализировать степень эффективности внедрения.
- Произвести описание существующих средств управления ITSM.
- Привести организационно-экономическое обоснование внедрения ITSM.

Объектом исследования заданной темы являются информационные технологии по обслуживанию клиентов банка.

Предметами исследования данной темы, являются современные пути удовлетворение потребностей бизнеса и поддержки ИТ-инфраструктуры коммерческого банка.

I АНАЛИТИЧЕСКАЯ ЧАСТЬ

1.1. Технико-экономическая характеристика предметной области Банка. Анализ деятельности «КАК ЕСТЬ»

1.1.1. Характеристика Банка и его деятельности

Публичное акционерное общество «Московский кредитный банк» — крупнейший негосударственный публичный банк в России, осуществляющий коммерческую деятельность в 22 регионах Центрального, Приволжского, Северо-Западного и Уральского федеральных округов. Включён Банком России в перечень системно значимых кредитных организаций. Головной офис расположен в городе Москве [1].

Акционерное общество открытого типа «АКБ «Московский кредитный банк» было создано в 1992 году по инициативе и на средства московского предпринимателя Бориса Борисова. В число первоначальных учредителей вошла группа частных предприятий (ЧМП «Ост», ЧМП «Пеленг», ЧМП «Эллипс» и другие, представлявшие собой группу аффилированных лиц) и товарно-сырьевая биржа «Потенциал России» (ныне не существует). Б. А. Борисов возглавил совет директоров банка [2]. Правление банка возглавил соучредитель банка В. А. Кухтаров. 19 августа 1992 года банком была получена лицензия на осуществление банковских операций № 1978, 2 декабря 1993 года получена лицензия на осуществление банковских операций в иностранной валюте [3].

В 1994 году произошло расширение состава учредителей и уже в том же году был приобретен структурами Романа Авдеева. В 1995 году банк сменил организационно правовую форму, став называться Общество с ограниченной ответственностью «Коммерческий банк «Московский кредитный банк». В 1995 году правление банка возглавил Валерий Комаровский. В 1995 году банк вошёл в сотню крупнейших банков России [3].

В 2000 году правление банка возглавил Андрей Донских, которого в 2004 году сменил Александр Хрилев, проработавший в банке до конца 2008 года. С 2008 по 31 января 2012 года правление возглавлял Александр Николашин,

работающий в банке с 1994 года. С 1 февраля 2012 года Александр Николашин занял пост президента банка. Председателем правления с того же дня был назначен Владимир Чубарь [3].

В 2016 году МКБ приобрел СКС Банк для развития направления инвестиционного банкинга.

Летом 2017 года МКБ наряду с «Бинбанком», «Промсвязьбанком» и ФК «Открытие» упоминался в письме УК «Альфа-Капитал». Позже УК «Альфа-Капитал» полностью дезавуировала заявления своего работника. В компании пояснили, что это было частное мнение одного из сотрудников, которое не отражает позицию «Альфа-Капитала».

Банк 13 сентября 2017 года включён в список системно значимых кредитных учреждений, составленный ЦБ РФ Помимо МКБ в перечень входит еще 10 банков, среди которых «Юникредит банк», «Газпромбанк», ВТБ, «Альфа-банк», «Сбербанк», «ФК Открытие», «Росбанк», «Промсвязьбанк», «Райффайзенбанк» и «Россельхозбанк». На их долю приходится более 60 % совокупных активов российского банковского сектора.

В июне 2018 года АКБ МКБ продал 100 % акций своей дочерней компании «МКБ-Лизинг» за 1,55 млрд руб. Согласно отчету, после выбытия дочерней группы банк лишился 703 млн руб., а чистый приток средств к получению составил 1 236 млн руб. Признанная МКБ прибыль от продажи дочерней компании составила 637 млн руб.

В феврале 2019 года Московский кредитный банк (МКБ) подал в ФАС РФ ходатайство о покупке 99,9 % акций Азиатско-Тихоокеанского банка (АТБ).

В 2019 года МКБ запустил новую платформу по выдаче кредитов, которая является универсальной, и клиент может сам подобрать для себя срок размещения вклада.

В результате кредитных обязательств 3 апреля 2019, через банкротство, банку перешла детская торговая сеть «Бегемот».

МКБ 18 мая 2020 года приобрел у группы компаний «Регион» банки «Веста» и Руснарбанк. Стоимость покупки «Весты» составила 1,08 млрд руб., а Руснарбанка — 2,97 млрд руб.

В марте 2021 года у УГМК был приобретён банк «Кольцо Урала», интеграция которого в структуру МКБ началась 31 мая.

В мае 2021 года МКБ объявил о размещении допэмиссии 3,6 млрд акций по цене 6,3 руб. Половину выпуска намерен купить «Россиум». Общая сумма привлекаемых дополнительных средств — 22,7 млрд руб.

В первом квартале 2022 года МКБ продал Руснарбанк 11 физическим лицам, доля каждого из которых в приобретенном банке составила 9,1 %

1.1.2. Организационная структура управления банка

Организационно правовая форма — Публичное акционерное общество (ПАО) в России — форма организации акционерного общества, при которой его акционеры пользуются правом отчуждать свои акции без необходимости согласования с другими акционерами [4].

Организация и деятельность публичных акционерных обществ регулируется федеральным законом Российской Федерации. Поскольку открытое акционерное общество рассматривается законодателем как публичное, для него предусматривается обязанность по раскрытию информации в более широком формате по сравнению с непубличным акционерным обществом. Данная норма предназначена для повышения публичности и прозрачности процессов инвестирования.

Особенности ПАО:

- неограниченное число акционеров;
- свободное обращение акций на рынке;
- отсутствие необходимости внесения денежных средств в уставный капитал предприятия до его регистрации и открытия накопительного счёта.

По виду деятельности ПАО «Московский кредитный Банк» является коммерческой организацией, цель которого — получение коммерческой прибыли [5].

Структура управления банком — многолинейная (штабная) структура, при данной структуре управления, можно отдавать распоряжения напрямую любым нижестоящим инстанциям. В результате каждое нижестоящее подразделение получает распоряжения не от одной, а от многих вышестоящих инстанций, перед которыми несет ответственность за их выполнение. Схема структуры управления (рис. 1.1).



Рис. 1.1. Схема организационной структуры управления ПАО «Московский кредитный банк»

Председатель правления банка:

- представляет банк;
- исполняет решения высшего органа управления банка, заботится об их проведении в жизнь;

- поддерживает инициативу работников банка и вносит предложения по совершенствованию деятельности банка;
- организует и руководит трудовым коллективом банка; -отвечает за законность работы банка перед органом управления банка.

Контрольный орган банка должен контролировать деятельность банка через исполнительные органы, директора банка, кредитные и другие специальные службы и представлять самостоятельный отчет и свои предложения по дальнейшему совершенствованию деятельности КБ.

Исполнительные органы банка при выполнении своих функций (реализации всех решений органов управления непосредственно в текущей деятельности банка) опираются на конкретную организационную структуру банка.

Собрание акционеров (пайщиков) созываются ежегодно, не позднее чем через месяц после составления баланса банка за отчетный год. Чрезвычайные собрания акционеров могут созываться по решению совета банка, требованию ревизионной комиссии или акционеров, владеющих не менее чем 1/3–1/10 акционерного капитала [6].

Собрание акционеров (пайщиков):

- вносит изменения и дополнения в устав банка;
- принимает решения о дополнительном выпуске акций и увеличении уставного капитала;
- избирает совет и ревизионную комиссию банка;
- рассматривает и утверждает баланс банка, отчет о прибылях и убытках за истекший операционный год, заключение и отчет ревизионной комиссии;
- устанавливает порядок распределения прибыли банка, порядок образования и использования фондов банка;
- принимает решение о прекращении деятельности банка;
- заключает договоры от имени банка о трудовых отношениях с членами совета банка;

- рассматривает другие вопросы, вынесенные на собрание по решению совета, ревизионной комиссии банка или акционеров, обладающих не менее чем 1/10 акционерного капитала.

Для общего руководства работой банка, а также наблюдения и контроля за работой правления и ревизионной комиссии банка собрание акционеров избирает совет банка(правление) обычно со сроком полномочий до 5 лет. Количество членов совета банка определяется общим собранием акционеров.

Члены совета из своего состава большинством голосов выбирают председателя совета банка и его заместителей. Члены совета банка не могут быть одновременно членами правления или членами ревизионной комиссии банка.

Совет банка решает стратегические задачи управления и развития деятельности банка, его заседания проводятся не реже одного раза в год. В своей работе совет руководствуется действующим законодательством и нормативными актами [7].

Совет банка:

- определяет направление деловой политики банка, расширение масштаба и круга операций в зависимости от определенных экономических условий, размеры процентных ставок и дивидендов;
- устанавливает в соответствии с действующим законодательством и интересами ликвидности и прибыльности структуру привлекаемых пассивов и их размещение, предел допустимой задолженности банка в стране и за границей;
- осуществляет контроль за работой правления и ревизионной комиссии банка;
- утверждает годовой баланс и распределение полученного дохода;
- внутрибанковские инструкции;
- решает вопрос об открытии филиалов и представительств банка;
- осуществляет контроль за выполнением проводимой банком кредитной и инвестиционной политики; -избирает председателя банка, его

заместителей, назначает других руководящих лиц в банке и его отделениях;

- утверждает постоянно действующие комитеты и избирает их членов.

Члены совета несут личную ответственность за нарушение законодательных актов, регулирующих деятельность банка; за убытки в результате принятия некомпетентных решений; за выполнение операций, не предусмотренных уставом банка.

Председатель правления банка осуществляет руководство текущей деятельностью в соответствии с уставом и практически реализует решения совета банка. Он является главой банка и отвечает за управление оперативной деятельностью. Его заместители возглавляют ведущие управления или отделы. Количество заместителей определяется объемом выполняемых операций и возможностями управления.

Совет утверждает членов правления банка, которое определяет на основе утвержденных направлений деловой политики банка ближайшие цели и условия привлечения и размещения кредитных ресурсов, разрабатывает план работы на текущий год, решает кадровые вопросы.

При совете (правлении) банка обычно создаются два комитета: кредитный и ревизионный. В функции кредитного комитета входят:

- разработка кредитной политики банка, структуры привлекаемых средств и их размещения;
- контроль за решением вопросов, относящихся к компетенции совета банка, не требующих постоянного внимания;
- разработка заключений по предоставлению наиболее крупных ссуд, ссуд, превышающих установленные лимиты, по уровню процентных ставок на отдельные виды кредитов;
- рассмотрение вопросов, связанных с инвестированием фондов, ведением трастовых операций;
- проведение различных исследований деятельности отдельных подразделений банка.

Ревизионный комитет (комиссия) выбирается общим собранием акционеров (пайщиков).

В состав ревизионного комитета не могут быть избраны члены совета (правления) банка, а также другие лица, занимающие какие-либо штатные должности в банке.

Ревизионный комитет из своего состава избирает председателя и его заместителя. Члены ревизионного комитета несут ответственность за выполнение возложенных на них обязанностей в порядке, определяемом действующим законодательством.

Ревизионный комитет проверяет соблюдение банком законодательных и других актов, регулирующих его деятельность; постановку банковского контроля; кредитные, расчетные, валютные и другие операции, проведенные банком в течении операционного года (сплошной проверкой или выборочно); состояние кассы и имущества. Ревизионный комитет представляет совету банка, собранию акционеров (пайщиков) и Центробанку отчет о проведенных ревизиях, сопровождаемый рекомендациями по устранению недостатков.

При необходимости функции комитетов могут быть расширены. Это зависит от объема и вида выполняемых банком активных и пассивных операций.

1.2. Анализ деятельности ПАО «Московский кредитный банк»

Московский кредитный банк — второй крупнейший негосударственный банк в России по размеру активов, который начал свои деятельность с 1992 г.

Банк работает с частными клиентами, крупными и средними компаниями, малым бизнесом и индивидуальными предпринимателями. Банк стремится создавать для них понятные и выгодные продукты, развивать удобные, надежные и безопасные цифровые каналы, предлагать комфортный и заботливый клиентский сервис.

В банке работают более 5,5 тысяч профессиональных сотрудников, количество клиентов на апрель 2023 г составляет 1,5 млн [8].

Частным клиентам банк предлагает следующие продукты:

- кредитование;
- страхование;
- программы рефинансирования;
- дебетовые и кредитные карты;
- платежи и переводы;
- размещение депозитов;
- налоговый сервис;
- услуги на рынке ценных бумаг;
- онлайн-сервисы для управления счетами;
- программы индивидуального обслуживания;

Юридическим лицам МКБ предлагает такие продукты:

- кредитование;
- эквайринг;
- размещение депозитов;
- зарплатные проекты;
- инкассация и самоинкассация;
- корпоративные и таможенные карты;
- хеджирование рисков;
- услуги на валютном рынке;
- услуги по обслуживанию ВЭД.

Финансовые данные организации за период январь 2021 г.–январь 2022 г. представлены в [9].

1.2.1. SWOT-анализ ПАО «Московский кредитный Банк»

SWOT-анализ — метод стратегического планирования, заключающийся в выявлении факторов внутренней и внешней среды организации и разделении их на четыре категории: Strengths (сильные стороны), Weaknesses (слабые стороны), Opportunities (возможности), Threats (угрозы).

Сильные (S) и слабые (W) стороны являются факторами внутренней среды объекта анализа, (то есть тем, на что сам объект способен повлиять); возможности (O) и угрозы (T) являются факторами внешней среды (то есть тем, что может повлиять на объект извне и при этом не контролируется объектом). Например, предприятие управляет собственным торговым ассортиментом — это фактор внутренней среды, но законы о торговле не подконтрольны предприятию — это фактор внешней среды [10].

SWOT-анализ обладает следующими достоинствами:

1. Определение силы и слабости бизнеса, выявление факторов роста и внешних угроз.

2. Простота проведения и эффективность для любых форм коммерческой деятельности. Экспресс-анализ может провести любой предприниматель или группа сотрудников без помощи профессионалов.

3. Выявление возможностей компании, которые влияют на работу с реальными проблемами бизнеса.

4. Определение связей между недостатками и сильными сторонам в разрезе возможностей роста с учетом внешних рисков. Это одна из главных задач, которую решает SWOT-анализ — найти рычаги воздействия на недостатки и стать лучше.

5. Не нужно собирать массивы информации для проведения расчетов. Довольно часто все данные уже под рукой, нужно их только систематизировать.

6. Проектирование перспектив компании, предприятия.

7. Количественный расчет факторов, вариантов эффективного развития с учетом всех реалий рынка. Сводный или смешанный алгоритм расчета позволяет глубоко проработать характеристики роста.

8. Оценка рентабельности проекта в существующих реалиях.

9. Укрепление конкурентных преимуществ, разведка ситуации на рынке.

10. Оценка внутреннего потенциала компании, ресурсов предприятия, определение возможных проблем и разработка мероприятий по их нивелированию.

11. Выявить угрозы, которые являются наиболее критичными в существующем положении, принять меры для эффективной защиты.

Проведем SWOT — анализ ПАО «Московский кредитный Банк», который поможет установить сильные и слабые стороны Банка, а также внешними угрозами и возможностями (табл. 1.1).

Таблица 1.1

SWOT-анализ ПАО «Московский кредитный Банк»

	Сильные стороны	**Слабые стороны**
Внутренние факторы	1. Относительно высокая стоимость фондирования. 2. Партнерство с другими банками (Юни кредит, Россгострах, Альфа банк). 3. Стратегия банка — постоянное расширение и ориентация на нужды и потребности клиентов. 4. Большой запас ликвидности активов банка).	1. Высокая конкуренция в сфере банковских услуг. 2. Нестабильность экономики РФ и санкции. 3. Недостаточные маркетинговые усилия по продвижению бренда. 4. Малое распространение офисов по РФ (Москва и М. о.)
	Возможности	**Угрозы**
Внешние факторы	1. Ухудшение позиций конкурентов. 2. Направление средств в маркетинг. 3. Распространение электронных платежей. 4. Распространение зарплатных проектов среди организаций региона. 5. Продвижение на рынок своих предложений по депозитам. 6. Улучшение инвестиционного климата в стране. 7. Снижение инфляции. 8. Рост уровня доходов населения.	1. Сложность возврата просроченных кредитов. 2. Нехватка качественных заемщиков. 3. Недоверие населения банкам. 4. Недостаточно сформированный рынок банковских услуг. 5. Нестабильность курса доллара и евро. 6. Попадание в санционные списки.

Проведя SWOT анализ, был сделан вывод, что необходимо расширять свою сеть офисов за пределы Москвы и Московской области. Также необходимо постоянно исследовать рынок банковских услуг, для получения конкурентных продуктов, также необходимо развивать собственные ИТ-отделы. Для развития ИТ отделов и был как раз внедрен ITSM [11].

1.2.2. Стратегия внедрения ITSM в ПАО «Московский кредитный банк»

В соответствии с методологией ITSM, можно выделить три модели ее реализации, которые различаются последовательностями внедрения базовых

процессов поддержки и предоставления ИТ-услуг. Выбор наиболее подходящей модели зависит от размера ИТ-подразделения, его функций и взаимоотношений с потребителями [12].

В ITIL выделены семь групп базовых процессов:

- управление инцидентами (INC) и организация службы поддержки (Service Desk, SD) позволяют наладить взаимодействие с пользователями и снять наиболее острые проблемы их поддержки, такие как «потери» и повторение инцидентов, длительное время реакции;
- управление конфигурацией (CFG) нацелено на формирование и поддержание в актуальном состоянии описания инфраструктуры, а также на ее стандартизацию. Этот процесс играет роль поддерживающего для большинства других процессов ITIL;
- управление изменениями (CHG) минимизирует ущерб от изменений путем их согласованного интегрированного внедрения;
- управление проблемами (PRB) позволяет уменьшить число сбоев — в первую очередь, критичных для функционирования ИТ-инфраструктуры;
- управление уровнем сервиса (SLM) направлено на выявление потребностей заказчиков и обеспечение согласованного качества услуг;
- управление инфраструктурой и приложениями (ICT) охватывает низкоуровневые процессы, обеспечивающие базовые инфраструктурные операции (например, резервное копирование) и поддержку жизненного цикла приложений [12].

Классическая модель чаще всего используется, внедряющими процессы ITIL, и является наиболее апробированной. Она подразумевает внедрение процессов в следующей последовательности: INC (+SD) > CFG > CHG > PRB > SLM. Такой подход позволяет быстро снять наиболее острые проблемы взаимодействия с бизнес-пользователями на основе процесса управления инцидентами и обеспечить поддержку этого процесса. Кроме того, удается заложить надежную основу для дальнейшего развития процессного подхода. Правда, классическая

модель требует существенных инвестиций и организационных изменений на начальном этапе внедрения.

Контрактная модель направлена на формализацию взаимоотношений ИТ-службы с бизнес-подразделениями и особенно удобна при подготовке перехода ИТ на аутсорсинг. Последовательность внедрения процессов такова: SLM > CFG > INC (+SD) > CHG > PRB. Собранные и формализованные требования заказчика позволяют четко определить стратегию развития ИТ. Однако необходимость заключения контрактов об уровне обслуживания (SLA) не всегда встречает понимание у бизнес-руководителей. А неумение управлять ожиданиями заказчика может повлечь за собой невыполнение требований SLA и существенное ухудшение имиджа ИТ-отдела [13].

Инфраструктурная модель ориентирована на формирование управляемой и предсказуемой ИТ-инфраструктуры путем внедрения процессов ITIL в такой последовательности: ICT > CFG > PRB > INC (+SD) > SLM (+CHG). Инфраструктурная модель олицетворяет упреждающий подход к управлению, поэтому инвестиции в подобный проект обычно легко обосновать. В то же время следует учитывать возможные трудности с выбором поставщика ПО и поддержкой актуальности конфигурационной базы данных [14].

Таким образом из всех представленных стратегии, банк выбрал инфраструктурную модель.

1.2.3. Способ приобретения ИС для внедрения ITSM в ПАО «Московский кредитный банк»

Способ приобретения ИС — последовательность действий от определения и формализации потребностей в информационной системе до момента, пока ИС не будет внедрена на предприятии [15].

Классификация способов приобретения ИС:

- покупка готовой ИС;
- разработка ИС (самостоятельная или заказная);
- покупка и доработка ИС;
- аутсорсинг ИС.

Преимуществами закупки готовых ИС являются: время разработки равное нулю; система тиражирована (наличие документации)

Недостатками закупки готовых ИС являются:

- система тиражирована (вопросы защиты информации);
- необходима адаптация к предъявляемым требованиям.

Недостатками разработки ИС специализированной фирмой является длительное время разработки.

Недостатками самостоятельной разработки ИС являются:

- длительное время разработки;
- отсутствия должной квалификации разработчиков;
- необходимость создания отдела ИТ.

Преимуществами самостоятельной разработки ИС являются:

- система уникальна;
- хорошая адаптация к предъявляемым требованиям.

Преимуществами разработки ИС специализированной фирмой являются:

- система уникальна;
- хорошая адаптация к предъявляемым требованиям;
- наличие должной квалификации разработчиков.

Под аутсорсинг ИС понимают:

- заказ информационной системы фирмой-потребителем у фирмы-производителя ИС;
- сдача ИС фирмой-производителем в аренду фирме-потребителю ИС;
- выполнение сторонней фирмой обработки информации для фирмы-потребителя.

Преимуществами аутсорсинга ИС являются:

- возможность сфокусировать внимание компании на ее основном бизнесе;
- возможность гибко реагировать на изменения на рынке и внутри компании;
- отсутствие необходимости в расширении штата компании;

- сокращение затрат на операции.

Одним из недостатков аутсорсинга ИС относят возможность потери поставщика (надежность).

Из анализа изложенных выше данных, можно сделать обоснованный вывод о том, что руководством банка было принято решение о покупке готового программного решения по ITSM.

1.3. Обоснование проектных решений

1.3.1. Обоснование проектных решений по информационному обеспечению

Информационное обеспечение (ИО) — важнейший элемент ИС и ИТ, который предназначен для отражения информации, характеризующей состояние управляемого объекта и являющийся основой для принятия управленческих решений. Информационное обеспечение — это создание информационных условий функционирования системы, обеспечение необходимой информацией, включение в систему средств поиска, получения, хранения, накопление, передачи, обработки информации. В состав информационного обеспечения включаются два комплекса [16]:

- внемашинное — классификаторы технико-экономической информации и документы;
- внутримашинное — макеты и экранные формы для ввода первичных данных или вывода результатной информации, структура информационной базы: входных, выходных файлов, базы данных.

Для эффективного поиска, обработки и передачи, экономическую информацию необходимо представить в цифровом виде. С этой целью ее нужно сначала упорядочить (классифицировать), а затем формализовать (закодировать) с использованием классификатора.

Классификатор — это документ, с помощью которого осуществляется формализованное описание экономической информации в экономической информационной системе, содержащей наименования объектов, наименования классификационных группировок и их кодовые обозначения.

По сфере действия выделяют: межгосударственные, общегосударственные, отраслевые и локальные классификаторы.

Основной компонентой внемашинного ИО является система документации, применяемая в процессе управлении экономическим объектом. Под документом понимается определенная совокупность сведений, используемая при решении экономических задач, расположенная на материальном носителе в соответствии с установленной формой.

Система документации — это совокупность взаимосвязанных форм документов, регулярно используемых в процессе управления экономическим объектом.

К внемашинному ИО можно отнести следующие информационные документы:

- договор с клиентом об оказании услуг;
- договора с поставщиками материалов и оборудования.

При разработке входных и выходных документов допускается использование принципов оригинального проектирования, так как большинство документов, участвующих в документообороте, являются внутрифирменными и не выходят за пределы предприятия.

Однако, при составлении договора с клиентом, необходимо соблюдение и применение унифицированной формы, поскольку договор является документом, используемым в юридических отношениях с заказчиком.

Также счет, формируемый после выполнения заказа клиента, требует соблюдения унифицированных форм.

К внутримашинному ИО относится описание экранных форм. При построении экранных форм для документов с постоянной информацией, следует иметь ввиду, что макеты используются для ввода и актуализации записей информационной базы, поэтому целесообразно применить анкетную форму расположения реквизитов, удобную для выполнения этих операций. В основе выбора экранных форм лежат принципы минимальной трудоемкости и стоимости ввода информации, максимальной степени читабельности результатной

информации, выводимой на экран, и максимальной надежности, и достоверности выполнения этих операций.

Основной частью внутримашинного ИО является Информационная база (ИБ) — определенным образом организованная совокупность данных, хранимых виде файлов в памяти вычислительной системы. Существуют следующие способы организации ИБ:

- совокупность локальных файлов, поддерживаемых функциональными пакетами прикладных программ;
- интегрированная база данных.

Организация локальных файлов связана с большим дублированием данных в разных приложениях, а также негибкостью доступа к информации, поэтому может применяться только в специализированных приложениях.

Для данного проекта целесообразно использовать интегрированную базу данных. Данная организация позволяет объединить различные источники информации, управлять файлами различных форматов. Кроме того, очевидны преимущества использования для хранения информации базы данных:

- совместимость данных;
- соответствие данных реальному состоянию объекта;
- удобство и увеличение скорости совместной обработки данных;
- поддержка целостности данных.

Основными способами организации баз данных являются: централизованные и распределенные базы данных.

Критерием выбора из способов организации баз данных является достижение минимальных трудовых и стоимостных затрат на проектирование структуры ИБ, программного обеспечения системы ведения файлов. На основании этих критериев и необходимости обеспечения надежности хранения данных выбран централизованный способ организации баз данных. Файлы с результатной информацией (отчеты), предполагается хранить в системе как архивные, с целью составления статистической отчетности за год. Остальные файлы, которые представляют собой выборки из файлов базы данных, хранить нет

необходимости, поскольку они могут быть сформированы путем обращения к базе данных в любой момент времени.

1.3.2. Обоснование проектных решений по программному обеспечению

Программное обеспечение (ПО) включает совокупность программ, реализующих функции и задачи ИС и обеспечивающих устойчивую работу комплексов технических средств. В состав программного обеспечения входят общесистемные и специальные программы, а также инструктивно-методические материалы по применению средств программного обеспечения [17].

Операционная система (ОС) составляет основу программного обеспечения компьютера. ОС представляет комплекс системных и служебных программных средств, который обеспечивает взаимодействие пользователя с компьютером и выполнение всех других программ.

В зависимости от алгоритма управления процессом операционные системы подразделяются на:

- однозадачные и многозадачные;
- однопользовательские и многопользовательские;
- однопроцессорные и многопроцессорные системы;
- локальные и сетевые.

В однозадачных системах используются средства управления периферийными устройствами, средства управления файлами, средства общения с пользователями.

Многозадачные ОС используют все эти средства и управляют разделением совместно используемых ресурсов (ОЗУ, процессор и тд.). В зависимости от областей использования многозадачные ОС подразделяются на:

- системы пакетной обработки;
- системы с разделением времени;
- системы реального времени.

В многопользовательских ОС каждый пользователь настраивает для себя интерфейс, кроме того, существуют средства защиты информации каждого пользователя от несанкционированного доступа других пользователей.

На компьютерах, используемых в качестве рабочих мест пользователей, применяется ОС Windows 10.

Рассмотрим классификацию систем управления баз данных (СУБД):

- по выполняемым функциям: операционные и информационные;
- по сфере применения: универсальные и проблемно-ориентированные;
- по используемому языку общения: замкнутые (имеющие самостоятельные языки общения пользователей с базами данных) и открытые (для общения с базой данных используется язык программирования, расширенный операторами языка манипулирования данными);
- по числу поддерживаемых уровней моделей данных: одно-, двух-, трехуровневые системы;
- по способу установления связей между данными: реляционные, иерархические и сетевые базы данных;
- по способу организации хранения данных и выполнение функций обработки базы данных: централизованные и распределенные.

1.3.3. Обоснование проектных решений по техническому обеспечению

Техническое обеспечение — это персональный компьютер, оргтехника, линии связи, оборудования сетей. Вид информационной технологии, зависящий от технической оснащенности (ручной, автоматизированный, удаленный) влияет на сбор, обработку и передачу информации. Комплекс технических средств составляют:

- компьютеры;
- устройства сбора, накопления, обработки, передачи и вывода информации (жесткие диски, устройства хранения данных, сканеры, принтеры и т.д.);

- устройства передачи данных (маршрутизаторы, коммутаторы и т.д.);
- эксплуатационные материалы (бумага, флеш-накопители и т.п.).

При выборе компьютера необходимо учитывать такие характеристики как:

- надежность;
- стоимостные затраты,;
- производительность;
- простота использования и др.

От значения данных параметров зависит возможность работы с требуемыми программными средствами, а значит, и успех создания системы.

Для технической реализации системы необходим сервер баз данных, на котором будет хранится сама база данных. К серверу баз данных будет осуществляться доступ с локальных станций конечных пользователей, используя сетевой коммутатор. В случае необходимости удаленного доступа к серверу баз данных используется маршрутизатор.

Сервер и персональные компьютеры, работающие в организации, имеют технические характеристики, превышающие требуемые для работы информационной системы. Значит разработка модуля возможна на любом из имеющихся в наличии компьютеров и сервера. Для печати, сканирования и копирования документов установлено соответствующее оборудование, так же, для обеспечения сохранности данных при аварийном отключении электропитания, рабочие места оборудованы блоком бесперебойного питания. Поэтому внедрение разрабатываемой системы не требует закупки и установки дополнительных технических средств [18].

II ПРОЕКТНАЯ ЧАСТЬ

2.1. Понятие и сущность ITSM

ITSM (IT Service Management, управление ИТ-услугами) — подход к управлению и организации ИТ-услуг, направленный на удовлетворение потребностей бизнеса. Управление ИТ-услугами реализуется поставщиками ИТ-услуг путём использования оптимального сочетания людей, процессов и информационных технологий. Для содействия реализации подхода к управлению ИТ-услугами используется серия документов ITIL [19].

В отличие от более традиционного технологического подхода, ITSM рекомендует сосредоточиться на клиенте и его потребностях, на услугах, предоставляемых пользователю информационными технологиями, а не на самих технологиях. При этом процессная организация предоставления услуг и наличие заранее оговоренных в соглашениях об уровне услуг параметров эффективности (KPI) позволяет ИТ-отделам предоставлять качественные услуги, измерять и улучшать их качество.

Важным моментом при изложении принципов ITSM является системность. При изложении каждого составного элемента ITSM (управление инцидентами, управление конфигурациями, управление безопасностью и т. д.) в обязательном порядке прослеживается его взаимосвязь и координация с остальными элементами (службами, процессами) и при этом даются необходимые практические рекомендации.

ITIL не является конкретным алгоритмом или руководством к действию, но она описывает передовой опыт (best practices) и предлагает рекомендации по организации процессного подхода и управления качеством предоставления услуг. Это позволяет оторваться от особенностей данного конкретного предприятия в данной конкретной отрасли. Вместе с тем, несмотря на определённую абстрактность, ITIL всячески нацелено на практическое использование. В каждом разделе библиотеки приводятся ключевые факторы успеха внедрения того

или иного процесса, практические рекомендации при этом превалируют над чисто теоретическими рассуждениями.

Процессы ITSM. IT Service Management (ITSM) объединяет 10 процессов, описанных в книгах «Service Support» и «Service Delivery» библиотеки ITIL. Модель CobIT (Control Objectives for Information and Related Technology) — это набор документов, в которых изложены международные стандарты управления, контроля и аудита информационных систем любого масштаба и сложности (табл. 2.1) [20, 21].

Таблица 2.1

Процессы ITSM

Название процесса	Цель процесса
Управление инцидентами (Incident management)	Цель процесса обеспечить устранение инцидентов в предельно сжатые сроки. Инцидент — это любое событие: сбои, запросы на консультации и т.п., которое может привести к понижению качества предоставления услуги. Для успешного управления инцидентами необходимо создание диспетчерской службы (Service desk), которая должна являться единой точкой контакта с пользователями и координирует устранение инцидентов.
Управление проблемами (Problem management)	Организация процесса направлена на уменьшение количества инцидентов, за счет выявления и устранения причин возникновения инцидентов.
Управление конфигурациями (Configuration management)	Процесс заключается в создании и поддержании в актуальном состоянии логической модели инфраструктуры компании
Управление изменениями (Change management)	Целью процесса является организация проведения изменений с наименьшим риском возникновения инцидентов, вызванных изменениями
Управление релизами (Release management)	Цель процесса — обеспечение работоспособности производственной среды при внедрении изменений
Управление уровнем сервиса (Service level management)	Цель процесса — выявить состав и уровень сервиса на основании требовании потребителей и поставщиков ИТ-сервисов, контролировать достижение установленного уровня сервиса
Управление финансами (Financial management for IT services)	Цель процесса заключается в обеспечении стабильного финансирования всех прочих процессов
Управление мощностью (Capacity management)	Цель этого процесса исключить возникновение инцидентов, по причине недостаточной мощности ИТ инфраструктуры компании, и в то же время избежать неоправданных затрат на приобретение излишних, неиспользуемых мощностей
Управление непрерывностью (IT service continuity management)	Организация процесса направлена на обеспечение гарантированного восстановления предоставления ИТ-сервисов до уровня, необходимого для продолжения бизнес-операций за определенный промежуток времени, в случае чрезвычайной ситуации (пожара, наводнения, отключения электроэнергии)
Управление доступностью (Availability management)	Процесс включает в себя обеспечение согласованного уровня доступности сервиса, а также оценку текущей доступности сервиса и планирование действий, направленных на ее дальнейшее улучшение

Модель или открытый стандарт CobiT создается ISACF (Фонд аудита и контроля информационных систем) и поддерживается ассоциацией ISACA (Ассоциации аудита и контроля информационных систем).

Модель CobiT также, как и модель ITIL являются открытыми стандартами, независимыми от конкретных производителей, платформ и технологий. Данные стандарты описывают часто используемые ИТ-процессы. Однако библиотека ITIL направлена в основном на управление ИТ-процессами, а стандарт CobiT в первую очередь предназначен для контроля и аудита информационных систем компании.

Следует отметить, что имеется несколько принципиальных отличий.

CobiT (книга «Принципы управления») представляет инструменты управления ИТ-процессами более высокого уровня по сравнению с ITIL. В ITIL приводится подробное описание процедур, направленных на внедрение ИТ-процессов на уровне взаимодействия «Директор по ИТ (СЮ) — Руководители подразделений ДИТ». CobiT ориентирован на уровень взаимодействия «Куратор ИТ от бизнеса — Директор по ИТ (СЮ)».

Стандарт CobiT — это единый подход к сбору и анализу информации, подготовке выводов и заключений на всех этапах управления, контроля и аудита информационных систем. CoBiT позволяет использовать лучший опыт в сфере аудита и контроля информационных систем с учетом существующих ИТ-процессов:

- подавляющем большинстве организаций процессы, а особенно их цели, стабильны и изменяются нечасто, по сравнению с организационными объектами (сотрудники, отделы, департаменты и пр.);
- внедрение информационных технологий, как правило, не ограничивается рамками одного отдела или департамента, а затрагивает всю структуру организации и ИТ-службу.

Прикладное пользовательское программное обеспечение является неотъемлемой объекты контроля CobiT и стандартно оценивается в рамках единой структуры с применением единых метрик.

Модель MOF (Microsoft Operations Framework) — это коллекция руководств по управлению ИТ-системами, разработанная компанией Microsoft на основе лучшего многолетнего опыта разработки, управления и обслуживания крупномасштабных информационных систем. Данная модель направлена на то, чтобы помочь компаниям достигнуть оптимального уровня надежности, доступности, управляемости ИТ-систем, основанных на продуктах и технологиях Microsoft.

Модель MOF — это гибкий подход к управлению ИТ-процессами, основанный:

- на библиотеке ITIL, являющейся международным стандартом в сфере организации и управления информационными технологиями;
- на стандарте ISO 15504, который поддерживается Международной организацией стандартизации (International Organization for Standardization);
- на опыте компании Microsoft, накопленном при работе с корпоративными клиентами. MOF включает в себя набор документов: статей (white papers), руководств (operations guides), материалов обучающих курсов.

MOF предлагает три основные модели, каждая из которых обобщает лучший практический опыт в своей сфере:

- модель процессов (MOF Process Model);
- модель команды (MOF Team Model);
- модель управления рисками (MOF Risk Model).

Модель MOF предназначена для создания среды, в которой компания и ИТ-подразделение смогут совместно работать над совершенствованием деятельности и использовать при этом проактивную модель, определяющую процессы и стандартные процедуры, направленные на повышение эффективности и продуктивности ИТ-услуг.

Модели MOF расширяют и реорганизовывают процессы библиотеки ITIL, а также дополняют их практическими рекомендациями по внедрению.

Модель процессов (MOF Process Model) описывает процессы управления обслуживанием ИТ-систем, представленные в виде функций управления услугами (Service Management Functions, SMF). В рамках данного процесса управления команда, обслуживающая ИТ-систему, несет полную ответственность за управление всеми изменениями в ИТ-инфраструктуре компании.

Эффективный контроль над изменениями достигается за счет формирования родственных служб в серию «выпусков» (групп изменений), каждый из которых может планироваться и управляться отдельно. MOF Process Model представлена в виде 20 SMF-функций, распределенных на четыре квадранта.

Большинство SMF-функций совпадает с процессами ITIL, также модель MOF предлагает дополнительные SMF-функций: «Управление людскими ресурсами» (квадрант «Оптимизация») и все функции квадранта «Обслуживание». Функция «Управление людскими ресурсами (Workforce Management)» включает рекомендации по управлению ИТ-персоналом (набор, сохранение и мотивация). В квадрант «Обслуживание» выделены стандартные процессы обслуживания ИТ-систем, направленные на достижение предсказуемого поведения. системы:

- системное администрирование (System Administration) — ежедневные операции по администрированию информационной системы. Данный процесс координирует деятельность всех остальных функций данного квадранта;
- администрирование системы безопасности (Security Administration) включает в себя обеспечение безопасности ИТ-системы, определение и контроль параметров защиты корпоративной информации, контроль деятельности персонала с точки зрения безопасности;
- сетевое администрирование (Network Administration) — обеспечение непрерывной и стабильной работы сетевой инфраструктуры;
- мониторинг услуг (Service Monitoring and Control) — получение персоналом актуальных сведений о состоянии ИТ-услуг: состояние процессов, загрузка серверов, время отклика приложений и прочее;

- администрирование служб каталога (Directory Services Administration) — поддержка корпоративной службы каталога и контроль приложений, взаимодействующих с каталогом;
- управление хранением данных (Storage Management) — включает в себя создание плана архивации и восстановления данных, мониторинг систем хранения и оценку необходимости предоставления новых услуг по резервированию данных;
- планирование работ (Job Scheduling) — эффективное управление процессом выполнения работ для выполнения соглашения об уровне услуг;
- управление результатами (Print and Output Management) контролирование процесса предоставления данных в отчетах.

Руководства (operations guide), входящие в набор документов MOF, содержат рекомендации по внедрению процессов управления квадранта «Обслуживание», на базе продуктов и технологий Microsoft. Модель команды (MOF Team Model) описывает процедуру создания команды, обслуживающей территориально распределенную ИТ-систему, распределение ролей в команде и их функциональные обязанности, принципы совмещения ролей, варианты масштабирования команды, управление распределенной ИТ-системой, построенной на платформе Microsoft, а также связи с другими моделями Microsoft Enterprise Services.

Международный стандарт ISO/IEC 20000:2005, основанный на стандарте BS 15000:2002, разработанном BSI, является обобщением мирового опыта в организации управления ГГ-услугами и применим к любой организации, вне зависимости от отрасли и размеров, в деятельности которой ГГ-у слуги играют важную роль [22].

Стандарт определяет требования и взаимосвязанные процессы, необходимые для создания и эффективного использования системы менеджмента. В нём предлагаются универсальные критерии, по которым можно объективно

оценивать возможности компании при выполнении требований пользователей с учётом особенностей бизнеса. Стандарт состоит из двух частей:

1. ISO 20000-1:2005 «Information technology — Service management. Part 1: Specification» представляет собой подробное описание требований к системе менеджмента ИТ-сервисов и ответственность за инициирование, выполнение и поддержку в организациях. Эта часть состоит из 10 разделов, 13 процессов, собранных в пять ключевых групп:

а) процессы предоставления сервисов (Service delivery process): в группу входят управление уровнем сервисов, управление непрерывностью и доступностью, управление мощностями, отчётность по предоставлению сервисов, управление информационной безопасностью, бюджетирование и учёт затрат;

б) процессы управления взаимодействием (Relationship processes): эта область включает в себя управление взаимодействием с бизнесом, управление поставщиками;

в) процессы разрешения (Resolution processes): разработчики стандарта фокусируются на инцидентах, которые удалось предотвратить или успешно разрешить — управление проблемами, управление инцидентами;

г) процессы контроля (Control processes): в данном разделе рассматриваются процессы управления изменениями и конфигурациями;

д) процессы управления релизами (Release process): речь идёт о выработке новых и коррекции уже имеющихся решений.

2. ISO 20000-2:2005 «Information technology — Service management. Part 2: Code of Practice» — это практические рекомендации по процессам, требования к которым сформулированы в первой части. Является руководством для аудиторов и компаний, намеренных пройти сертификацию. Содержит 10 разделов. Оценка соответствия ИТ сервисов требованиям ISO 20000-1:2005 позволяет представить объём нереализованных требований. Кроме того, удаётся запланировать их выполнение с учётом рекомендаций ISO 20000-2:2005, библиотеки ITIL или любой другой методологии. Внедрение ISO 200002:2005 или ITIL не является обязательным требованием соответствия стандарту ISO 20000-1:2005, но

использование практик, упоминаемых в ISO 20000-2:2005 или ITIL, делает этот процесс гораздо более простым и ясным. Стандарт ISO 20000:2005 предлагает модель улучшения процессов — цикл PDCA (цикл Деминга):

а) планирование (PLAN) — установка целей управления услугами и определение процессов управления услугами, необходимых для получения результатов, соответствующих требованиям потребителей и политикам поставщика услуг;

б) реализация (DO) — внедрение процессов управления услугами;

в) проверка (CHECK) — контроль и измерение процессов управления услугами и самих услуг на соответствие политикам поставщика услуг, целям управления услугами и требованиям потребителей услуг;

г) действие (ACT) — выполнение действий по постоянному улучшению показателей процессов.

Кроме того, в стандарте выдвигаются требования к мере ответственности руководителей компании, предоставляющей ИТ-услуги, а также к управлению документацией, компетенции, осведомлённости и подготовке персонала.

Чтобы обеспечить интегрированный подход к оказанию высококачественных и эффективных ИТ-услуг, стандарт ISO 20000:2005 предлагает переход к сервисной модели ИТ, который реализуется путём разработки и внедрения формальной системы управления ИТ-услугами, которая позволяет повысить уровень капитализации предприятия и способствует его признанию на международном уровне.

После внедрения системы управления ИТ-услугами предприятие подходит к сертификации. В ходе сертификации по стандарту ISO 20000 проверяются политика и цели компании, система оценки рисков ИТ-сервисов, используемые процедуры и соответствие требованиям стандарта. Таким образом, стандарт ISO 20000:2005, во-первых, предоставляет средства для оценки и измерения эффективности деятельности внутренней организации ИТ. Во-вторых, стандарт направлен на реализацию задач, связанных с проведением тендеров при выборе внешнего поставщика ИТ-услуг. Независимая сертификация по этому стандарту

позволяет организациям продемонстрировать своим клиентам соответствие качества оказываемых услуг лучшим мировым практикам.

2.1.1. Ошибки на этапах внедрения ITSM и их описание

В определенный момент развития компании руководство ИТ-подразделения понимает, что его работа становится неэффективной, решение инцидентов занимает слишком много времени, пользователи недовольны предоставляемыми услугами, владельцы бизнеса не выделяют финансирование, а внутренняя организация работы представляет собой полный хаос. Внедрение ITSM (Information Technology Service Management) может решить все эти проблемы, но необходимо выбрать правильный подход к реализации проекта, чтобы получить положительный эффект, а не просто потратить время и средства [23].

Следует отметить, что существует некоторая путаница в понятиях.

Надо четко понимать, что ITSM — это сервисный подход к управлению ИТ, в нем деятельность ИТ-подразделения рассматривается как перечень услуг, которые оно предоставляет другим подразделениям в соответствии с SLA (соглашение об уровне услуг). Управление ИТ осуществляется как отдельным бизнесом, со своими бизнес-процессами [24].

В свою очередь ITIL (Information Technology Infrastructure Library) — это библиотека рекомендаций, основанных на опыте многих компаний, о том, как должно работать ИТ-подразделение и как в нем реализовать ITSM. Именно рекомендации, а не готовые решения или шаги по реализации [25].

Ошибкой будет полагать, что, руководствуясь книгами ITIL, можно как по инструкции внедрить ITSM.

Внедрение ITSM нужно не только ИТ, но и бизнесу. С внедрением процессной модели работа ИТ-подразделения становится прозрачной и понятной бизнесу. Когда руководство видит, какие услуги оказывает ИТ-отдел, становится проще оценивать эффективность его работы и планировать бюджет на его содержание. Для рядовых сотрудников компании внедрение ITSM обеспечивает более высокое качество предоставления услуг, быструю реакцию на

возникающие проблемы, работу без простоев и гарантированные сроки исполнения запросов [25].

Таким образом, ошибкой является внедрение ITSM только для ИТ, этот процесс затрагивает всю компанию.

Считают, что на внедрение ITSM не нужен отдельный бюджет. Однако это не совсем правильное мнение.

Внедрение ITSM — дорогостоящий процесс, в нем задействовано большое число человеческих и материальных ресурсов. Полагаться в этом только на внутренние резервы ИТ-подразделения ошибочно, необходимо четко обосновать перед бизнесом финансовую целесообразность и окупаемость проекта, чтобы получить бюджет на внедрение [25].

Основными преимуществами внедрения ITSM для бизнеса могут стать: организация эффективной деятельности ИТ-подразделения за счет использования процессов, описанных в ITIL (управление инцидентами, конфигурациями, проблемами, изменениями, уровнем обслуживания); повышение надежности и стабильности услуг ИТ (управление мощностью и доступностью); финансовая прозрачность деятельности ИТ (управление финансами ИТ) [25].

Создавая процессы управления ИТ можно увидеть, что трудозатраты на оказание некоторых видов услуг превышают отдачу от них, передав неэффективные услуги на аутсорсинг (обслуживание оргтехники, хостинг сайта, кабельные и слаботочные сети), можно сосредоточить усилия на более ценных для бизнеса, улучшив их качество. ITSM поможет определить правила взаимодействия заказчика с исполнителем, закрепить в SLA их обязанности и параметры качества предоставления услуг.

Внедрение службы поддержки Service Desk (управление инцидентами, оценка качества предоставления услуг, портал самообслуживания) повысит лояльность пользователей к ИТ-подразделению и сделает ИТ неотъемлемой частью других бизнес-процессов.

Ошибкой будет попытка внедрения ITSM только на средства ИТ без согласия и помощи бизнеса.

Пройдя курсы ITIL или прочитав множество примеров внедрения ITSM, руководитель ИТ-подразделения покупает коробку с программным комплексом и делегирует сотрудникам его установку, настройку и внедрение. Но процесс внедрения ITSM начинается не с этого.

В первую очередь необходимо провести аналитическую работу: аудит текущего состояния ИТ-отдела и процессов, которые он использует, определить потребности бизнеса в оказываемых и новых ИТ-услугах, построить регламенты использования методологии ITIL. В разработанном техническом задании формулируются процессы ITIL, которые предполагаются к внедрению, состав и порядок их внедрения. Техническое задание может стать основным документом, по которому будет осуществляться переход компании на процессную модель ИТ собственными силами или с помощью компании-подрядчика.

Даже грамотное внедрение трех важных процессов — управление инцидентами, активами и уровнем обслуживания — после проведения аудита и регламентации этапов проведения работ позволят наладить контакт между бизнесом, пользователями и ИТ, построить бизнес-ориентированную модель предоставления ИТ-услуг и повысить их качество.

Внедрение ITSM «из коробки» без проведения подготовительных работ и четко выстроенных процессов является ошибкой.

Внедрение ITSM по методологии ITIL — это в первую очередь бумажная работа. Создание опросников, проведение аудита, определение требований бизнеса и ожиданий от ИТ, анализ текущей системы управления ИТ, определение внедряемых процессов, определение системы автоматизации, отчеты и презентации для защиты выбранного решения, подготовка ТЗ с подробными описаниями всех процессов — это все не требует никаких средств автоматизации, только времени и желания достигнуть поставленных целей. Необходима мотивация и взаимодействие сотрудников, которые внедряют и будут в будущем отвечать за процесс.

После завершения подготовительных работ наступает этап внедрения средств автоматизации. Можно ограничиться ведением базы в таблицах или на

бумаге, для приема заявок использовать электронную почту, а обратную связь от пользователей получать по телефону. Но этот способ обладает настолько низкой эффективностью, что никогда не окупит вложенные средства и время. Кроме того, без развернутых отчетов о деятельности ИТ-подразделения после внедрения ITSM сложно будет обосновывать затраты на дальнейшую эксплуатацию системы и оценивать ее экономическую выгоду для бизнеса.

Внедрение Service Desk позволяет повысить скорость решения инцидентов, экономит время высококвалифицированных специалистов за счет использования базы знаний на первом уровне поддержки, увеличивает важность ИТ для сотрудников компании. Портал самообслуживания (сайт Service Desk) является точкой коммуникации пользователей и ИТ, прозрачной и понятной, местом, где всегда можно получить помощь.

Ошибкой является использование устаревших систем коммуникации и накопления данных при внедрении современной системы ITSM.

Естественным желанием при внедрении ITSM является самостоятельность. Кажется, что, прочитав несколько книг и практик внедрения, все можно сделать своими силами. Создать команду из сотрудников ИТ-подразделения или нанять новых, поставить перед ними задачу и ждать успешного завершения внедрения. Только процесс оказывается настолько трудоемким, что начинает тормозить выполнение остальных функций ИТ, сотрудники разрываются между изучением ITIL и выполнением своих основных обязанностей. Грамотное описание внедряемых процессов требует отличного знания текущего устройства ИТ, а анализ бизнес-потребностей — коммуникабельности и умения анализировать разрозненную информацию.

В большинстве случаев выгоднее использовать услуги сторонней компании для консультирования или комплексного внедрения, которая за своими плечами имеет большой опыт внедрения проектов ITSM. ИТ-специалисты должны принимать участие во внедрении, но не заниматься им непосредственно, их обязанностью станет эффективная эксплуатация готовой системы и предо-

накопление базы знаний, улучшение качества обслуживания, внедрение новых сервисов.

Ошибкой является внедрение ITSM только своими силами, это приведет к множественным проблемам и зря потраченным ресурсам компании.

ITSM — это непрерывный процесс, который пронизывает все направления бизнеса и работы, над которым не останавливаются никогда, единожды начавшись. Правильный подход к внедрению, выбор платформы и компании консультанта-интегратора, позволят достичь поставленного результат и организовать эффективное и удобное управление ИТ.

2.1.2. Организационно-правовые и программно-аппаратные средства обеспечения информационной безопасности и защиты информации

Информационная безопасность предполагает отсутствие угроз, направленных на целостность; конфиденциальность; доступность; защита человека от информации [26].

Целостность информации — предполагает отсутствие модификации, изменения или уничтожения информации.

Конфиденциальность информации — это защита информации от несанкционированного доступа.

Доступность (отсутствие потери информации) — это доступность информации со стороны всех заинтересованных лиц, которые имеют право на эту информацию.

Угроза информации — это потенциально возможное событие, которое приводит к последствиям нарушения целостности, доступности и конфиденциальности информации.

Нарушение безопасности — называется реализация данной угрозы безопасности.

Угроза безопасности бывает объективная — не зависящая от человека, и субъективная — преднамеренная и не преднамеренная.

Не преднамеренные субъективные (искусственные) угрозы:

1. Искусственные, не умышленные действия людей, персонала, которые приводят к частичному или полному выводу компьютерных систем из строя.

2. Не правомерное использование оборудования или изменения режимов работ этого оборудования.

3. Не умышленная порча носителей информации.

4. Запуск технологически не правомочных программ (не лицензионных программ).

5. Это не легальное использование не учтённых программ (не лицензионное оборудование).

6. Заражение ПК или системы вирусами.

7. Не осторожное разглашение конфиденциальной информации, делающей её общедоступной для не санкционированного круга пользователей.

8. Нарушение атрибутов, правил, разграничений и т.д.

9. Это изначально не правильное проектирование архитектуры системы, в которую заранее заложены «люки», «лазы» и «дырки» для постороннего нарушителя. Игнорирование посторонних нарушений.

10. Вход в компьютерную систему в обход установленных правил.

11. Не компетентность в использовании КС и установление правил разграничения доступа.

12. Это ошибочная пересылка данных по не санкционированному адресу абонента.

13. Ввод ошибочных данных.

14. Не умышленное повреждение каналов передачи данных.

Основные преднамеренные искусственные угрозы:

1. Физическое разрушение системы.

2. Вывод из строя обеспечивающих систему.

3. Дезорганизация компьютерной или вычислительной системы.

4. Внедрение в число персонала «заинтересованного» человека.

5. Преднамеренная искусственная угроза: шантаж, угроза персонала компьютерной системы.

6. Применение средств технических разведок: фотографирование, подслушивание и т.д.

7. Перехват побочных электромагнитных излучений и наводок (ПЭМИН).

8. Перехват передаваемых данных по каналу связи и т.д.

9. Хищение носителей информации.

10. Не законное получение правил и атрибутов разграничения доступа (паролей, логинов и т.д.).

11. Не законное воспользование терминалами законных пользователей с целью проникновения в систему под именем санкционированного пользователя.

12. Вскрытие шифров криптозащиты санкционированных пользователей.

13. Внедрение закладок типа «троянских коней», «жучков», «ловушек» и т.д. с целью внедрения не декларированного программного обеспечения санкционированных пользователей.

14. Не законное подключение к линиям передачи данных с целью работы между строк, выдавая себя за законного пользователя.

Информационная безопасность — это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации. Рассматривая информацию как товар можно сказать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т. д. С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т. д.), можно утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления — производстве, транспорте и др.

Именно поэтому при определении понятия "информационная безопасность" на первое место ставится защита информации от различных воздействий. Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности. Согласно ГОСТу 350922-96 защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью. Исходя из этого, отметим следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации — это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять. В ряде случаев понятие «информационная безопасность» подменяется термином

«компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем.

Выделим три основные уровня формирования режима информационной безопасности в банке:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры [27].

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений,

проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.). Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу [28].

К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например, антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Так, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей системой EFS (Windows) или специальной программой шифрования. Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения [29].

Несмотря на то, что возможностей взломать и забрать информацию всегда много, обеспечение безопасности банковских данных — процедура вполне реальная.

Благодаря наличию современных методов теперь усовершенствована система криптографии, а также реализована такая мера, как электронная цифровая подпись (ЭЦП). Она так называемый аналог и заменяет собственноручную подпись. Также она обладает непосредственной привязкой к электронному ключу, хранящемуся у владельца подписи. У этого ключа две части: открытая и закрытая, а также есть защита — наличие специального кода.

Система безопасности, в общем, является непрерывным процессом идентификации, анализа и контроля.

Основные принципы, согласно которым обеспечивается информационная безопасность банка:

1. Проблемы своевременно устанавливаются и обнаруживаются.

2. Можно спрогнозировать развитие.

3. Предпринятые меры должны быть актуальными и эффективными.

Также стоит отдельно выделить, насколько важна тщательная и регулярная работа с персоналом, так как обеспечение безопасности информации зависит и от того, насколько качественно и аккуратно выполняются требования службы безопасности [30, 31].

Рассмотрим основные угрозы информационной безопасности банка [26].

Человеческий фактор — основная и главная угроза информационной безопасности, напрямую зависящий от человеческих отношений. Утечка информации чаще всего происходит во вине банковского персонала.

Как показывает статистика, примерно 80% правонарушений происходит из-за банковских сотрудников — из-за тех, кто обладает доступом к данным.

При этом обеспечение внутренней информационной безопасности банка, является крайне необходимой мерой как для того, чтобы защитить конфиденциальность данных от обычной халатности, так и для того, чтобы исключить намеренный взлом баз данных.

Есть не только внутренний фактор — но и наличие технической угрозы информационной безопасности, как банковских организаций, так и компаний. Технические угрозы — это взломы информационных систем, лицами, не

имеющими прямого доступа к системе. Это могут быть криминальные или конкурирующие организации.

Снимают и получают информацию в этом случае с помощью особенной аудио или видео аппаратуры. Современная популярная форма взлома — когда применяются электрические и электромагнитные излучения. Злоумышленники за это время получают конфиденциальную информацию, ЭЦП.

Опасность и угроза для программного обеспечения исходит и от различных вредоносных для носителя информации компьютерных вирусов, программных закладок, способных привести к разрушению введенных кодов.

Самый известный способ решения подобных компьютерных проблем — установка лицензионных антивирусных программ, успешно справляющихся с данной проблемой.

В защите банковской информации от внутренних и внешних утечек может помочь поможет грамотный специалист в этой области и программное обеспечение, которое будет заниматься отслеживанием и блокировкой передачи информации на съемные носители (например, флешки).

2.2. Описание существующих ITSM-систем управления IT сервисов

На рынке существует множество ITSM-систем, которые можно разбить на две группы [32]:

- Open-source решения (бесплатное решение с открытым кодом).
- Коммерческие решения.

Рассмотрим особенности и функциональные возможности некоторых ITSM-систем. Для анализа отберем наиболее популярные решения, предлагаемые на российском рынке, с которыми автор настоящей работы имеет практический опыт работы: Bpm`online; OTRS; Naumen SD; Omnitracker.

Анализ этих систем проводится по следующим критериям:

- сложность внедрения;
- соответствие ITIL;

- удобство работы и дизайн.

Поэтому в дальнейшем все решения будут анализироваться с точки зрения «коробочных» решений

Bpm`online Service

В начале немного расскажу по системам. И первая в очереди bpm`online. Система для нашей компании новая и только запускается на одном из проектов. Но уже сейчас можно поделиться своими впечатлениями.

Это система от украинско-российского разработчика. Всего вендор предлагает три решения: Marketing, Sales и Service Enterprise. Как раз последнее и отвечает за автоматизацию процессов ITIL, но не ограничивается ей.

В систему также уже включены надстройки Контакт центра и часть функционала CRM, что расширяет возможности системы ITSM, нет «толстого» клиента и всё взаимодействие происходит через веб-интерфейс, что в свою очередь дает возможность доступа к личному кабинету с любого устройства. Интерфейс очень дружелюбный как для пользователя, так и для специалистов. Система позволяет подавать заявки не только через портал самообслуживания, но и через чат-боты. Благодаря простой и гибкой настройке решения новый не сложный бизнес-процесс можно построить буквально за два часа. Из «коробки» уже поддерживает восемь процессов ITIL:

1) управление инцидентами и запросами на обслуживание;
2) управление изменениями;
3) управление уровнем сервиса;
4) управления проблемами;
5) управление знаниями;
6) управление релизами;
7) управление конфигурациями;
8) управление портфелем услуг.

Omnitracker

Второе решение — детище немецкого разработчика Omninet. Система появилась на российском рынке в 2009 году. У ITSM есть как «толстый», так и «тонкий». Систему можно полностью настроить под себя, как самостоятельно, так и через вендора, но, если это делать самим, потребуются высококвалифицированные специалисты и, соответственно, дополнительные затраты на внедрение. Под свои внутренние нужды мы как раз используем Omnitracker, но настроенный нашими специалистами, под наши процесс и полностью под себя. Мы же рассмотрим готовое решение ITSM Center, что не мало важно, сертифицированное по ITIL v3. В данной сборке реализованы 15 основных процессов ITIL:

1) управление инцидентами;
2) управление проблемами;
3) управление изменениями;
4) управление запросами на обслуживание;
5) управление событиями;
6) управление активами и конфигурациями;
7) идентификация и управление доступом;
8) управление релизами и развертыванием;
9) управление уровнем услуг;
10) управление каталогом услуг;
11) управление мощностями;
12) управление доступностью;
13) управление знаниями;
14) управление справочными данными и адресами;
15) возможность интеграции процесса оплаты услуг.

Система отчетности здесь внешняя Crystal report, что опять же влечет за собой дополнительные расходы на приобретение данного продукта. Нет мобильной версии, имеется адаптированный веб-интерфейс, что с одной стороны можно посчитать плюсом, т.к. не требуется установка, но и минусом из-за невозможности работать в офлайн-режиме или с нестабильным интернетом.

Naumen Service Desk

Третья система снова российская. Naumen — довольно интересная отечественная разработка, на рынке с 2001 года.

Имеет так же только веб-интерфейс, как и bpm`online service. На данный момент считается лидером на российском рынке ITSM-систем по отзывам клиентов. Гибкий интерфейс системы позволяет настроить из коробки 12 ITIL процессов:

1) управление инцидентами;
2) управление запросами на обслуживание;
3) управление проблемами;
4) управление сервисными активами и конфигурациями;
5) управление изменениями;
6) управление каталогом услуг;
7) управление уровнем услуг;
8) управление событиями;
9) управление знаниями;
10) управление согласованиями и доступом;
11) управление задачами/нарядами;
12) управление финансами.

OTRS

И последний представитель — бесплатная open-source система OTRS. И опять у системы есть только «тонкий» клиент. В коробочном решении представлены основные ITIL-процессы, в данной версии их шесть:

1) управление инцидентами;
2) управление проблемами;
3) управление активами и конфигурациями;
4) управление изменениями;
5) управление запросами на обслуживание;
6) управление знаниями.

Это «коробочное» решение не бесплатное в отличие от самой системы и поставляется пока единственным интегратором на территории России.

Сравнительная характеристика основных показателей распространенных ITSM-систем сведены в таблице 2.2.

Таблица 2.2

Сравнительная характеристика показателей распространенных ITSM-систем

Показатель	Bpm`online Service	OTRS	Naumen SD	Omnitracker
Готовый функционал	Высокий	Высокий	Средний	Средний
Гибкость продукта	Высокий	Высокий	Высокий	Высокий
Бренд	Средний	Высокий	Высокий	Средний
Компания-разработчик	Creatio	OTRS AG	Naumen	Omni
Примерная стоимость внедрения, млн руб.	1	5,5	6	0,95

Список процессов можно расширить самостоятельно путем доработки, благо оболочка позволяет кастомизировать систему под свои нужды, как угодно.

В заключении следует отметить, что специалисты могут развернуть любое из этих решений практически за два часа. Но есть один большой минус — нужны высококвалифицированные программисты для поддержки и развития.

2.3. Этапы внедрения ITSM

Переход к сервисному управлению информационными технологиями (Information Technology Service Management, ITSM) предполагает реинжиниринг действующих в организации бизнес-процессов, которые пока принято считать вспомогательными [33]. При этом предусматривается создание новой или модернизация существующей системы автоматизации ITSM.

Реинжиниринг действующих процессов управления ИТ не должен нарушить повседневную деятельность организации. Его следует проводить с учетом корпоративной культуры конкретной компании и уровня зрелости всех ее бизнес-процессов. Требуется определить порядок реализации нового процесса, спроектировать и внедрить систему его автоматизации. Наконец, необходимо обучить сотрудников ИТ-подразделения способам исполнения нового процесса с использованием системы автоматизации — без нарушения деятельности ИТ-подразделения и всей организации. Таким образом, внедрение ITSM

представляет собой достаточно сложный проект, который должен реализовываться по определенной технологии.

В России растет количество компаний, которые предлагают услуги внедрения ITSM и реализуют собственные технологии, основанные на общем походе к ITSM. Многообразие приводит к тому, что заказчикам приходится выбирать ту технологию и того исполнителя проекта, которые соответствуют его требованиям к стоимости и срокам внедрения. Немаловажным фактором является удовлетворенность заказчика результатами внедрения, то есть их качеством. А последнее зависит не только от соответствия организации-исполнителя стандартам ISO 20000, ИСО 9000 и от функционала системы автоматизации, но и от выполнения корпоративных стандартов и других нормативных документов заказчика.

Более подробно рассмотрим особенности внедрения ITSM [33].

Многообразие технологий внедрения ITSM является следствием комплексности соответствующих проектов, включающих в себя три взаимосвязанных, но разноплановых вида услуг — реинжиниринг процесса, создание системы автоматизации процесса, обучение участников процесса. Реинжиниринг процесса, согласно общепринятой классификации, относится к услугам, основанным на обработке информации и направленным на нематериальные активы. Создание системы автоматизации процесса является услугой, нацеленной на объекты собственности. Наконец, обучение участников процесса — это услуга, направленная на человека.

Порядок реализации каждой из этих консалтинговых услуг хорошо известен. Так, для предоставления услуги реинжиниринга процесса необходимо создать команду проекта, в которую войдут консультанты компании-исполнителя и сотрудники заказчика. Консультанты должны иметь практический опыт реализации таких проектов. Со стороны заказчика в команду рекомендуется включить менеджеров среднего звена, не находящихся друг у друга в подчинении. Они хорошо знают детали и способны увидеть картину в целом [7]. Для оказания услуги создания системы автоматизации в команду проекта должны быть включены консультанты исполнителя, имеющие практический опыт организации

подобных систем. Со стороны заказчика в команду рекомендуется включить специалистов, которые будут администрировать создаваемую систему, а также сотрудников, занимающихся системами, которые намечено с ней интегрировать. Для реализации услуги обучения исполнитель должен ввести в состав команды консультанта-преподавателя.

В материалах ITIL (Information Technology Infrastructure Library) отсутствует детальное описание порядка комплексной реализации этих относительно простых консалтинговых услуг, что приводит к различиям «составляющих» этапов внедрения ITSM разными исполнителями.

Используемые сегодня в России технологии внедрения ITSM можно разделить на три вида: технологии с акцентом на реинжиниринг процесса, на создание системы автоматизации и технологии сбалансированного типа

Технологии реинжиниринга базируются на мировых практиках успешных бизнес-процессов и включают в себя следующие шаги:

1. Обследование. Согласно практикам реинжиниринга бизнес-процессов, в начале проекта внедрения ITSM консультанты исполнителя могут не проводить обследование действующего процесса и не разрабатывать его модель («как есть»), а сразу приступить к проектированию будущего процесса.

2. Проектирование. Работа консультантов на этапе логического проектирования заключается в организации совещаний и семинаров с сотрудниками заказчика. Задачи консультантов — объяснить сотрудникам заказчика, какими должны быть проектируемый процесс (согласно рекомендациям ITIL) и роли его участников, как нужно реализовать подпроцессы, другие действия и процедуры проектируемого процесса. Чаще всего у большинства сотрудников заказчика отсутствуют практические навыки проектирования бизнес-процессов. В такой ситуации есть риск, что не весь накопленный опыт реализации действующего процесса будет учтен в процессе проектируемом.

Далее сотрудники заказчика, включенные в команду проекта, разрабатывают документы с описанием процесса, ролей его участников, зон их ответственности и основных обязанностей по реализации спроектированного

процесса. Продолжительность разработки документации и ее качество (во многом определяемое степенью соответствия требованиям стандартов ISO 20000 и ИСО 9001) зависят от наличия соответствующих навыков у сотрудников заказчика. Разработанную документацию проверяют консультанты исполнителя.

Физическое проектирование проходит аналогично логическому проектированию процесса. После семинаров, организованных консультантами, сотрудники заказчика детально проектируют процесс. Документы с результатами физического проектирования процесса, разработанные сотрудниками заказчика, как и на этапе логического проектирования, проверяются консультантами. При такой организации проектирования весьма непростым вопросом является обеспечение необходимого качества документации на спроектированный процесс. Оно определяется соответствием документации требованиям стандартов (в первую очередь, ISO 20000 и ИСО 9001), уровнем детализации, стилем изложения и другими характеристиками.

На этапе физического проектирования консультанты обычно настраивают прототип (опытный образец) системы автоматизации, обучают сотрудников заказчика работе с системой, разрабатывают план ввода решения (процесса и системы его автоматизации) в эксплуатацию. Настройка прототипа системы автоматизации проводится на стенде заказчика. Далее, как правило, прототип тестируется на соответствие разработанному процессу, корректируется ранее созданная документация на процесс и демонстрируется работоспособность прототипа сотрудникам заказчика. Обучение последних обычно представляет собой инструктаж по основным правилам работы с создаваемой системой.

3. Опытная эксплуатация**.** План ввода решения (процесса и системы его автоматизации) в эксплуатацию разрабатывается на совместных совещаниях консультантов с сотрудниками заказчика. Эти сотрудники реализуют план ввода решения в эксплуатацию, осуществляют полномасштабное развертывание системы автоматизации и проводят, при необходимости, ее опытную эксплуатацию. Консультанты могут периодически проверять ход внедрения. Для данной традиционной технологии с акцентом на реинжиниринг бизнес-процесса

характерно то, что ответственность за соблюдение сроков реализации проекта, качество документации на спроектированный процесс и за полноту использования функциональности системы (за качество реализации) полностью лежит на заказчике. В России имеются консалтинговые компании, уже реализовавшие проекты в соответствии с этой технологией, которые были оценены в СМИ как успешные. Однако по ряду причин получить объективную, критическую оценку таких проектов не представляется возможным.

Для исполнения проекта в соответствии с традиционной технологией приходится отвлекать сотрудников заказчика, вошедших в команду проекта, от исполнения их основных должностных обязанностей. Как правило, эти «дорогостоящие» сотрудники не являются специалистами по работам, проводимым в рамках проекта. Их участие в проектной деятельности является временным и имеет специфический характер. Им приходится получать множество нетипичных для постоянной деятельности знаний и навыков. Опыт их участия в проекте, как правило, в дальнейшем не находит применения. Привлечение же к проектной деятельности новых или менее «дорогих», а, следовательно, менее подготовленных сотрудников чревато низкой результативностью реинжиниринга бизнес-процесса.

Технологии, основанные на создании системы автоматизации базируются на российском опыте создания автоматизированных систем, основные положения которого изложены в ГОСТ 34-й серии. Использование данных технологий характеризуется следующими основными моментами:

1. Обследование**.** Обследование выполняется консультантами исполнителя с целью сбора данных, необходимых для ввода создаваемой системы в эксплуатацию и для обеспечения ее интеграции с другими системами. Обследование действующего процесса осуществляется при необходимости его «подгонки» под функциональность создаваемой системы автоматизации.

2. Проектирование**.** Логический и физический этапы проектирования процесса, как и обследование, осуществляются консультантами. В целом проектирование сводится к одному из двух вариантов:

- «подгонка» (изменение) действующего процесса ITSM под функциональные возможности программного продукта, на основе которого создается система автоматизации процесса;
- выбор и использование одного из наиболее подходящих шаблонов процесса, который заложен разработчиком программного продукта либо создан и реализован консультантами в предыдущих проектах.

Первый вариант проектирования связан с наибольшими рисками. В наихудшем случае, при неопытности консультантов, он даже может привести к ситуации, известной как «автоматизация хаоса». Как показывает опыт, у организаций, реализовавших проектирование по первому варианту, но решивших внедрить ITSM, возникает необходимость в дополнительных работах (которые проводятся в рамках второго варианта проектирования) или в использовании других технологий внедрения ITSM.

Второй вариант проектирования дает положительные результаты при удачном выборе консультантами шаблона процесса ITSM. Процесс управления инцидентами и система его автоматизации были адаптированы и внедрены в макрорегионах с центрами в Екатеринбурге, Твери, Самаре, Нижнем Новгороде. Обучение сотрудников было проведено на основе практической отработки ими разных сценариев реализации этого процесса с использованием системы автоматизации.

3. Опытная эксплуатация. В упомянутом выше проекте развертывание системы и ее ввод в опытную эксплуатацию были осуществлены преимущественно силами консультантов. Затем сотрудники заказчика провели в макрорегионах опытную эксплуатацию решения (процесса и системы его автоматизации). Проект был реализован в относительно короткие сроки и признан руководством ПАО «Московский кредитным банком» успешным.

При использовании технологии с акцентом на создание системы автоматизации ответственность за соблюдение сроков реализации проекта, качество документации на спроектированный процесс и за полноту использования функциональности системы (за качество реализации) практически полностью лежит

на исполнителе. При умелом выборе шаблона процесса такая технология позволяет получить положительные результаты в относительно короткие сроки.

Технология сбалансированного типа хотя и является относительно новой, но уже опробована при внедрении разных процессов ITSM. Например, по этой технологии мы реализовали проекты «Внедрение процесса управления инцидентами в Основное отличие такой технологии заключается в высоком качестве результатов проекта, которое определяется соответствием проектной документации требованиям стандартов ISO 20000, ИСО 9001 и реализованной функциональностью системы автоматизации.

Данная технология базируется на учете взаимосвязей результатов, получаемых от трех указанных типов консалтинговых услуг.

Сложность взаимосвязей результатов как услуг, так и проекта в целом свидетельствует о том, что основными условиями для достижения положительных результатов при внедрении ITSM являются: привлечение для оказания консалтинговых услуг квалифицированных консультантов, имеющих нужные навыки и опыт практической реализации таких проектов, а также качественное проведение обследования:

1. Обследование**.** При реинжиниринге любого бизнес-процесса обследование принято проводить два-три месяца с помощью двух-трех квалифицированных аналитиков. Они выполняют следующие работы:

- подготовка и планирование обследования;
- сбор информации;
- анализ полученной информации;
- корректировка плана обследования (при необходимости);
- оформление результатов обследования, в том числе разработка модели действующего бизнес-процесса.

В отечественных условиях в большинстве проектов внедрения ITSM реализовать обследование таким образом не представляется возможным в силу следующих причин. Среди них недостаток квалифицированных специалистов по ITSM с практическим опытом внедрения этого процесса, ограниченность

времени, выделяемого на обследование (как правило, не более одного месяца), большие масштабы проектов (до нескольких десятков офисов одной организации, которые могут располагаться в разных городах), большая сложность проектов внедрения ITSM, связанная с их комплексностью.

В результате требуется изменить порядок обследования так, чтобы работы, связанные с организацией и проведением обследования, были распределены между консультантами на основе ролевого принципа и с учетом общепринятого порядка реализации трех консалтинговых услуг. Организация обследования по ролевому принципу заключается в том, что все задействованные в обследовании консультанты распределяются по ролям: аналитик-планировщик, бизнес-аналитик, аналитик-системотехник, ассистент. Каждой из ролей соответствуют свои состав работ, область ответственности и требования к уровню квалификации специалистов.

Аналитик-планировщик подготавливает и планирует обследование, собирает информацию, анализирует ее, при необходимости корректирует план обследования, участвует в оформлении его результатов. Бизнес-аналитик собирает информацию о действующем процессе ITSM, его взаимосвязях с другими бизнес-процессами, в том числе ITSM, анализирует собранную информацию, при необходимости формирует предложения по корректировке плана обследования, оформляет документацию с его результатами. Аналитик-системотехник собирает информацию об имеющихся системах, средствах автоматизации действующего процесса ITSM и других автоматизированных системах, которые могут быть использованы как источники информации для системы автоматизации внедряемого процесса ITSM. Он анализирует собранную информацию, при необходимости формирует предложения по корректировке плана обследования, оформляет документацию с его результатами. Ассистент собирает информацию о действующем процессе ITSM, имеющихся системах или средствах его автоматизации, о других автоматизированных системах, помогает бизнес-аналитикам и аналитикам-системотехникам оформлять документацию с результатами обследования.

Порядок обследования по ролевому принципу предусматривает те же основные работы, которые проводятся при общепринятом порядке обследования. При подготовке и планировании обследования нужно получить исходную информацию для обследования, уточнить состав сотрудников организации и вопросы для проведения опроса, разделить объект обследования (то есть действующий процесс ITSM, автоматизированные системы и средства автоматизации, используемые при его реализации) на логические секторы. Такое разделение и распределение секторов между консультантами нужно осуществлять исходя из особенностей предметной области и состава привлекаемых к обследованию консультантов. Планирование работ предполагает составление плана обследования и его согласование с руководством ИТ-подразделения организации.

Сбор информации включает в себя сбор документов по действующему процессу ITSM, автоматизированным системам и средствам автоматизации, используемым при его реализации, опрос сотрудников ИТ-подразделения и документирование его результатов. Анализ полученной информации подразумевает рассмотрение данных с точки зрения основных составляющих действующего процесса ITSM (подпроцессов, функций, действий и т.п.), описание источников данных для системы автоматизации внедряемого процесса, при необходимости — составление списков уточняющих вопросов и запрашиваемой документации.

В процессе корректировки плана обследования нужно уточнить перечень сотрудников ИТ-подразделения, подлежащих опросу, сроки и объем опроса (с учетом возможности появления дополнительных, уточняющих вопросов и, соответственно, увеличения времени опроса). При оформлении результатов обследования должны быть разработаны документы с описанием модели действующего процесса ITSM, автоматизированных систем и средств автоматизации, которые используются при реализации действующего процесса и могут служить источниками данных для внедряемого процесса. Кроме того, учитываются пожелания сотрудников ИТ-подразделения по поводу внедряемого процесса ITSM и системы его автоматизации.

Такой порядок организации и проведения обследования позволил нам в упомянутых проектах осуществить обследования с требуемым качеством. Были привлечены консультанты с разными уровнями квалификации. Сроки обследования, по сравнению с общепринятыми, сократились. Повысилась эффективность работы квалифицированных консультантов по ITSM (они могли быть задействованы одновременно в нескольких проектах), повысилась заинтересованность консультантов в профессиональном росте. По ролевому принципу строится работа консультантов исполнителя и на других этапах внедрения ITSM.

2. Проектирование**.** Работа консультантов на этапе проектирования заключается не только в проведении семинаров и совещаний с сотрудниками заказчика, но и в подготовке документов с результатами проектирования процесса, в обсуждении и согласовании результатов проектирования с сотрудниками заказчика. Такие обсуждение и согласование проводятся как на совместных семинарах и совещаниях, так и в рабочем порядке, то есть с отдельными сотрудниками исполнителя.

На этапе физического проектирования консультанты настраивают прототип (опытный образец) системы автоматизации на стенде заказчика, тестируют и демонстрируют работоспособность прототипа сотрудникам заказчика. С участием последних система развертывается и подготавливается к опытной эксплуатации. Перед ее началом консультанты проводят углубленное обучение, подразумевающее практическую отработку участниками процесса разных сценариев реализации спроектированного процесса с использованием системы его автоматизации.

3. Опытная эксплуатация**.** Опытную эксплуатацию решения (процесса и системы его автоматизации) проводит заказчик. При этом присутствуют консультанты, которые при необходимости помогают сотрудникам заказчика и обучают некоторых из них на рабочих местах.

При использовании технологии сбалансированного типа ответственность за соблюдение сроков проекта делится поровну между исполнителем и заказчиком проекта, а ответственность за качество проектной документации и полноту

использования функциональности системы (за качество реализации) принимает на себя исполнитель. Данная технология позволяет заказчику получить проектную документацию, в полной мере соответствующую требованиям ISO 20000 и ИСО 9001, а также полнофункциональную систему автоматизации внедряемого процесса ITSM.

2.4. «OMNITRACKER ITSM Center» как оптимальный программный продукт для внедрения в организацию

В разделе 2.2 был произведен сравнительный анализ текущих ITSM систем, представленных на Российском рынке, в результате ПАО «Московский кредитный Банк», было принято решение о внедрении OMNITRACKER ITSM Center, который отвечает поставленным задачам в банке.

OMNITRACKER ITSM Center является сертифицированным инструментом для автоматизации процессов ITSM, основанным на стандарте де-факто «IT Infrastructure Library» (ITIL). Он обеспечивает не только управление ИТ услугами (IT Service Management), но также структуризацию и оптимизацию других процессов ИТ организаций [34]. Процессы систематизируются, их основные показатели контролируются для обеспечения качества. Благодаря своей масштабируемости и гибкости OMNITRACKER ITSM Center может быть использован для реализации процессов ITSM в ИТ организациях самого разного масштаба — от внутреннего отдела ИТ небольшой компании до крупных международных концернов с необходимостью управления как внутренними, так и внешними поставщиками ИТ услуг (рис. 2.1).

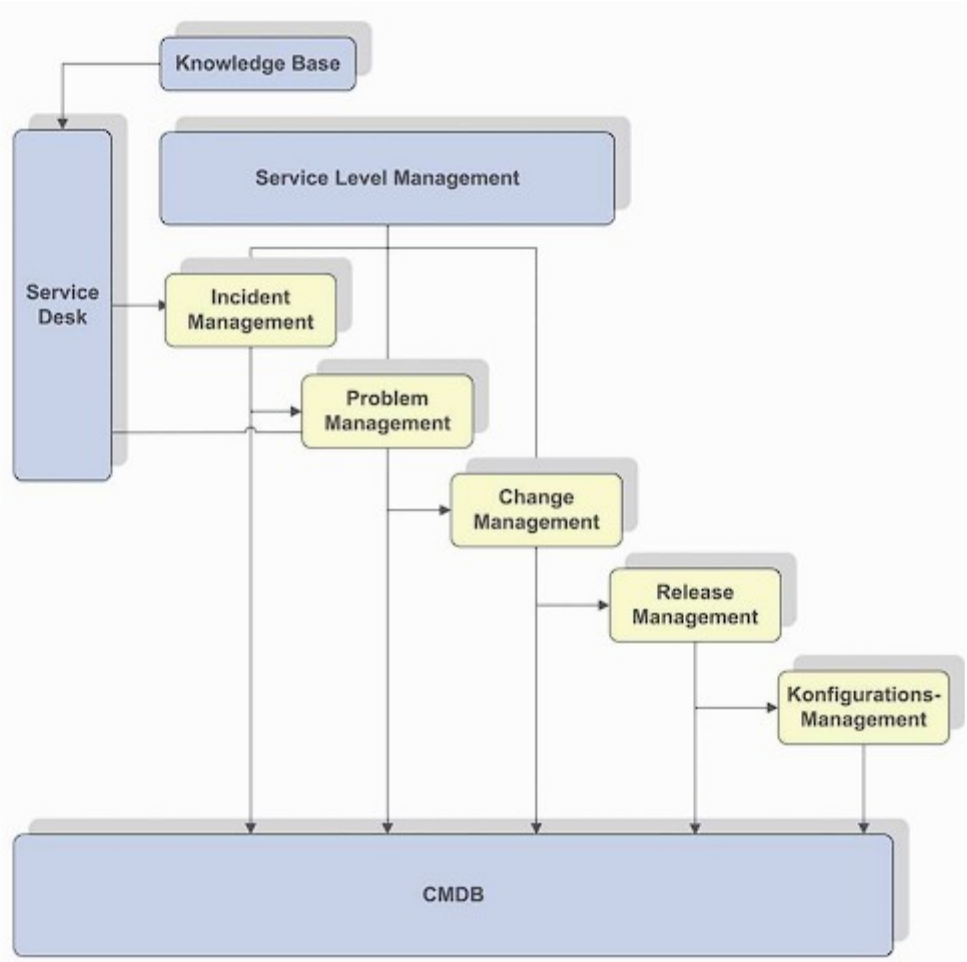

Рис. 2.1. Взаимодействие в omnitraker

Являясь инструментом для автоматизации процессов ITIL/ITSM, сертифицированным компанией Pink Elephant, OMNITRACKER ITSM Center объединяет все основные процессы IT Service Management в одном приложении и допускает расширение функционала в соответствии с требованиями поставщика ИТ услуг. Тем самым, он обеспечивает поэтапное внедрение и миграцию процессов ITSM на предприятии — от управления инцидентами (Incident Management) до полноценной реализации остальных процессов ITSM. Благодаря прозрачности всех процессов внедрение OMNITRACKER ITSM Center повышает эффективность исполнения и контроля процессов ITSM. Консолидированные отчёты для оценки показателей производительности (KPI) помогают добиться постоянного совершенствования процессов и повышения качества ИТ услуг.

Рассмотрим общий вид пользовательский интерфейса (рис. 2.2):

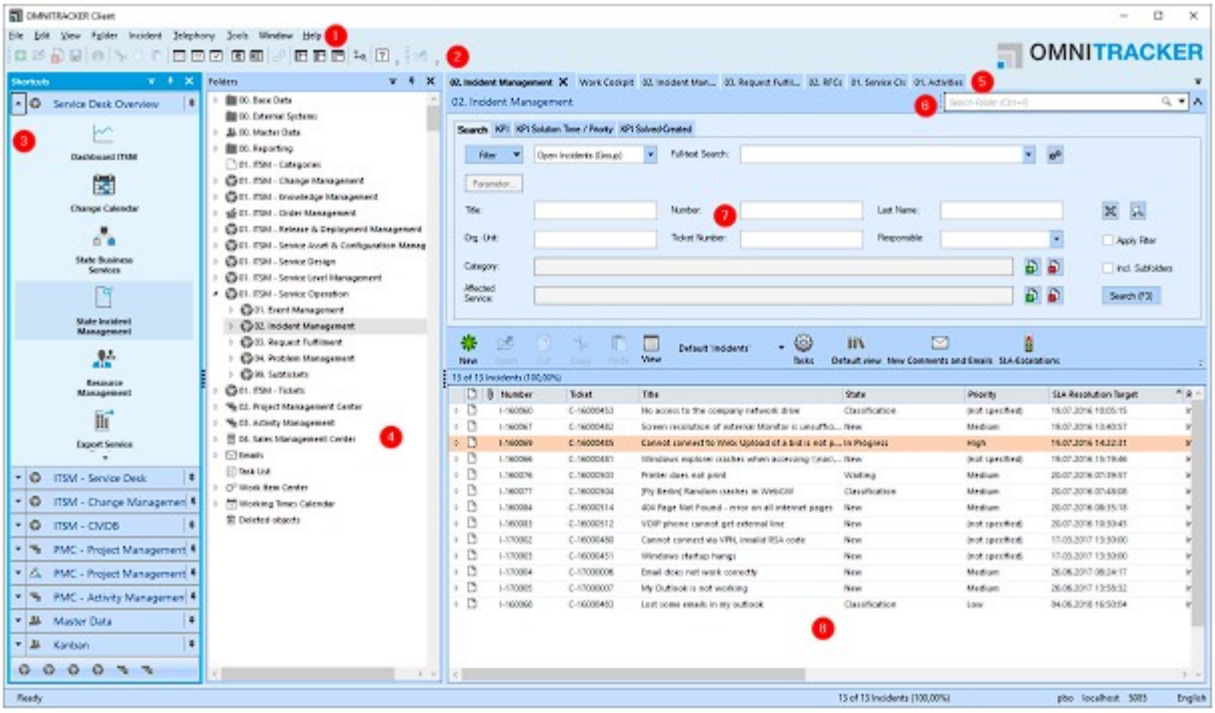

Рис 2.2. Пользовательский интерфейс

1. Строка меню обеспечивает быстрый доступ к основным настройкам OMNITRACKER, которые могут быть кастомизированы при необходимости.

2. Панель инструментов обеспечивает быстрый доступ к важным функциям.

3. Панель быстрого запуска позволяет получить доступ к сохраненным функциям, таким как объекты, папки, задачи и файлы. Она может быть свободно изменена и расширена авторизованным пользователем.

4. Дерево папок содержит папки, которые отображаются в базе данных OMNITRACKER виде структуры дерева. В дереве папок также используется навигация.

5. Программа может открывать несколько объектов параллельно как вкладка/вкладки. Открытая в данный момент вкладка будет выделена.

6. При помощи поля поиска можно легко найти объекты OMNITRACKER (поиск по категориям и полнотекстовый поиск).

7. Форма поиска предлагает широкие возможности различных типов поисковых запросов:

- фильтры (выберите существующие фильтры или создайте новые);

- полнотекстовый поиск (поиск по индексированным полям или файлам);
- поле поиска.

8. В списке объектов отображаются только те объекты, которые находятся в выбранной папке и доступны для просмотра текущему пользователю. При помощи настройки вида может быть выбрано не только отображение списком, но и другие варианты вида (например, календарь или временная шкала).

Наряду с процессами IT Service Management OMNITRACKER обеспечивает возможность реализации процессов ERP и их интеграции с процессами ITSM, такими как:

- управление лицензиями;
- управление заказами;
- управление проектами;
- управление продажами.

Основные характеристики OMNITRACKER ITSM Center представлены в таблице 2.3

Таблица 2.3

Характеристики OMNITRACKER ITSM Center

Общее	**Планирование и управление**	**Обработка и контроль**	**Представление и отображение**
Сертификация Pink Verify Service Support Enhanced (ITIL v2) Быстрый ввод сбоев, запросов и заказов Эффективная командная работа и коммуникации Управление и совершенствование процессов ITSM Эффективное использование ресурсов	ИТ услуги создаются в соответствии с требованиями клиентов и предоставляются на основании контрактов Структурированное управление и администрирование данных о клиентах Стандартизированное планирование, внедрение и контроль изменений CMDB для управления всеми компонентами, их взаимосвязями и зависимостями База знаний с функцией полнотекстового поиска	Планирование, сборка, тестирование и развертывание релизов в соответствии с ITIL Единая точка контакта по вопросам поддержки с возможностью обращения по телефону, электронной почте или через Web-портал Учёт затрат в разрезе задач Объединение взаимосвязанных обращений Администрирование предоставляемых сервисов Определение требований к времени исполнения задач и восстановления ИТ услуг Учет любых типов CI (Configuration Item) Мониторинг предоставляемых ИТ услуг Контроль и оптимизация прямых расходов	Встроенные отчеты для измерения KPI и гибкая подсистем формирования отчетов Процессные показатели в режиме реального времени (Dashboards) Отображение зависимостей и взаимосвязей Прозрачность всех процессов

Процессы ITSM в продукте OMNITRACKER ITSM Center: управление инцидентами, управление проблемами, управление конфигурациями, управление изменениями, управление релизами, управление уровнем ИТ услуг

Данные об организациях и пользователях очень важны для взаимодействия между поставщиками ИТ услуг и их клиентами. OMNITRACKER ITSM Center обеспечивает полноценное управление данными о клиентах, включая учет компаний, стран, адресов, центров затрат и отдельных пользователей.

Задачей процесса управления инцидентами является максимально быстрое восстановление согласованного уровня ИТ услуг после сбоя. Влияние инцидентов на бизнес-процессы должно быть сведено к минимуму. OMNITRACKER ITSM Center обеспечивает быстрый ввод инцидентов и обращений пользователей, которые классифицируются, обрабатываются, контролируются и закрываются службой Service Desk. Обращения могут приниматься по телефону, SMS, электронной почте, факсу или через Web. В зависимости от способа передачи, обработка обращений осуществляется автоматически или вручную.

Процесс управление проблемами позволяет предотвратить или, как минимум, ограничить негативное влияние ошибок, инцидентов и проблем на ИТ услуги. Для этого требуются как проактивные, так и реактивные меры. Проблема — это корневая причина, лежащая в основе одного или нескольких инцидентов. После определения причины и обходного решения вызванных ей инцидентов (Workaround) или нахождения постоянного решения, проблема становится известной ошибкой (Known error). OMNITRACKER ITSM Center организует обработку проблем в два этапа: контроль проблем (Problem control) и контроль ошибок (Error control). В процессе обработки сначала выполняется регистрация проблем, в большинстве случаев на основании инцидентов. При этом проблема создается не посредством эскалации существующего инцидента, а как отдельный объект с целью определения причины инцидентов. OMNITRACKER ITSM Center интегрирует процессы управления инцидентами и проблемами, позволяя связы-

контролировать статус обработки инцидентов, связанных с данной проблемой и наоборот.

База знаний OMNITRACKER ITSM Center поддерживает процессы ITSM, предоставляя и обеспечивая поиск информации: о стандартных решениях для управления инцидентами об известных ошибках для управления проблем набор описаний, статей, предложений и документов, позволяющий быстро находить ответы на вопросы пользователей. Поиск необходимых данных обеспечивает высокопроизводительная система полнотекстового поиска.

Процесс управления конфигурациями контролирует все конфигурационные единицы (CI, Configuration Item) — ИТ услуги, системы и приложения, компоненты. При этом должны регистрироваться, определяться, описываться и проверяться все CI с их взаимосвязями и зависимостями. Учет информации выполняется в единой базе данных всех управляемых компонентов (CMDB, Configuration Management Database). Важным условием результативности управления конфигурациями является гарантированное предоставление другим процессам ITSM — процессу управления инцидентами, процессу управления изменениями и другим — точной информации об ИТ инфраструктуре. CMDB в OMNITRACKER ITSM Center обеспечивает единый подход для описания любых CI с настраиваемым набором характерных атрибутов. Описание CI может в любой момент свободно расширяться, обеспечивая реализацию текущих и будущих потребностей. Для отображения физических и логических связей элементов ИТ инфраструктуры используются связи между CI в CMDB. Существующие связи представляются графически и в виде детальных перечней (рис. 2.3).

В связи с быстрым развитием информационных технологий управление изменениями становится критическим фактором успеха. Требования бизнеса, новые технологии, потребности пользователей должны быстро и контролируемо внедряться в жизнь. Процесс управления изменениями определяет единые процедуры внесения изменений эффективно и с минимальными последствиями для бизнеса. В OMNITRACKER ITSM Center могут автоматически регистрироваться все поступающие из различных источников запросы на изменения RFC (Request

For Change), например, требования из процессов управления инцидентами или проблем, а также требования, поступающие непосредственно от заказчиков. Запросы на изменения регистрируются в стандартной форме и одобряются или отклоняются в рамках процесса управления изменениями. Принятый запрос на изменение классифицируется по приоритетности, поступает на разработку, а затем на тестирование. В случае успешного тестирования изменение внедряется в эксплуатацию. После реализации изменения выполняется заключительная оценка его результативности и эффективности. OMNITRACKER ITSM Center поддерживает все типы запросов на изменение:

- базовое изменение (Basic change);
- стандартное изменение (Standard change);
- срочное изменение (Urgent change).

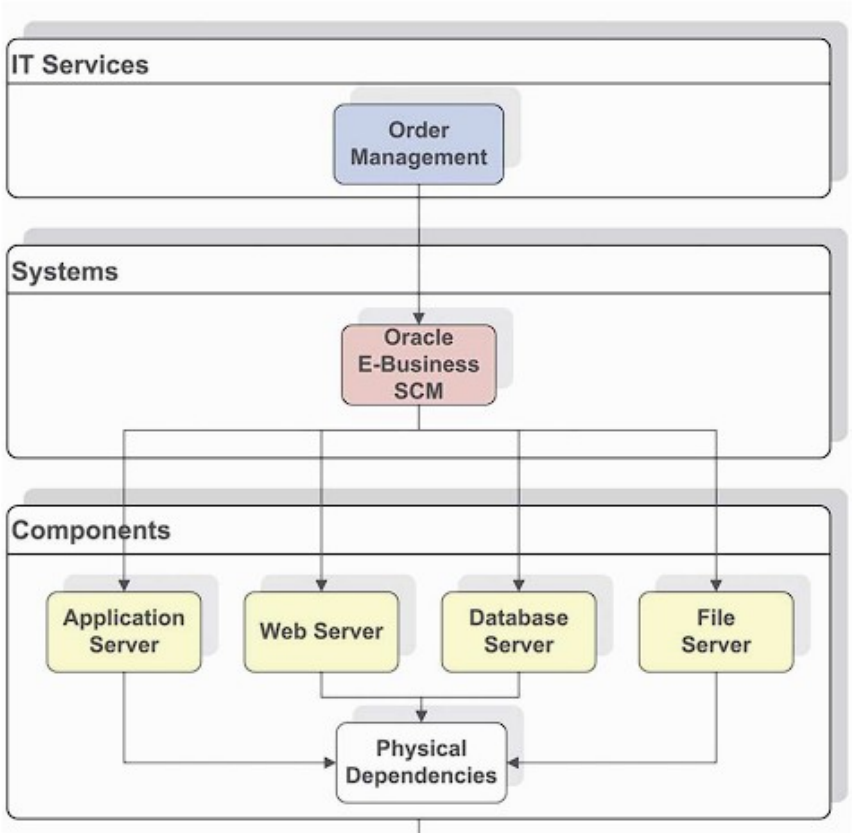

Рис. 2.3. Физические и логические связи элементов ИТ инфраструктуры

В зависимости от типа выбирается соответствующая процедура обработки. В случае стандартного изменения — например, замена клавиатуры —

изменение может быть реализовано немедленно и, в целях оптимизации ресурсов, без сложных согласований.

Аналогично процессу управления изменениями, процесс управления релизами направлен на качественное предоставление ИТ услуг. Растущее число отдельных изменений должно оставаться под контролем. Это обеспечивается точным планированием. В то время, как процесс управления изменениями планирует и контролирует внедрение новых элементов, управление релизами обеспечивает оперативное внедрение. Так как изменения касаются CI, необходима интеграция с процессом управления конфигурациями. Управление релизами получает детальную информацию о подлежащих изменению CI из CMDB. После внесения изменений (Rollout) необходимо выполнить обновление данных CMDB. OMNITRACKER ITSM Center поддерживает планирование, компоновку, тестирование и развертывание различных типов релизов — Full, Delta и Package. После успешного выпуска планируемые изменения автоматически вносятся в CMDB. Если в результате серьезной ошибки потребуется прекращение работы над релизом и возврат в исходное состояние, все изменения в CI автоматически аннулируются.

В рамках процесса управления уровнем услуг выполняется учет и обработка запросов на новые услуги, подготовка предложений новых или измененных ИТ услуг, определение состава услуг и заключение с клиентами соглашений о уровне услуг (SLA). Одной из задач этого процесса является также контроль и оценка качества — соответствия фактического уровня предоставляемых услуг согласованным SLA. OMNITRACKER ITSM Center поддерживает учет предложений услуг в Каталоге услуг. На основе записей в каталоге услуг ведутся переговоры и заключаются контракты. Обеспечивается управление следующими типами контрактов: соглашения об уровне услуг (SLA), договоры об операционном уровне (OLA) и внешние контракты (UC). В зависимости от типа объекта (инцидент, проблема, RFC) и его приоритета в OMNITRACKER ITSM Center могут устанавливаться и контролироваться определенные контрактом сроки реагирования, прибытия на место работ, выполнения работ. Для оценки качества услуг

в отчёты о предоставлении ИТ услуг включаются необходимые значения и контрольные показатели.

Управление работами в рамках процессов ITSM обеспечивает эффективное использование имеющихся ресурсов путём планирования работ с учетом приоритетов, времени и персонала. Для управления работами OMNITRACKER ITSM Center позволяет регистрировать задания и вести детальный учёт трудозатрат и расходов на их выполнение.

Качество предоставляемых ИТ услуг наглядно оценивается по показателям качества и метрикам (KPI). Отчеты по KPI являются основой для оценки возможностей поставщика услуг и помогают выявить способы улучшения работы. OMNITRACKER ITSM Center предлагает большой выбор готовых форм отчетов по KPI процессов ITSM. Готовые отчеты могут очень просто и гибко адаптироваться к специфическим требованиям организаций. Наряду с формированием отчетов за произвольные периоды времени OMNITRACKER ITSM Center может предоставлять отчеты о работе процессов управления ИТ сервисами в режиме реального времени.

III. ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

Проведем расчёт показателей экономической эффективности ITSM.

После проведенного исследования, было установлено, что 45% инцидентов, происходящих на рабочих местах пользователей, требуют выхода инженера на место инцидента для сбора информации об оборудовании, установленном ПО, сети и т.п. Возможность получить такую информацию непосредственно с рабочего места инженера позволяет снизить затраты на устранение инцидента в среднем на 25% [35].

Таким образом за счет экономии рабочего времени пользователей и технических специалистов внедрение ITSM позволило ощутимо сократить как издержки, связанные с устранением инцидентов, так и прямые затраты на восстановление работоспособности ИТ-инфраструктуры благодаря своевременному выявлению потенциальных источников инцидентов[36].

Рассмотрим расчеты до внедрения ITSM и после внедрения.

До внедрения:

- В штате ИТ-службы поддержки Банка работает 20 человек.
- Средняя заработная плата специалиста ИТ-службы поддержки составляет 25 000 рублей.
- Количество пользовательских рабочих мест в компании — 1000.
- Среднее количество инцидентов в месяц — 750.
- Среднее время, которое специалист тратит на решение одного инцидента: 4 часа.

В таком случае мы получаем (рис. 3.1):

- Стоимость обслуживания 1 рабочего места в месяц: (20×25 000)/1000 = 500 рублей.
- количество заявок, требующих выхода на место инцидента: 750×0,45 = 337 ед.

- Суммарное время на решение инцидентов (до внедрения): 337×4 = 1348 часов.
- Экономия времени при внедрении на решение одного инцидента: 4×0,25 = 1 час.
- Экономия времени по всем инцидентам за месяц: 337×1 = 337 часов.
- Один час работы специалиста стоит 25000/176 = 142 рублей.
- Стоимость устранения инцидентов (до внедрения): 1348×142 = 191 416 рублей в месяц, и 2 296 992 рублей в год соответственно.
- Сокращение затрат за счет внедрения ITSM: 142×337 = 47 854 рублей в месяц, что за год составит 47 854×12 = 574 248 рублей**.**

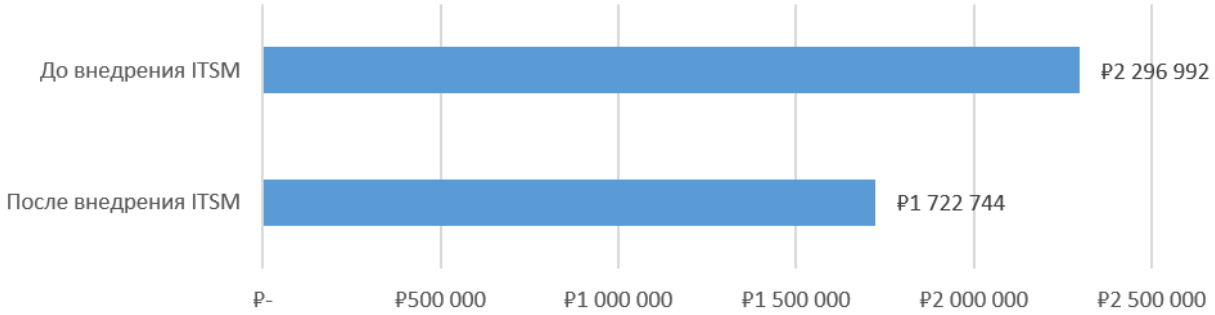

Рис. 3.1. Сокращение затрат на устранение инцидентов при внедрении ITSM

Из проделанных вычислений можно сделать вывод, что экономический эффект достигается за счет высвобождения части трудовых и финансовых ресурсов, получаемых от:

1. Снижения трудозатрат на устранение инцидентов.
2. Снижения времени на решение инцидентов.
3. Снижения стоимости устранения инцидентов.

ЗАКЛЮЧЕНИЕ

В рамках впускной квалификационной работы бы ли достигнуты следующие результаты согласно поставленным задачам:

- проведён организационно-экономический анализ деятельности ПАО «Московский кредитный Банк»;
- проанализирована степень эффективности внедрения;
- произведено описание существующих средств управления ITSM;
- приведено организационно-экономическое обоснование внедрения ITSM.

По результатам работы можно сделать вывод:

ITSM — это непрерывный процесс, который пронизывает все направления бизнеса и работы, над которым не останавливаются никогда, единожды начавшись. Правильный подход к внедрению, выбор платформы и компании консультанта-интегратора, позволят достичь поставленного результат и организовать эффективное и удобное управление ИТ.

В отличие от более традиционного технологического подхода, ITSM рекомендует сосредоточиться на клиенте и его потребностях, на услугах, предоставляемых пользователю информационными технологиями, а не на них самих. При этом процессная организация предоставления услуг и наличие заранее оговоренных в «Соглашениях об уровне услуг» параметров эффективности позволяет IT-подразделениям предоставлять качественные услуги, измерять и улучшать их качество.

Неотъемлемой частью процессной организации по ITSM является Service Desk — подразделение (в терминологии ITIL «функция»), обеспечивающее единую и единственную точку входа для всех запросов конечных пользователей и унифицированную процедуру обработки запросов. Зачастую внедрение процессного подхода к предоставлению услуг начинается именно с внедрения функции Service Desk.

Приоритетными направлениями в управлении ИТ в банках, являются поддержка критично важных для банков бизнес-процессов, обеспечиваемых средствами ИТ; оптимизация и повышение эффективности банковской ИТ-инфраструктуры; разумные инвестиции в технологии и решения, непосредственно ориентированные на получение прибыли от клиентов и развитие бизнеса в среднесрочной перспективе.

Управление работами в рамках процессов ITSM обеспечивает эффективное использование имеющихся ресурсов путём планирования работ с учетом приоритетов, времени и персонала.

Внедрение ITSM — это сравнительно дорогостоящий процесс, в нем задействовано большое число человеческих и материальных ресурсов. Полагаться в этом только на внутренние резервы ИТ-подразделения ошибочно, необходимо четко обосновать перед бизнесом финансовую целесообразность и окупаемость проекта, чтобы получить бюджет на внедрение.

Основными преимуществами внедрения ITSM для ПАО «Московский кредитный Банк» стало: организация эффективной деятельности ИТ-подразделения за счет использования процессов, описанных в ITIL (управление инцидентами, конфигурациями, проблемами, изменениями, уровнем обслуживания); повышение надежности и стабильности услуг ИТ (управление мощностью и доступностью); финансовая прозрачность деятельности ИТ (управление финансами ИТ).

Внедрение ITSM нужно не только ИТ, но и бизнесу. С внедрением процессной модели работа ИТ-подразделения становится прозрачной и понятной бизнесу. Когда руководство видит, какие услуги оказывает ИТ-отдел, становится проще оценивать эффективность его работы и планировать бюджет на его содержание. Для рядовых сотрудников компании внедрение ITSM обеспечивает более высокое качество предоставления услуг, быструю реакцию на возникающие проблемы, работу без простоев и гарантированные сроки исполнения запросов.

Таким образом поставленные в работе цели и задаче поставленные в работе были выполнены в полном объеме.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. «Банк России» // URL: https://cbr.ru/banking_sector/credit/coinfo/?id=450000226

2. «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (официальный сайт) // URL: https://mkb.ru/about

3. Википедия Публичное акционерное общество «Московский кредитный банк» // URL: https://ru.wikipedia.org/wiki/Московский_кредитный_банк

4 Консультант Плюс ГК РФ ПАО статья 97 // URL: https://www.consultant.ru/document/cons_doc_LAW_5142/6c23b984e7fc78fbe96d6ed767f0ae3795005169/.

5. Коммерческая структура Банка // URL: https://brobank.ru/kommercheskij-bank/

6. Управление Банком и его структура // URL: https://spravochnick.ru/bankovskoe_delo/upravlenie_bankom_i_ego_struktura/

7. Принципы деятельности в управлении Банком // URL: https://www.sinref.ru/000_uchebniki/00800economica/000_lekcii_bank_01_raznoe_/784.htm

8.Банки ру. Московский кредитный Банк // URL: https://www.banki.ru/banks/bank/mkb/tver~/

9.Банки ру финансовая отчётность ПАО «Московский кредитный Банк» // URL: https://www.banki.ru/banks/ratings/?BANK_ID=7292&date1=2022-02-01&date2=2022-01-01

10. SWOT анализ // URL: https://studbooks.net/1395803/menedzhment/swot_analiz

11. SWOT анализ на примере организации // URL: https://neiros.ru/blog/marketing/swot-analiz-ehlementy-strategii-primery/

12. ITSM система подход к внедрению // URL:https://www.azone-it.ru/itsm

13. Никишин М.Е. Обоснование использования методологии ITIL/ITSM в управлении ИТ-службы коммерческого банка // URL:https://journal.itmane.ru/node/411

14. Чеботарева, Г. С. Организация деятельности коммерческого банка: учеб. пособие / Г. С. Чеботарева ; М-во образования и науки Рос. Федерации, Урал. федер. ун-т. — Екатеринбург : Изд-во Урал. ун-та, 2018. — 120 с.

15. Способы приобретения ИС// URL: https://knigi.studio/tehnologii-menedjmente-informatsionnyie/kakie-suschestvuyut-sposobyi-156461.html

16. Обоснование проектных решении // URL: https://prog.bobrodobro.ru/75328

17. Сидорова, Н.П. Информационное обеспечение и базы данных: практикум по дисциплине «Информационное обеспечение, базы данных» / Н.П. Сидорова, Г.Н. Исаева, Ю.Ю. Сидоров; Технологический университет. — Москва; Берлин: Директ-Медиа, 2019. — 85 с.

18. Басыня, Е.А. Системное администрирование и информационная безопасность : учебное пособие : / Е.А. Басыня ; Новосибирский государственный технический университет. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с.

19. ITSM // Свободная энциклопедия «Википедия» // URL: https://ru.wikipedia.org/wiki/ITSM

20. ITIL // Свободная энциклопедия «Википедия» // URL: https://ru.wikipedia.org/wiki/ITIL

21. Книги библиотеки ITIL // URL: https://helpiks.org/7-85258.html

22. ГОСТ Р ИСО/МЭК 20000 «Информационная технология. Менеджмент услуг».

23. Жиляев А.Ю. Управление IT проектами в банковской сфере // Гуманитарные научные исследования. — 2020. — № 9 [Электронный ресурс]. URL: http://human.snauka.ru/2020/09/28444

24. Артюшина, Л.А. Управление ИТ-сервисами и контентом : учеб. пособие / Л А. Артюшина, Е.А. Троицкая; Владим. гос. ун-т им. А.Г. и Н.Г. Столетовых. — Владимир: Изд-во ВлГУ, 2021. — 280 с.

25. Как не надо внедрять ITSM// URL: https://it-guild.com/info/blog/kak-ne-nado-vnedryat-itsm-v-kompanii-2/

26. Информационная банковская безопасность и ее необходимость // URL:https://finexpert24.ru/poleznye-materialy/articles/bankovskaya deyatelnost/informatsionnaya-bankovskaya-bezopasnost-i-ee-neobhodimost/

27. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ.

28. ГОСТ Р ИСО/МЭК 15408–1–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

29. ГОСТ Р ИСО/МЭК 15408–2–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

30. ГОСТ Р ИСО/МЭК 15408–3–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

31. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи: учебник / Б.И. Филиппов, О.Г. Шерстнева. — Москва; Берлин: Директ-Медиа, 2019. — 241 с.

32. Сравнение ITSM систем //
URL: https://habr.com/ru/companies/icl_services/articles/352196/

33. Внедрение ITSM для начинающего //
URL: http://alib.spb.ru/blog/page/article-135

34. ITSM centr omnitracer// URL:
https://www.omnitracker.com/ru/produkty/prilozheniya/it-service-management-center/#

35. Градусов, Д. А. Управление информационными системами в экономике : учеб.-практ. пособие / Д.А. Градусов, А.В. Шутов; Владим. гос. ун-т им. А.Г. и Н.Г. Столетовых. — Владимир: Изд-во ВлГУ, 2019. — 99 с.

36. Экономическое обоснование внедрения ITSM // URL: https://www.inframanager.ru/library/about-methodology/feasibility-study-implementation-itsm/