Банк Москвы

Банк Москвы

В партнерстве с ВТБ

Обеспечение безопасности информации банковских приложений на различных стадиях жизненного цикла при разработке ИС своими силами

Окулесский Василий Андреевич к.т.н.

Начальник управления информационной безопасности

- **Банк Москвы** — один из крупнейших универсальных банков России (входит в топ-5), предоставляющий диверсифицированный спектр финансовых услуг как для юридических, так и для частных лиц. Основным акционером Банка является Группа ВТБ (95,53%).
- Банк насчитывает 284 обособленных подразделений, включая дополнительные офисы и операционные кассы. По состоянию на 1 января 2014 года в регионах России работает 149 подразделение Банка. В Москве и Московской области действует 135 офисов Банка. Кроме того, услуги населению оказываются в 424 почтово-банковских отделениях столичного региона. Стратегией развития Банка определено, что Банк Москвы будет развиваться как самостоятельный универсальный коммерческий банк в составе Группы ВТБ.
- В сеть Банка также входят 3 дочерних банка, находящихся за пределами России: АО «БМ Банк» (Украина), ОАО «Банк Москва-Минск» (Беларусь), Эстонский кредитный банк (Эстония).
- Высокую надежность Банка Москвы подтверждают рейтинги международных рейтинговых агентств. Долгосрочный кредитный рейтинг Банка по версии Moody’s Investors Service — Ba2, по версии Standard & Poor’s долгосрочный кредитный рейтинг — BBB.

Главные тезисы

- *Все новые ИС должны отвечать требованиям бизнеса*
- *Все новые ИС должны отвечать требованиям безопасности*
- *Безопасность – это не головная боль «безопасников», а спокойствие бизнеса*

Этапы жизненного цикла информационной системы с точки зрения ИБ

- *Разработка Технического задания : обязательный раздел в ТЗ и ПиМИ*
- *Разработка информационной системы : периодический контроль выполнения ТЗ*
- *Тестирование системы : протоколы и Акты испытаний в соответствии с ПиМИ, план работ по устранению замечаний*
- *Эксплуатация : сбор, обработка и исправление замечаний*
- *Вывод из эксплуатации системы либо ее элементов : передача в архив копий СУБД и данных, уничтожение информации на носителях, документирование действий*

Куда надо смотреть

- *Управление процессами обеспечения безопасности информации*
- *Периодическая оценка безопасности используемого оборудования, сервисов*
- *Управление уязвимостями*
- *Идентификация и управление доступом*
- *Безопасность на рабочих местах пользователей*
- *Обеспечение непрерывности автоматизируемого процесса*

Состав требований при разработке ТЗ

- *Обеспечение безопасности среды разработки;*
- *Методическое и инструментальное обеспечение;*
- *Меры и процедуры выявления и устранения недостатков ;*
- *Виды и представление документации*
- *Наличие и реализуемость достаточного количества контрольных операций.*

Состав требований к документации должен включать

- *к эксплуатационным документам по всем этапам ЖЦ, включая вывод из эксплуатации и утилизацию;*
- *к обеспечению поддержки доверия при эксплуатации;*
- *к обеспечению безопасности эксплуатирующей организации;*
- *к аудиту безопасности;*
- *к управлению модификациями;*
- *к мониторингу и поддержке безопасности разработчиком.*

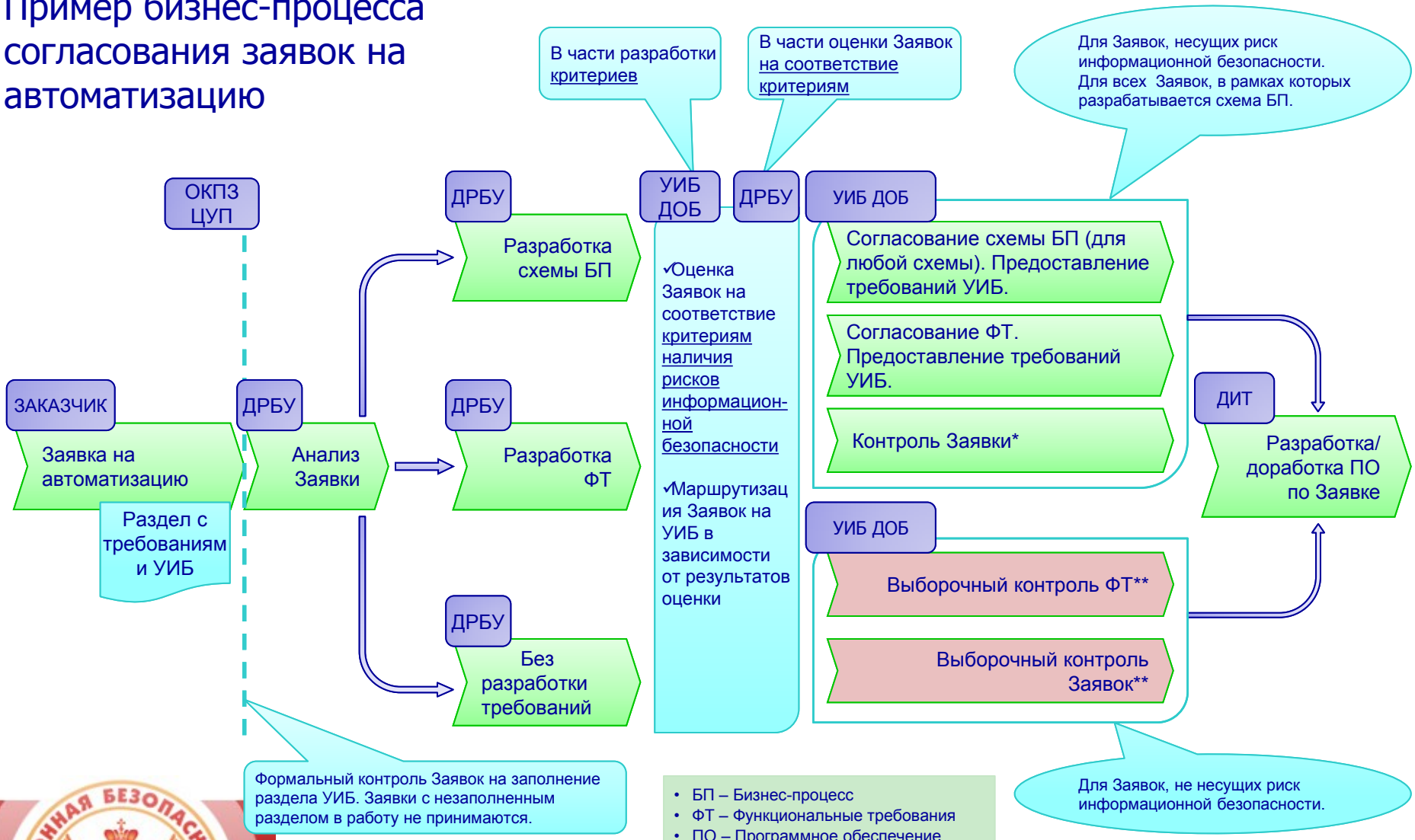
Что могут включать требования по ИБ

- *Требования по управлению доступом на основе ролей*
- *Требования по логированию действий администраторов и пользователей*
- *Требования по обеспечению целостности всех видов информации в системе*
- *Требования по обеспечению доступности системы и ее элементов, требования по резервному и архивному копированию*
- *Требования к SLA информационной системы*

Что могут включать требования по защите от фишинга (примерчик)

- *Исключение принципиальной возможности негласного несанкционированного получения персональных данных*
- *Использование динамичеких элементов в WEB-интерфейсе интернет ресурсов*
- *Защита от кросс-сайдинга, SQL-инъекций, в том числе защиты от исполняемых элементов(от скриптов), ограничение длины строки, анализ содержимого строки и т.д.*

Пример бизнес-процесса согласования заявок на автоматизацию



- БП – Бизнес-процесс
- ФТ – Функциональные требования
- ПО – Программное обеспечение

* По результатам контроля УИБ Заявки, направляемые для реализации в ДИТ без разработки схемы/ФТ, могут быть дополнены требованиями УИБ либо возвращены в ДРБУ для разработки ФТ (с предоставлением требований УИБ).

** УИБ ДОБ вправе направить замечания в ДРБУ не позднее срока, установленного для согласования документа (для заявок без требований – не позднее трех рабочих дней с даты поступления заявки в УИБ ДОБ).

Критерии оценки Заявки на автоматизацию на соответствие требованиям информационной безопасности

► Общие требования к Заявке на автоматизацию (формальный контроль ОКПЗ ЦУП).

1. Все Заявки должны быть утверждены на уровне руководителя самостоятельного структурного подразделения (ЭП руководителя).
2. Если Заказчик не является владельцем дорабатываемой информационной системы, то должно быть получено согласие владельца информационного ресурса на данную доработку (ЭП руководителя) (*вступает в силу после разработки порядка, определяющего формирование и сопровождение реестра владельцев ИТ- ресурсов*).
3. В Заявке должны быть отражены предполагаемые пользователи дорабатываемой функциональности (подразделение/должность).
4. Заявка должна содержать заполненное приложение «Требования информационной безопасности».

►Требования и критерии обеспечения ИБ в части распределения/назначения прав доступа (критерии используются ДРБУ при маршрутизации Заявок в УИБ ДОБ)

1. В Заявке должно быть отражено требует ли эта доработка внесение изменений в права на доступ для пользователей дорабатываемой функциональности (да/нет). **Если указано ДА, то необходимо согласование УИБ ДОБ.**

►Требования и критерии обеспечения ИБ в части информационного обмена (критерии используются ДРБУ при маршрутизации Заявок в УИБ ДОБ)

1. В Заявке должно быть отражено предполагается ли обработка и передача данных пластиковых карт (да/нет). **Если указано ДА, то необходимо согласование УИБ ДОБ**.
2. В Заявке должно быть отражено предполагается ли применение криптографических средств (шифрование, ЭП) (да/нет). **Если указано ДА, то необходимо согласование УИБ ДОБ**.
3. В Заявке должно быть отражено предполагается ли информационный обмен между информационными системами (как внутри сети, так и с внешними системами) (да/нет). **Если указано ДА, то необходимо согласование УИБ ДОБ.** (должна быть разработана схема обмена данными, с указанием по каким протоколам предполагается обмен).
4. В Заявке должно быть отражено, предполагается ли обработка и передача персональных данных клиентов вне сети Банка (да/нет). **Если указано ДА, то необходимо согласование УИБ ДОБ**.

Спасибо за внимание.

Тел. +7(495) 925 -8000
доб. 114-58
E-mail: Okulessky_VA@mmbank.ru