Главные вызовы проектов приведения системы управления операционными рисками в соответствие с требованиями 716-П

Илья Лозинский, PhD, MBA

Управляющий партнер

Компания Ланселот

LANCELOT
information technologies

Разработка решений для специалистов риск-менеджмента, кредитного и клиентского подразделений финансовых и кредитных организаций.

Внедрение аналитических приложений и систем делового интеллекта (BI).

Наши клиенты с ПО для управления операционными рисками:

citibank

MITSUBISHI MOTORS
Надежно.

MC Bank Rus
a subsidiary of Mitsubishi Corporation

РН Банк

Toyota Bank

ЮMoney | Яндекс Деньги

БКС

Особенности положения ЦБ о требованиях к системе управления операционными рисками в кредитной организации:

- Необходимо отслеживать источники происхождения инцидента, события Информационной безопасности, Информационных систем, проводки Автоматизированных банковских систем, операции платежных систем.

- Требуется ведение большой базы расчётных показателей, базирующихся на массиве исторических данных не менее чем 5 лет, с использованием данных связанных с операционным риском источников событий

- Необходимо подтверждать эффективности мероприятий по устранению событий операционного риска на основании данных статистики по инцидентам и мероприятиям

Без реализации данных пунктов невозможно обосновать Регулятору правильность расчета Капитала под риском и начисляемые банку резервы

LANCELOT
information technologies

Ситуация в Банке до перехода на 716Р:

LANCELOT
information technologies

Группа риска по 716п:

- В Банке до 5 000 событий оперрисков
- События ОР, повлекшие прямые убытки, не связаны с проводками в АБС
- Данные по прямым убыткам из базы по ОР не сверяются с АБС
- События ОР не импортируются в базу из CRM, HelpDesk, SIEM и т.п.
- Мониторится меньше 50 КИРов
- Отчетность ведется в таблицах (Excel, Lotus, MS Access и т.п.)
- Не разработан комплект ВНД (Политика по ИС, методики количественной оценки киберрисков, расчета прямых, косвенных, потенциальных потерь и т.д. /всего 84 документа/)
- Нет методолога и опыта развития культуры управления рисками по Базель 3 за последние 5 лет

LANCELOT
information technologies

Основные вызовы:

- Выявляется меньшая часть событий ОР
- Нет базы по ОР за 5 лет
- Нет методик определения убытков
- Нет методик количественной оценки рисков
- Данные о событиях ОР не поступают в базу ОР из смежных ИТ систем
- Нет методик расчета КИР и лимитов по ним
- Методология по управлению операционными рисками иностранных банков сильно отличается от требований 716П.

LANCELOT
information technologies

Риски проекта:

- 716п требует организованного взаимодействия оперрисков, СВА, СВК, СБ, ИБ и ИТ безопасности.
- Коллеги из смежных подразделений не знакомы с методологией 716п.
- Не все процессы описаны
- У них не прописана мотивация на обеспечение требований 716п.
- Команда без опыта работы по методологии 716п должна разработать эту методологию и поставить задачу разработчикам по автоматизации
- Команды внутренних разработчиков так же не владеют методологией 716п
- Чужие шаблоны ВНД не могут быть легко модифицированы под требования другого Банка
- На рынке труда нет опытных методологов по 716п

LANCELOT
information technologies

Риски аутсорсинга проекта:

- Команда без опыта работы по методологии 716п должна разработать ТЗ на эту методологию и проконтролировать разработчиков по автоматизации
- Вендоры предлагают «платформы» без методологии
- У подавляющего большинства вендоров нет опыта успешных внедрений ПО для 716п.
- Чужие шаблоны ВНД не могут быть легко модифицированы под требования другого Банка

LANCELOT
information technologies

Ситуация в Банке после перехода на 716Р:

LANCELOT
information technologies

Система управления операционными рисками:

- ВНД актуальны, KPI привязаны к мотивации
- Данные по прямым убыткам из АБС и базы ОР сверяются и совпадают
- Выявляет от 20 000 до 70 000 событий в год
- Более 300 КИРов осуществляют мониторинг агрегированных убытков по 7 классификаторам 716П
- BI-модуль позволяет спуститься от капитала под риском до любого события ОР
- Сценарный анализ проводится на актуальных моделях процессов

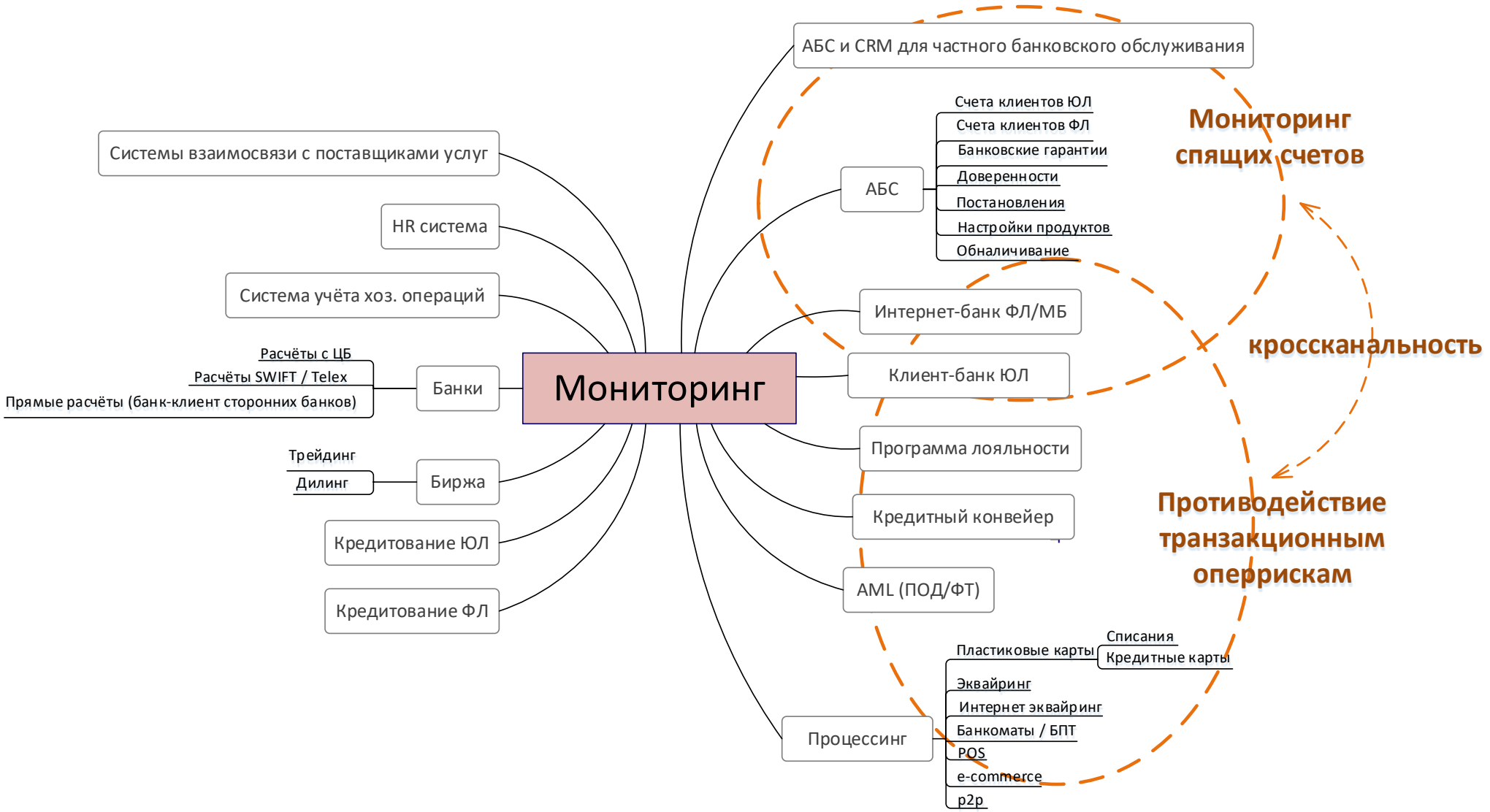
Ключевые технологии проекта:

- Автодетекция прямых убытков через анализ проводок АБС
- Автодетекция событий ОР из всех источников данных (26 источников)
- Детализация классификаторов (включая ИС системы, процессы и продукты)
- Методики расчета прямых, потенциальных и косвенных убытков
- Методика мониторинга совокупных агрегированных потерь по классификациям и лимитов по ним
- Шаблонизация обработки событий ОР
- Ведения отчетности по 716п, позволяющей в ходе проверки «провалиться» от капитала-под-риском до каждого события ОР и истории его выявления, оценки, расследования, борьбы с последствиями и предотвращения в будущем

LANCELOT
information technologies

LANCELOT
information technologies

АЛГОРИТМЫ И ВЫЯВЛЕНИЯ ОПЕРАЦИЙ НА ОСНОВАНИИ АБС И ПРОЧИХ СИСТЕМ



АБС

- Ошибки АБС;
- Ошибочное перечисление денежных средств;
- Неплатежеспособные, фальшивые купюры, подделки;
- Расхождение остатка денежных средств;
- Недостачи либо излишки в банкомате;
- Обход логики и ограничений АБС;
- На основании масок счетов: 25302, 26301, 26305, 26306, 26307, 26407, 27101, 27102, 27103, 27301, 27302, 27303, 27307, 27308, 47422, 47423, 60308, 60323, 70606

Внутренние риски

- Несанкционированные переводы средств со счетов клиентов;
- Несанкционированные операции по вкладам;
- Фиктивные зарплатные проекты для получения кредитов и обналичивания;
- Злоупотребления при заведении завещательных распоряжений и доверенностей;
- Несанкционированные переводы и увеличение лимитов по кредитным картам;
- Несанкционированное снятие ареста и других ограничений по счетам;
- Несанкционированное подключение Интернет-банка ФЛ;
- Злоупотребление полномочиями при проведении кассовых операций

ПРИМЕРЫ ОБЪЕКТОВ МОНИТОРИНГА

Интернет-банк

- Компрометация учётных записей в Интернет-банке;
- Несанкционированное использование карт;
- Изменение контактных данных в Интернет-банке и последующие операции по выводу денег;
- Попытка зарегистрировать Интернет-банк на клиентов из списка не благонадежных или входы с неблагонадежных адресов;
- Обход логики ограничений и лимитов в Интернет-банке;
- Использование продуктов банка для обналичивания денежных средств;
- Манипулирования со стороны клиентов программами бонусирования;
- Аномальная активизация «спящих» клиентов;
- Подмена реквизитов

LANCELOT
information technologies

ПРИМЕРЫ ОБЪЕКТОВ МОНИТОРИНГА

ПОД/ФТ

- Аномальный рост оборотов по счетам клиентов;
- Признаки транзитных операций у клиентов;
- «Чёрные», «серые», «белые» списки;
- Размер налоговых платежей не соответствует масштабам деятельности;
- Платежи по ЗП, НДФЛ и страховых взносов;
- Минимальные платежи по хозяйственной деятельности;
- Признаки аффилированности клиентов ЮЛ, ФЛ, сотрудников (платежи, контакты, должностные лица, устройства и пр.);
- Признаки вывода денежных средств на нерезидентов;
- Слом НДС у клиента;
- Увеличение доли снимаемых наличных денежных средств;
- Регулярные зачисления крупных сумм с последующим выводом;
- Аномальная активация «спящего» ЮЛ;
- Признаки обналичивания денежных средств и «веера»

Электронные кошельки и ТСО

- Компрометация учётных записей ЭК;
- Обход логики и ограничений ЭК;
- «Спящие» ЭК;
- Подмена сумм платежей на поставщиков услуг;
- Генерация «ложных» платежей на поставщиков услуг;
- Использование ЭК и ТСО для обналичивания;
- Заражение терминала вредоносным ПО;
- Подключение «ложного» терминала;
- Выход на интерфейс терминала;
- Обман купюроприёмника (подмена номинала, прогон купюры);
- Удаленное управление терминалом

Спасибо за внимание!

Контакты:

Илья Теодорович Лозинский
Управляющий партнер
ООО Ланселот
+ 7 499 380 7423
+7 925 963 7300
lozinsky@lancelot-it.ru