УДК 004

РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПАО «АКЦЕНТ-БАНК»

Муравьёв В.С., Губенко Н.Е.
Донецкий национальный технический университет
Кафедра компьютерных систем мониторинга

1 Актуальность проблемы

Одной из первостепенных задач, стоящих перед каждой банковской структурой, является ее постоянная адаптация к изменениям внешней среды, проявляющаяся в управлении кредитной и депозитной политиками, оптимизации филиальной сети, диверсификации номенклатуры основных продуктов и сопутствующих услуг и т.д. Банк является динамичной социотехнической системой, трансформирующейся с целью перехода в очередное устойчивое и управляемое состояние.

2 Построение структурной модели информационной системы (ИС)

Рассмотрим структуру банка с точки зрения информационной безопасности (ИБ).

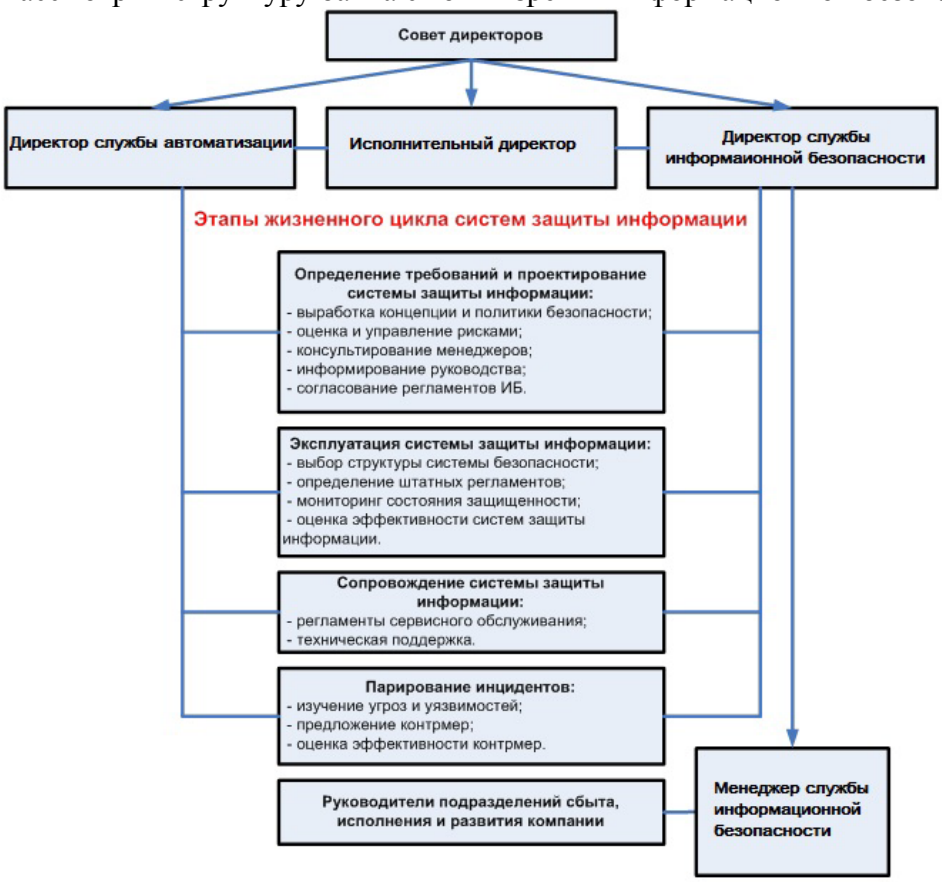

Рисунок 1 – Организационная структура ТОР-менеджмента «Акцент-Банк», ответственного за обеспечение безопасности

Графическое изображение конфигурации системы – ее структурная модель, на которой отображены аппаратные компоненты ИС, необходима для наглядного представления процесса функционирования системы. Эта модель позволяет проанализировать функции, возлагаемые на отдельные компоненты ИС и систему в целом.

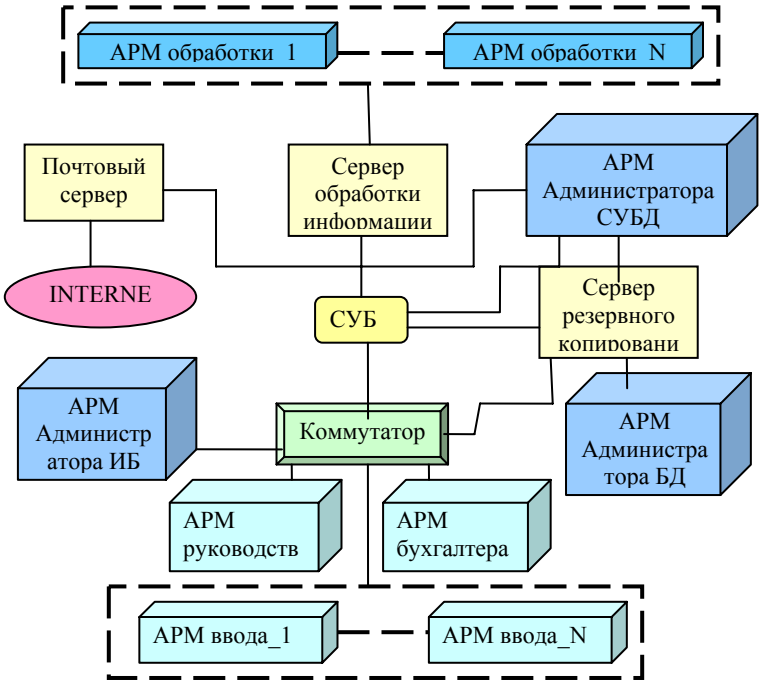

Рисунок 2 – Структурная модель информационной системы.

После определения структуры ИС банка назначаются ответственные за аппаратные ресурсы и регламент их использования для каждого из пользователей системы. В докладе рассматривается определение полномочий пользователей по отношению к аппаратным компонентам ИС и проводится идентификация информационных ресурсов с точки зрения их критичности.

3 Квалификация угроз, актуальных для ИС ПАО «Акцент-Банк»

При проведении оценки рисков должны рассматриваться три основные категории возможных потерь, описанные в таблице 1.

Таблица 1 – Категории возможных потерь

Категории возможных потерь	Описание
Денежная потеря	Денежная потеря определяется как потеря ценностей или увеличение стоимости или расходов.
Потеря производительности	Потеря производительности происходит тогда, когда персонал не способен продолжать выполнение своих обязанностей или когда необходимо повторять служебные обязанности.
Затруднения для организаций	Эта категория касается ситуаций, оказывающих влияние на установление общественного доверия. Следует учитывать также конфиденциальность, точность и согласованность

Оценку рисков проводим в соответствии с методикой, приведенной в [1]. При этом уровни риска подразделяются на три категории: высокий (В), средний (С) и низкий (Н).

Таблица 2 – Матрица оценки рисков

Зона Уязвимости	Угроза	Риск денежной потери	Риск потери производ-ти	Риск затруднения
Физический Уровень	Неавторизованное раскрытие защищаемой информации	С	С	Н
	Ухудшение обслуживания	Н	Н	Н
Сетевой Уровень	Неавторизованное раскрытие защищаемой информации	С	С	С
	Ухудшение обслуживания	Н	Н	Н
Уровень сетевых приложений	Неавторизованное раскрытие защищаемой информации	С	Н	Н
	Ухудшение обслуживания	Н	С	Н
Уровень ОС	Неавторизованное раскрытие защищаемой информации	С	В	В
	Ухудшение обслуживания	Н	С	С
Уровень СУБД	Неавторизованное раскрытие защищаемой информации	С	С	Н
	Ухудшение обслуживания	Н	С	С
Уровень приложений, необходимых для реализации основных функций ИС	Неавторизованное раскрытие защищаемой информации	В	В	В
	Ухудшение обслуживания	С	В	С
Уровень бизнес-процессов организации	Неавторизованное раскрытие, защищаемой инф-ции	В	В	В
	Ухудшение обслуживания	С	С	С

Как видно из таблицы 2 актуальными угрозами, объектом атаки которых является чувствительная либо высокочувствительная информация, для организации являются:

угроза неавторизованного раскрытия информации на уровне операционных систем, на уровне СУБД, на уровне приложений, необходимых для реализации основных функций ИС и на уровне бизнес – процессов;

угроза ухудшения обслуживания на уровне приложений, необходимых для реализации основных функций ИС и бизнес - процессов;

4 Разработка правил политики ИБ банка

Разработка и выполнение политики ИБ организации является наиболее эффективным способом минимизации рисков нарушения ИБ для организации. Политика безопасности представляет собой свод принципов и правил безопасности для наиболее важных областей деятельности и зон ответственности персонала. Политика информационной безопасности является требованием, в котором описываются цели и задачи мероприятий по обеспечению безопасности.

В процессе разработки политики безопасности формулируется свод правил информационной безопасности для противодействия угрозам информационной системы организации. На основе свода правил создается политика безопасности.

Правило №1:

В организации должны проводиться проверки выполняемых действий персонала.

Правило №2:

В организации следует оговаривать и периодически проверять обязанности пользователей по соблюдению мер безопасности.

Правило №3: Обеспечение защиты СУБД и хранение информации.

Правило №4: Обеспечение защиты бизнес-процессов филиала коммерческого банка.

Правило №5: Управление доступом.

Правило №6: Защита от вредоносного ПО.

Выводы

Описанные в тезисах методы для оценки риска, структурная модель и правила политики ИБ позволяют сформулировать политику безопасности ПАО «Акцент-Банк» в виде следующей таблицы.

Таблица 3 – Политика безопасности организации

Правила ИБ	Ответственные	Виды защитных мер
В организации должны проводиться проверки выполняемых действий персонала	Администратор ИБ	Организационные и технические
В организации следует оговаривать и периодически проверять обязанности пользователей по соблюдению мер безопасности	Администратор ИБ	Организационные
Обеспечение защиты СУБД и хранение информации	Персонал (операторы АРМ, администраторы)	Организационные и технические
Обеспечение защиты бизнес-процессов филиала коммерческого банка	Персонал (операторы АРМ, администраторы)	Организационные и технические
Управление доступом	Персонал (операторы АРМ, администраторы)	Организационные и технические
Защита от вредоносного ПО	Администраторы ИБ и СУБД	Организационные и технические

Список литературы

1. Алексеев В.М. Анализ угроз и разработка политики безопасности информационной системы организации.- Пенза 2007.- 30 с.
2. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 2007 г.