

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

Кафедра _____

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА – ДИПЛОМНАЯ РАБОТА

НА ТЕМУ: Внедрение средства управления ITSM для ПАО «Московский Кредитный Банк»

ФИО обучающегося: _____

Группа: _____

ФИО Руководителя: _____

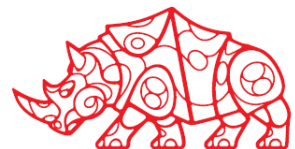


Актуальность, объект и предмет исследования

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.

Объект исследования – информационные технологии по обслуживанию клиентов банка.

Предмет исследования – современные пути удовлетворение потребностей бизнеса и поддержки ИТ-инфраструктуры коммерческого банка.

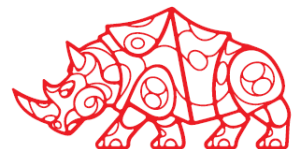


ЦЕЛЬ И ЗАДАЧИ

Цель исследования – провести исследование, на что повлияло внедрение средства управления ITSM в ПАО «Московский кредитный банк».

Задачи исследования:

- 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.

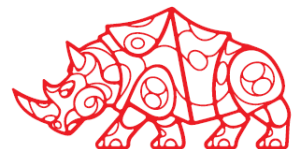


Процессы ITSM

Название процесса	Цель процесса
Управление инцидентами	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	Организация процесса направлена на уменьшение количества инцидентов, за счет выявления и устранения причин возникновения инцидентов.
Управление конфигурациями	Процесс заключается в создании и поддержании в актуальном состоянии логической модели инфраструктуры компании
Управление изменениями	Целью процесса является организация проведения изменений с наименьшим риском возникновения инцидентов, вызванных изменениями
Управление релизами	Цель процесса — обеспечение работоспособности производственной среды при внедрении изменений
Управление уровнем сервиса	Цель процесса — выявить состав и уровень сервиса на основании требования потребителей и поставщиков ИТ-сервисов, контролировать достижение установленного уровня сервиса
Управление финансами	Цель процесса заключается в обеспечении стабильного финансирования всех прочих процессов
Управление мощностью	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	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
Управление доступностью	Процесс включает в себя обеспечение согласованного уровня доступности сервиса, а также оценку текущей доступности сервиса и планирование действий, направленных на ее дальнейшее улучшение

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.

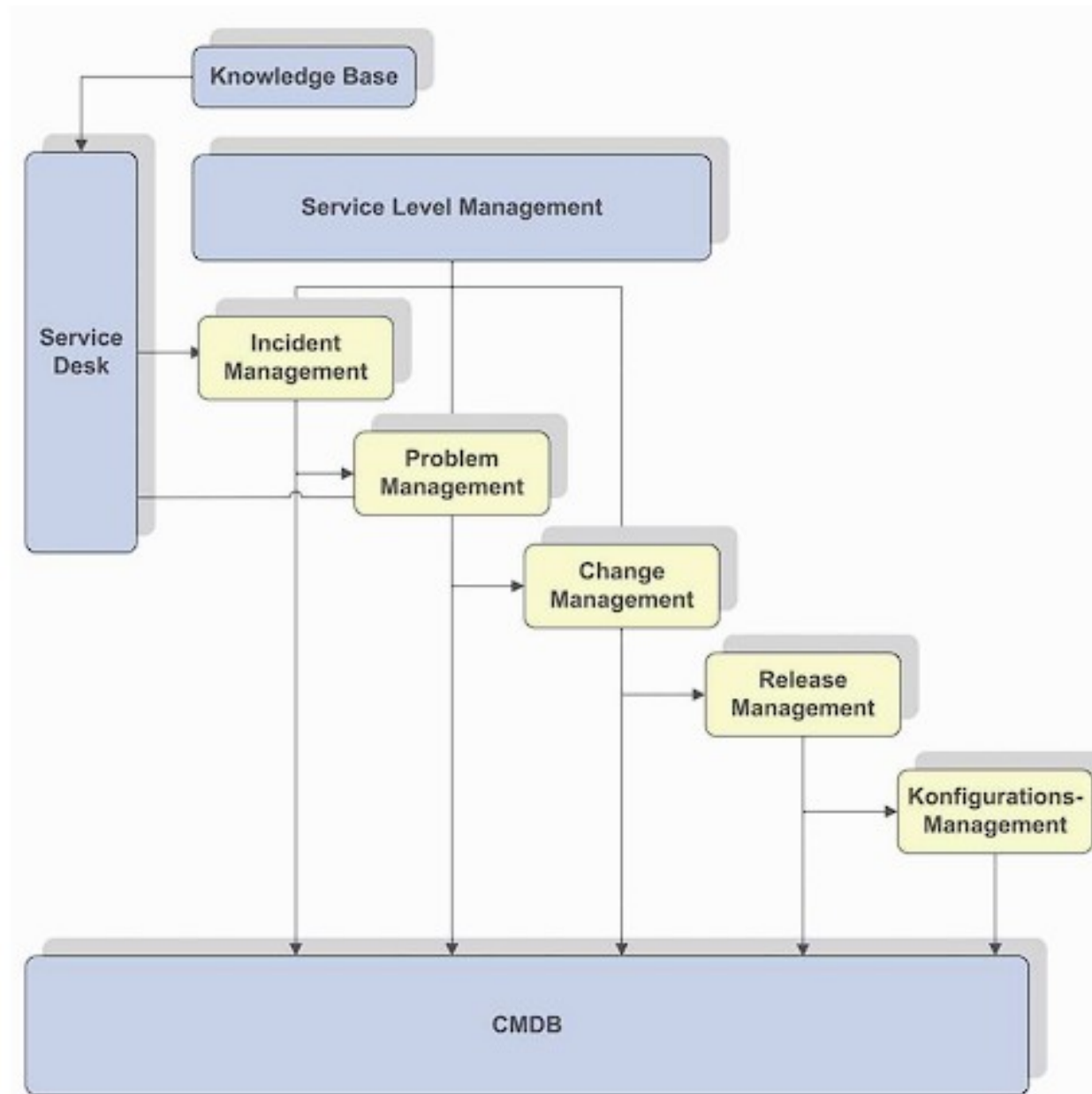


Сравнительная характеристика показателей распространенных ITSM-систем

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



Взаимодействие в omnitraker



Пользовательский интерфейс

The screenshot displays the OMNITRACKER Client application window. The interface is divided into several sections:

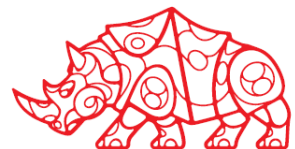
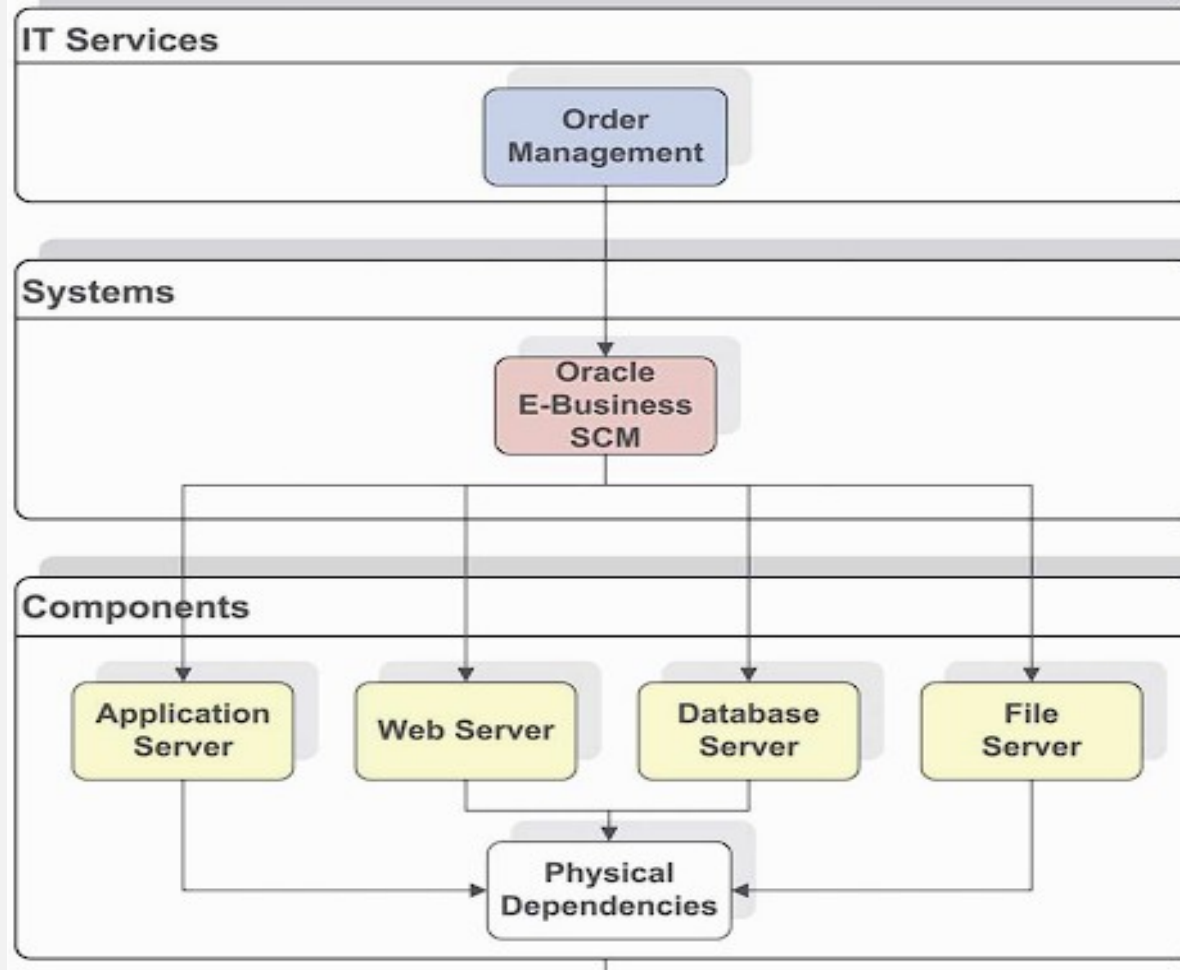
- Top Menu:** File, Edit, View, Folder, Incident, Telephony, Tools, Window, Help. (Callout 1 points to the Help menu).
- Toolbar:** Contains icons for various actions like New, Open, Print, etc. (Callout 2 points to the toolbar).
- Left Sidebar:** Contains a 'Shortcuts' section with icons for Service Desk Overview, Dashboard ITSM, Change Calendar, State Business Services, State Incident Management, Resource Management, and Export Service. (Callout 3 points to the Service Desk Overview icon).
- Folder Tree:** A hierarchical list of folders on the left side, including 00. Back Data, 00. External Systems, 00. Master Data, 00. Reporting, 01. ITSM - Categories, 01. ITSM - Change Management, 01. ITSM - Knowledge Management, 01. ITSM - Order Management, 01. ITSM - Release & Deployment Management, 01. ITSM - Service Asset & Configuration Management, 01. ITSM - Service Design, 01. ITSM - Service Level Management, 01. ITSM - Service Operation, 01. Event Management, 02. Incident Management (selected), 03. Request Fulfillment, 04. Problem Management, 05. Subscribers, 01. ITSM - Tickets, 02. Project Management Center, 03. Activity Management, 04. Sales Management Center, Emails, Task List, Work Item Center, Working Times Calendar, and Deleted objects. (Callout 4 points to the 02. Incident Management folder).
- Main Content Area:**
 - Incident Management Header:** Includes a search bar with 'Search Folder (Ctrl+F)' and a search button. (Callout 5 points to the search bar).
 - Search Filters:** Includes a 'Filter' dropdown, 'Open Incidents (Simple)', and a 'Full-text Search' field. (Callout 6 points to the search filters).
 - Form Fields:** Includes fields for Title, Number, Last Name, Org. Unit, Ticket Number, Responsible, Category, and Affected Service. (Callout 7 points to the Number field).
 - Buttons:** Includes buttons for 'Apply Filter' and 'Incl. Subfolders'. (Callout 8 points to the 'Search (F3)' button).
 - Table:** A table listing incidents with columns: Number, Ticket, Title, State, Priority, and SLA Resolution Target. The table shows 15 incidents, with the first one highlighted. (Callout 8 points to the table).



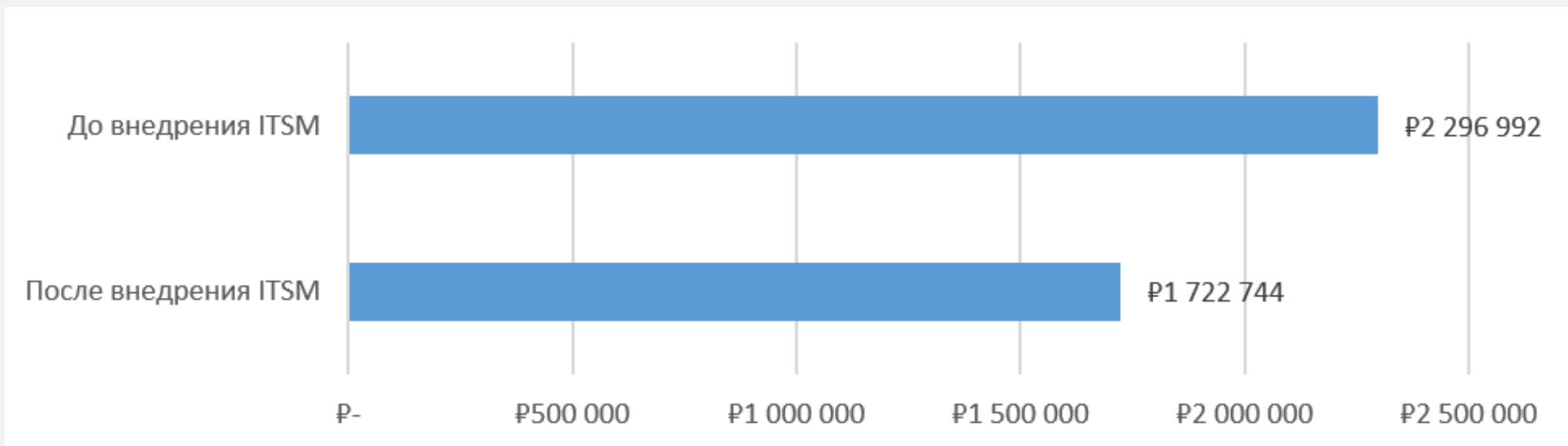
Характеристики OMNITRACKER ITSM Center

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 совершенствовани е 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

Физические и логические связи элементов ИТ инфраструктуры



Сокращение затрат на устранение инцидентов при внедрении ITSM



**СПАСИБО ЗА
ВНИМАНИЕ!**

