ГАЗПРОМБАНК

«Газпромбанк» Открытое акционерное общество)

Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем в ГПБ (ОАО)

Докладчик: Егоркин А.В.

Магнитогорск, 2014

Газпромбанк сегодня

Структура Газпромбанка: 35 филиалов, более **200** дополнительных офисов, **4** дочерних банка, более **10** стратегических промышленных активов.

Количество сотрудников: более **11 400** человек

Количество клиентов:

Физических лиц – более **3** миллионов

Юридических лиц – более **45** тысяч

Акционеры ГПБ

ОАО «Газпром»;

НПФ «Газфонд»;

ЗАО «Лидер»;

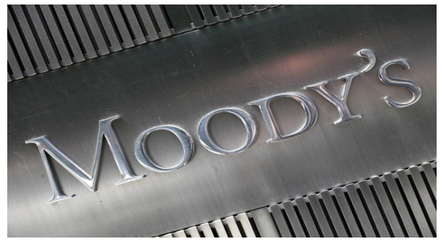
Внешэкономбанк;

ООО «Новфинтех».

Финансовые показатели	по состоянию на 01.01.2013	по состоянию на 01.01.2012
	млрд.рублей	млрд.рублей
Активы	***3 354,6***	*2,849,8*
Собственные средства	***366,0***	*271,9*
Чистая прибыль	***50,9***	*39,2*

Уставный капитал: 24 532 277 000 рублей

Рейтинг Газпромбанка



Baa3 (СТАБИЛЬНЫЙ)

RusRating a member of GlobalRating Group

A- (СТАБИЛЬНЫЙ)

ЭКСПЕРТ РА 10 РЕЙТИНГОВОЕ АГЕНТСТВО ЛЕТ

A++ (ВЫСОКИЙ)

Штатная структура ИБ в ГПБ (ОАО)

Председатель Правления ГПБ (ОАО)

- Правление ГПБ (ОАО)

  Заместитель Председателя Правления (Муранов А.Ю.)

  - **Департамент защиты информации (Егоркин А.В.)**
    - 71 сотрудник
    - 2 Управления: Управление информационной безопасности
      Управление технической безопасности
    - 2 Центра: Удостоверяющий центр, Ситуационный центр

Более 60 специалистов по информационной безопасности в штате
Отделов безопасности в 35 филиалах в 45 регионах РФ.

Этапы жизненного цикла АБС

ГПБ (ОАО)

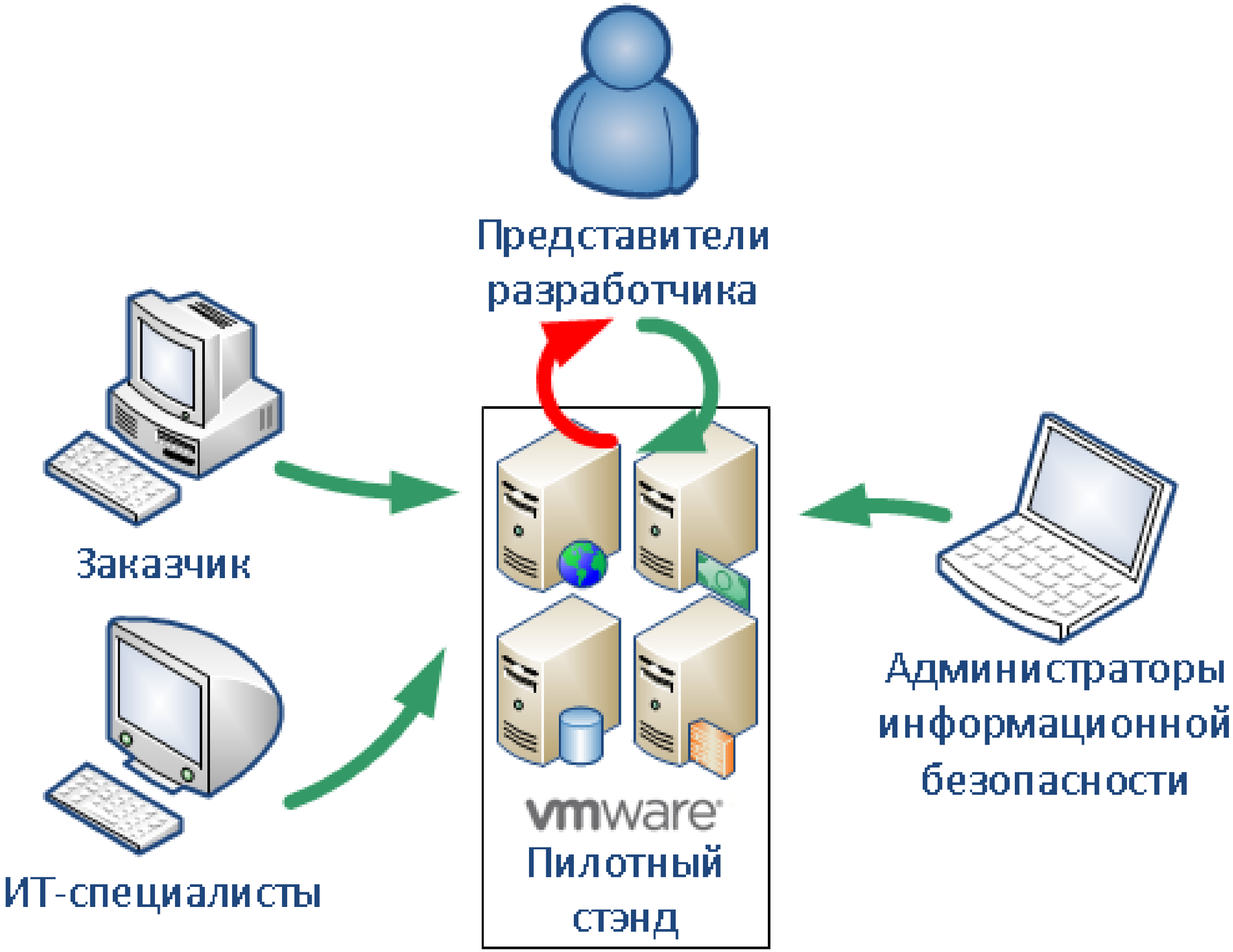
1. выбор решения;
2. пилотирование;
3. разработка технического задания;
4. проектирование;
5. создание;
6. тестирование;
7. приемка, ввод в опытную эксплуатацию;
8. опытная эксплуатация;
9. приемка, ввод в промышленную эксплуатацию;
10. промышленная эксплуатация;
11. модернизация;
12. снятие с эксплуатации.

СТО БР ИББС-20хх

1. разработка технического задания
2. проектирование;
3. создание и тестирование;
4. приемка и ввод в действие;
5. эксплуатация;
6. сопровождение и модернизация;
7. снятие с эксплуатации.

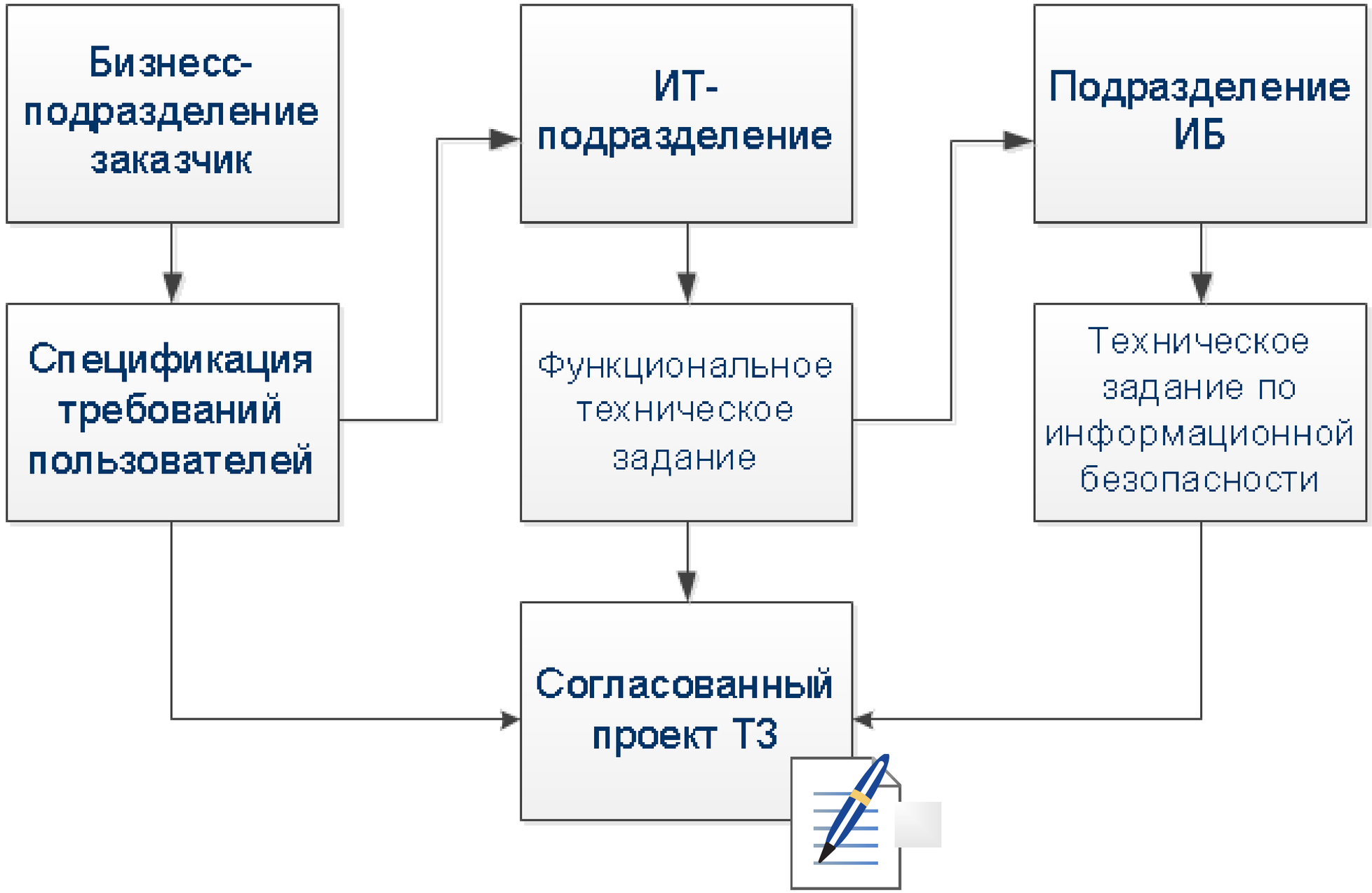
ГАЗПРОМБАНК

Этап пилотирования



ГАЗПРОМБАНК

Разработка технического задания



Разработка технического задания

Основные документы

ГОСТ 34.601-90
«Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»,

ГОСТ 34.602-89
«Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Типовые требования по информационной безопасности к автоматизированным системам в ГПБ(ОАО)

УТВЕРЖДАЮ

Начальник Департамента защиты информации

_____ А.В. Егоркин

Типовые требования
по информационной безопасности

Настоящие требования предъявляются к автоматизированным системам (АС), внедряемым или модернизируемым в ГПБ (ОАО), с целью обеспечения безопасности обрабатываемых в АС информационных активов.

№№	Код	Формулировка требования
1.	ИБ.1	**Общие принципы**
1.1.	ИБ.1.1	Автоматизированная система должна соответствовать требованиям стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС-1.0-2010 (стандарт Банка России).
1.2.	ИБ.1.2	В документации на АС должно быть указано автоматизацию какого вида технологического процесса обеспечивает внедряемая АС: банковского платежного технологического процесса или банковского информационного технологического процесса.
1.3.	ИБ.1.3	Комплекс программно-технических средств и организационных решений должен реализовываться в рамках системы защиты информации (СЗИ), которая включает в себя следующие подсистемы (детальное описание приведено в соответствующих разделах):

8 листов на А4 12 шрифтом с одинарными пробелами

Этап проектирования

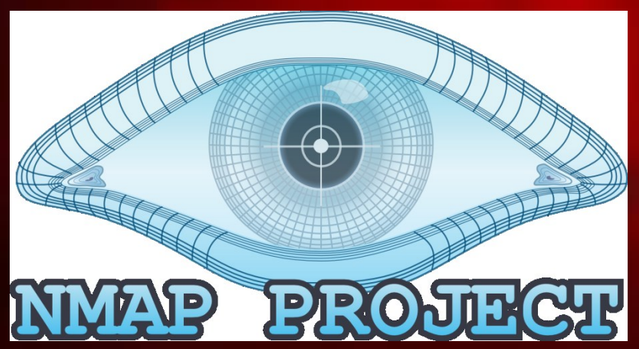
Основной документ: Техническое задание, в т.ч. перечень требований по информационной безопасности.

Этап тестирования выполнения требований по ИБ в АБС

1. Подготовка **программы-методики испытаний** по материалам технического задания
2. Проведение тестов по сценариям ПМИ
3. Использование инструментов для выявления:

- несоответствий ТЗ (полнота, корректность)
- типовых уязвимостей
- ошибок администраторов
- недокументированных возможностей
- программных закладок

4. Составление Актов



Этапы приемки. Ввод в эксплуатацию

Опытная эксплуатация

1. Акт о проведении приемо-сдаточных испытаний.
2. Перечень замечаний по ИБ, сгруппированных по степени критичности.
3. Распоряжение высшего должностного лица Банка – куратора проекта о вводе в опытную эксплуатацию (сроки, задачи, ответственные лица, контрольные точки).
4. Согласование перечня мероприятий для устранения выявленных недочетов и замечаний по ИБ.
5. В АБС отсутствует конфиденциальная информация.
6. Возможен доступ разработчиков в АБС.
7. Эксплуатация АБС осуществляется силами ИТ-блока Банка.
8. Загрузка конфиденциальной информации после устранения выявленных замечаний.
9. Персональная ответственной курирующего высшего должностного лица.

Промышленная эксплуатация

1. Акт о проведении приемо-сдаточных испытаний (без замечаний).
2. Распоряжение высшего должностного лица Банка – куратора проекта о вводе в промышленную эксплуатацию с даты подписания Распоряжения (назначение владельца ИТ-ресурса, администраторов, администраторов ИБ, групп пользователей и т.д.)
3. Утверждение комплекта эксплуатационной документации на АБС (регламент взаимодействия подразделений, инструкция пользователя, администратора, администратора ИБ, сетевые схемы доступа, планы реагирования в случае чрезвычайных ситуаций).
4. Размещение АБС в промышленном ЦОД.
5. Обеспечение непрерывности (резервное копирование, кластеризация).
6. Подключение к системе мониторинга в Ситуационном центре.

Этап эксплуатации / сопровождения

Основные документы по ИБ:

- Политика информационной безопасности ГПБ (ОАО)
- Частная политика обеспечения информационной безопасности на этапах жизненного цикла АБС
- Порядок предоставления и контроля доступа к ИТ-ресурсам в ГПБ (ОАО)
- Положение о конфиденциальности информации в ГПБ (ОАО)

Штатные функции ДЗИ:

- Согласование/ контроль заявок на предоставление доступа к ИТ-ресурсам.
- Мониторинг и расследование инцидентов ИБ в АБС;
- Разграничение доступа к АБС на уровне межсетевых экранов;
- Согласование ТЗ на доработку отдельных модулей АБС;
- Проведение аудитов ИБ в АБС, подготовка заключений;

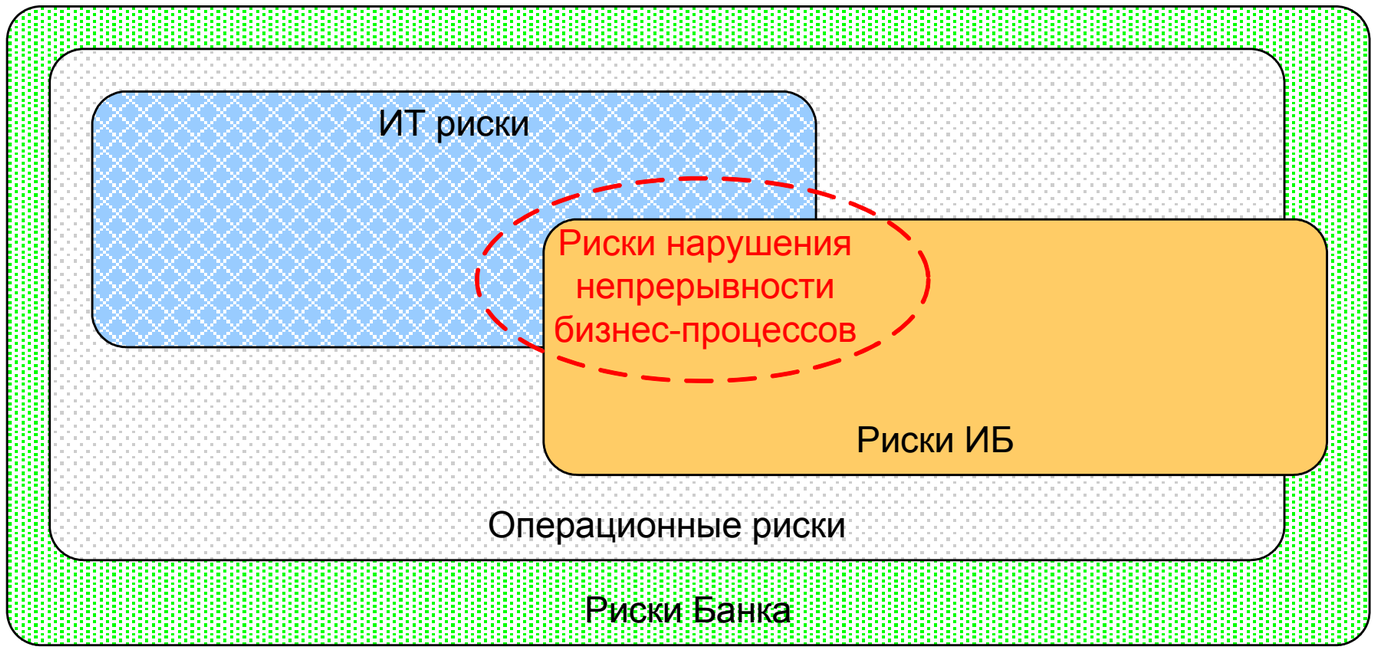
Этап модернизации

Основные документы:

1. Концепция. Управление информационной безопасностью ГПБ (ОАО) в период перехода на новую автоматизированную банковскую систему

2. Политика информационной безопасности ГПБ(ОАО)

3. Регламент управления информационно-технологическими проектами ГПБ (ОАО)



Этап вывода из эксплуатации

Основные задачи:

- контроль утечек и соблюдения правил и процедур обеспечения информационной безопасности;

INFOWATCH

- архивирование нужной информации, содержащейся в АБС;

- гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации АБС и (или) уничтожение машинных носителей информации.

ГАЗПРОМБАНК

Спасибо за внимание!

Готов ответить на Ваши вопросы

ГАЗПРОМБАНК

ДОКЛАДЧИК

Егоркин Александр Викторович

начальник Департамента защиты информации
ГПБ (ОАО) г. Москва

e-mail: AlexEgor@gazprombank.ru
тел: (495)-913-7933