Урок 7. Анализ: выявление проблемных мест, bottlenecks и зон для развития

ДЗ: Выберите любой процесс и выпишите все его ключевые показатели эффективности

Возьмем KPI банковского обслуживания. В банке всё строго регламентировано и завязано на экономике. Поэтому большинство KPI неразрывно связано с экономическими показателями. Однако, мы будем брать не весь банк, а только интернет-банкинг, дистанционное банковское обслуживание.

Всегда важно влияние технического прогресса на рентабельность собственного капитала (ROE). В свою очередь, этот показатель зависит от PM – показателя прибыли, AU – операционной эффективности и EM – мультипликатора капитала. На эту тему я писал научную статью, поэтому добавляю фрагменты из неё.

Дополнительный доход банку поступает от увеличения величины денежных потоков вследствие возрастания комиссионных взносов и/или уменьшения расходов благодаря росту операционной эффективности. Рассмотрим влияние научно-технического прогресса на рентабельность собственного капитала (Return on equity – ROE):

$$ROE = ROA \times EM = PM \times AU \times EM$$

где PM – маржа прибыли; AU – коэффициент оборачиваемости активов; EM – значение мультипликатора капитала. Ключевая переменная здесь PM – отношение чистой прибыли к совокупной выручке и AU – отношение совокупной выручки к стоимости активов. Коэффициент рентабельности собственного капитала представляет собой величину дохода банка на денежную единицу собственных средств:

$$ROE = NP/E$$

где NP (net profit) составляет чистую прибыль (разницу между доходами и расходами), E – средний собственный капитал.

Инвестиции в системы электронного банковского обслуживания увеличивают PM путём минимизации расходов и AU путём возрастания комиссионных доходов банка, поэтому ROA и ROE возрастут. Если расширение доли рынка и увеличение базы активов в результате внедрения инноваций превысит рост капитала, то полученный финансовый леверидж (более высокое значение EM) продвинет вперёд ROE. Банкам, имеющим излишки капитала относительно того минимума, который требуют регуляторы, необходимо инвестировать в электронный банкинг и другие продукты, использующие новейшие достижения в области цифровых технологий и искусственного интеллекта.

[…]

Для банка и его ДБО важен такой показатель, как ***чистый процентный доход*** банка $NIM = \frac{\text{Инвестиционный доход – процентные расходы}}{\text{Средняя доходность активов}}$. Показывает, как работают банковские активы.

Проблемный кредит $NPL = \frac{\text{Проблемные кредиты}}{\text{Кол-во всех кредитов}}$. Кредит может считаться проблемным, если регулярный платёж по кредиту был просрочен на 90 дней.

Чистое списание $NCO = \frac{\text{Общая сумма списанных кредитов}}{\text{Количество кредитов}}$. Показывает процент долга перед банком, который вряд ли будет взыскан.

[…]

Также в банке не менее важны показатели эффективности риск-менеджмента, о чем я говорил в предыдущих ДЗ. Для примера – тоже отрывок из моей статьи.

Современные системы обеспечения кибербезопасности должны быть хорошо автоматизированы, для своевременной реакции на возникающие инциденты. Немедленный запуск процесс реагирования должен происходить фактически от любого сигнала систем мониторинга состояния информационной безопасности. Эффективность выбранного способа реагирования можно проверить по формуле:

$$RRL = \frac{RE_{before} - RE_{after}}{RRC}$$

где RRL – эффект от снижения риска кибербезопасности (способ приемлем при $RRL > 1$);

RE_{before} и RE_{after} – подверженность риску кибератак до (before) и после (after) применения метода реагирования;

RRC – затраты, которые связаны с применением того или иного метода реагирования.

Конечно, детальный расчёт компенсационных расходов может быть проигнорирован при незначительных последствиях реализации риска кибератак.

Ревенков П.В., **Бердюгин А.А.** Количественный подход к оценке риска воздействия кибератак при использовании технологии электронного банкинга // Защита информации. Инсайд. 2020. № 2 (92). С. 36–42.

В другой статье я уже сам разработал KPI. Отрывок с одним из них привожу:

Аналитик-эксперт должен ответить на ряд контрольных вопросов по пятибалльной шкале, чтобы получить информацию о качестве управления риском кибербезопасности на предприятии. Каждый вопрос имеет свой вес, который аналитик определяет самостоятельно экспертным путём, предварительно согласовав свои действия с руководством. Индекс соответствия компонентов банка нормам внутренних нормативных актов определяется по формуле:

$$AGR = \frac{\sum(\text{Балл} \times \text{Вес})}{\sum \text{Весов}}$$

Значение индикатора AGR обратно пропорционально уровню качества системы управления риском кибербезопасности в системах электронного банкинга. Однако, такая оценка AGR представляет собой среднее арифметическое взвешенное и явно превышает единицу, что противоречит математическому определению вероятности, чем и является риск. Поэтому вычислим AGR проще – без присвоения веса (уровня значимости) вопросам:

$$AGR = \frac{\sum вопросов}{\sum баллов}$$

Некоторые эксперты предлагают оценивать возможные потери, используя достаточно общую формулу, в которой риск R определяется на основании агрегированных индексов качества обеспечения информационной безопасности AGR и так называемой «суммы под риском» S_R, показывающей величину ущерба.

Разделим мероприятия, выраженные агрегированными индексами, оценивающими обеспечение информационной безопасности, на программные $AGR_{ПРГ}$ и экономические $AGR_{ЭКН}$. Формула оценки риска кибербезопасности имеет вид:

$$R = S_R \cdot \left(AGR_{ПРГ} + AGR_{ЭКН} \right)$$

Реальная практика включает также юридические, аппаратные, криптографические и физические меры безопасности. Аппаратные, программные и криптографические меры можно объединить в технические. Перечень контрольных вопросов и способ определения индексов AGR приведён в работах [перечисление в статье], относятся к соблюдению политики информационной безопасности и для экономии места в работе опускается.

Преимущество данного подхода над тем, который предлагает Basel II, состоит в учёте индивидуальных особенностей аппаратно-программного обеспечения (АПО) конкретного банка без универсальных коэффициентов для общего случая.

Бердюгин А.А. Разработка алгоритма оценки риска воздействия кибератак в условиях электронного банкинга // Безопасность информационных технологий. 2019. Т. 26, № 2. С. 86–94. DOI: 10.26583/bit.2019.2.06.

Вообще показателей может быть гораздо больше, причем у каждого отдела – свои показатели. Достаточно перечислить отделы, чтобы понять, почему мы не рассматриваем все KPI банковского обслуживания:

- Отдел автоматизации;
- Отдел финансового мониторинга;
- Фондовый отдел;
- Кредитный отдел;
- Отдел по работе с клиентами;
- Отдел информационной безопасности;
- Операционный отдел;
- Бухгалтерия;
- Юридический отдел;
- Отдел внутреннего контроля;
- Планово-финансовый отдел;
- Отдел кассовых операций;
- Хозяйственный отдел;
- Отдел кадров;
- Инвестиционный отдел;
- Аналитический отдел;
- Управление риск-менеджмента.

И у каждого отдела есть свои ключевые показатели эффективности (KPI).