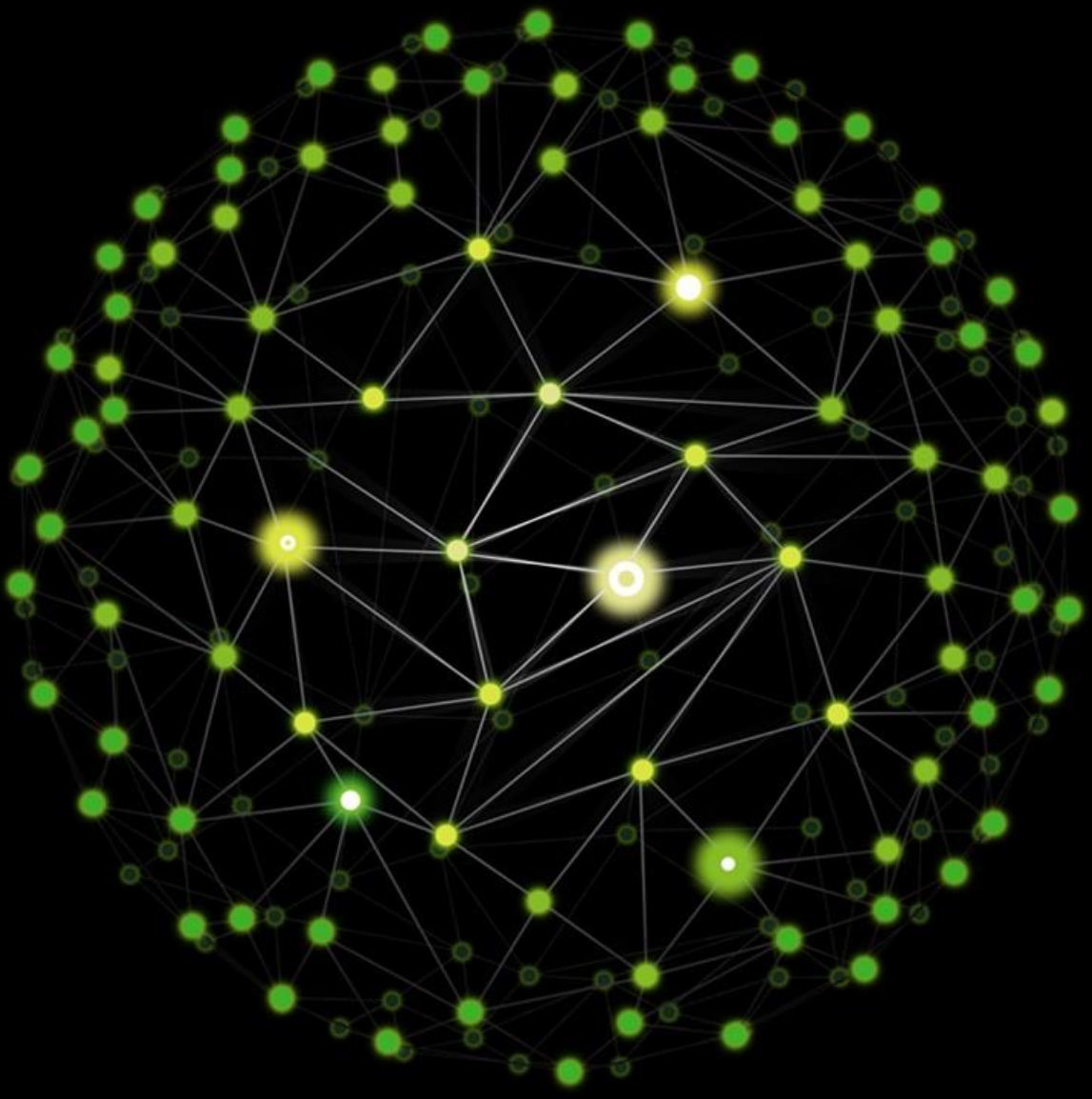
Deloitte.



Количественная оценка киберрисков

MAKING AN IMPACT THAT MATTERS since 1845

Что такое киберриски и зачем их оценивать

Риск - влияние неопределенности на цели

Определение международного стандарта ISO 31000:2018

Многие существенные риски современных организаций возникают в киберпространстве, а их последствия могут оказывать непосредственное влияние на финансовую и операционную деятельность. При этом глобальный ущерб от киберинцидентов растет год от года.

Совершенствование применяемых киберпреступниками методов и увеличение объемов совершаемых в Интернете транзакций усложняет обеспечение контроля за рисками информационной безопасности. Поддержание должного уровня безопасности требует инвестиций, которые далеко не всегда можно выделить в полном объеме. Руководители готовы выделять средства на решение подобных задач, однако требуют обоснования затрат и четкого понимания того, какие риски будут в результате минимизированы.

Особое внимание к управлению киберрисками уделяется в финансовой сфере. Согласно вступающему в силу 1 октября 2020 года Положению № 716-П Банка России, до 1 января 2022 года кредитные организации должны привести систему управления рисками в соответствие с новыми требованиями, включая требования к управлению риском информационной безопасности (включая киберриск) и риском информационных систем.

Практика «Делойта» по управлению рисками, связанными с использованием новейших технологий и автоматизацией бизнеса, помогает компаниям повышать эффективность бизнес-процессов и в наибольшей степени использовать потенциал внедряемых технологий. Наша цель – способствовать достижению операционных и финансовых целей организаций путем содействия в оценке, управлении и контроле за киберрисками.

Мы предлагаем вам ознакомиться с подходом к оценке киберрисков, применяемым «Делойтом» при построении системы управления информационной безопасностью в организации. Используемый комплексный подход к оценке рисков, основанный на бизнес-потребностях конкретных организаций, позволяет более точечно и осознанно подходить к инвестициям в информационную безопасность и фокусировать особое внимание на критически важных областях.

Таким образом, количественная оценка рисков позволяет:

1. На «языке бизнеса» рассказать о значимости управления рисками информационной безопасности в организации
2. В денежном выражении оценить влияние киберрисков на ключевые показатели бизнеса
3. Приоритизировать существующие киберриски
4. Определить необходимые мероприятия, проекты и технологии для дальнейшего управления киберрисками

Влияние киберрисков на деятельность банков и финансовых организаций растет

Основные виды атак на российские банки

- Социальная инженерия
- Утечка данных
- DDOS атаки

Источники: МВФ, Group-IB, Ponemon Institute, Positive Technologies, 2018

Векторы кибератак на банки

Проект положения Банка России "О требованиях к системе управления операционным риском в кредитной организации и банковской группе"

1. Требования к системе управления операционным риском, включая требования к системам управления риском информационной безопасности (ИБ) и риском информационных систем (ИС).

2. Определяет подходы к требованиям к капиталу в рамках внутренних процедур оценки достаточности капитала, необходимого на покрытие потерь от киберриска.

3. Требования к классификациям, используемым в системе управления операционным риском и рисками ИБ:
   - *Категории источников рисков ИБ;*
   - *Виды риска;*
   - *Типы событий;*
   - *Направления деятельности кредитных организаций.*

4. Требования к процедурам управления рисками информационной безопасности:
   - *Выявление и идентификация;*
   - *Сбор информации о событиях;*
   - *Количественная и качественная оценка;*
   - *Способы реагирования;*
   - *Мониторинг и контроль за эффективностью управления.*

5. Процедура качественной оценки уровня операционного риска, в дополнение к количественной оценке, включает:
   - *Самооценку операционного риска и способов контроля;*
   - *Экспертную профессиональную оценку (профессиональное мнение внутренних и внешних экспертов);*
   - *Автоматизированную оценку с использованием программного обеспечения;*
   - *Сценарный анализ операционных рисков.*

6. Процедура количественной оценки уровня операционного риска, включает:
   - *Агрегированную оценку уровня операционного риска;*
   - *Оценку необходимого капитала для целей ВПОДК на покрытие потерь;*
   - *Оценку ожидаемых потерь от реализации операционного риска.*

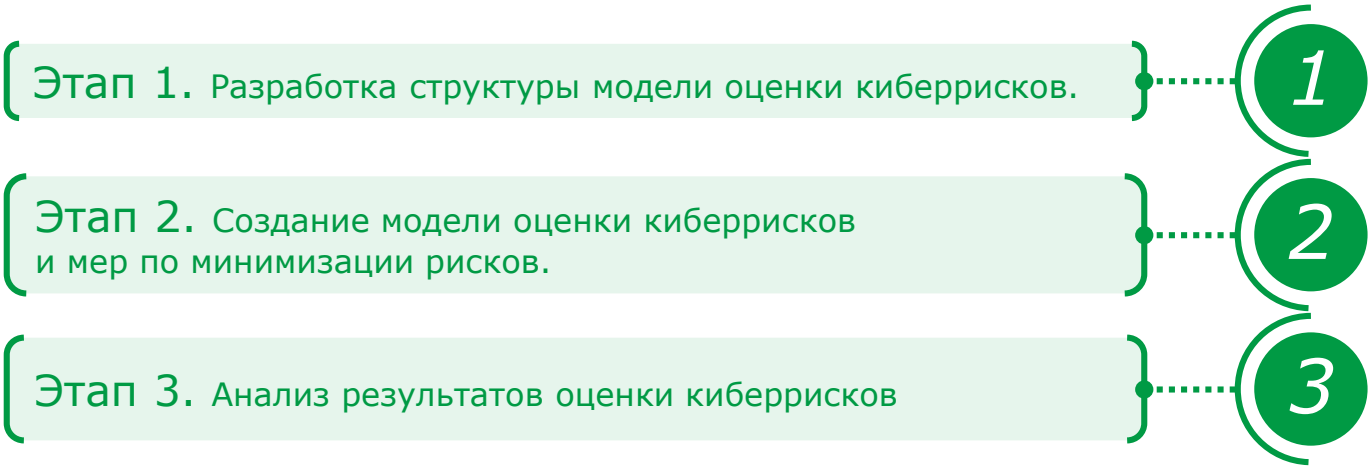
«Делойт» разработал собственный подход к оценке киберрисков

Подход Делойт по оценке киберрисков отвечает требованиям международных стандартов по управлению рисками (COSO ERM, ISO 31000, ISO 27001) и требованиям Банка России, а также лучшим практикам в области оценки рисков.

Методология оценки киберрисков Делойт предполагает разработку индивидуальной модели, позволяющей оценивать киберриски, в том числе в денежном выражении, а также их влияние на отклонение ключевых показателей деятельности организации от плановых значений. Для оценки кибберрисков используются методы факторного и сценарного анализа и имитационного моделирования с учетом оценки распределения потенциальных потерь на основании имеющихся исторических данных и экспертной оценки базовых компонентов.

Помимо этого, модель позволяет рассчитывать размер риска с учетом комбинаций инициатив по минимизации риска для оценки экономической целесообразности внедрения данных инициатив.

Подход Делойт по оценке киберрисков включает в себя несколько этапов:

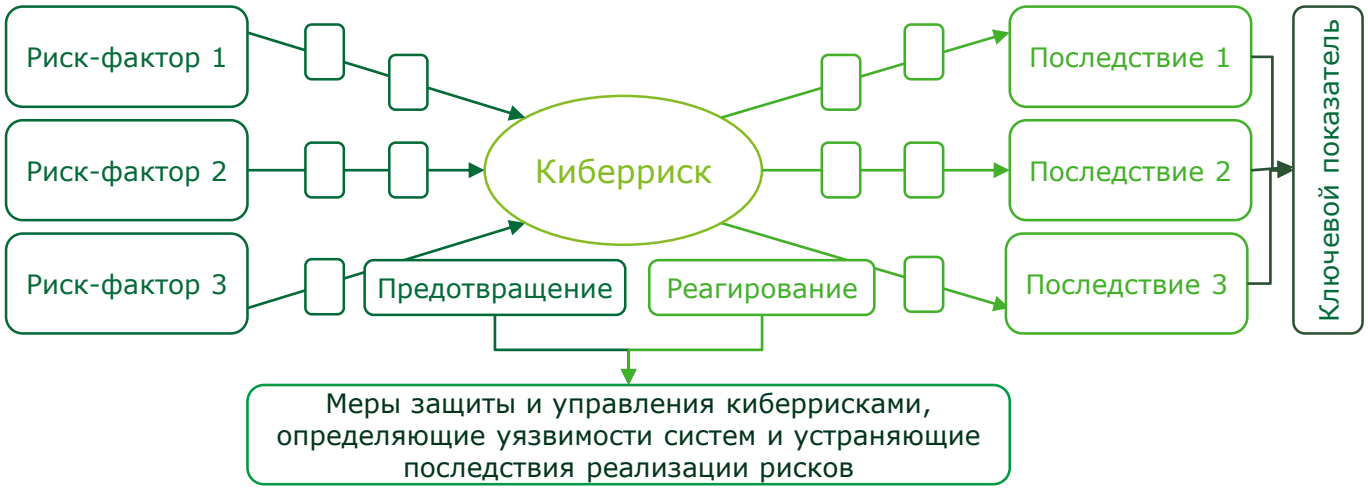


Этап 1. Разработка структуры модели оценки киберрисков.

1

- Проведение интервью с ключевыми бизнес-подразделениями с целью определения критичных активов, для которых будут оцениваться киберриски;
- Определение ключевых финансово-экономических показателей бизнеса для анализа влияния рисков на их значения;
- Выявление потенциальных киберрисков, их риск-факторов и последствий с помощью метода «галстук-бабочка»;
- Определение критичных киберрисков для проведения их количественной оценки;
- Определение мер по минимизации киберрисков;
- Определение взаимосвязей между критичными рисками, мерами и ключевыми показателями.

Диаграмма «галстук-бабочка» для анализа киберриска

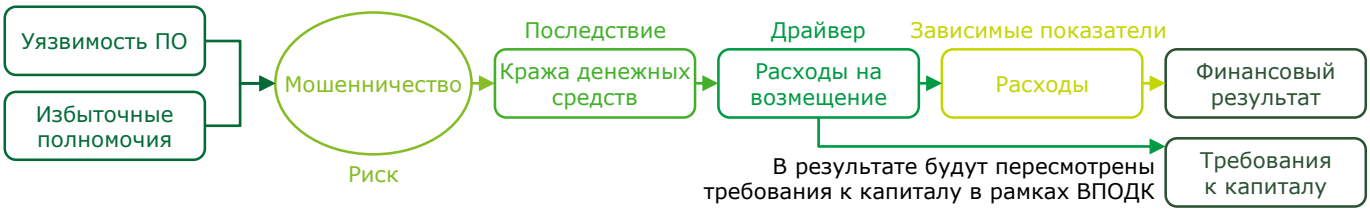


Пример взаимосвязи киберриска и ключевых показателей деятельности для нефинансовой организации

Реализация риск-факторов	… может быть использована для атаки на системы, что вызовет их недоступность	Это приведет к приостановке деятельности	… и изменению основных драйверов бизнеса	… а также зависимых от драйверов показателей	В конечном итоге плановый показатель деятельности не будет достигнут

Пример взаимосвязи киберриска и ключевых показателей деятельности для банка

Реализация риск-факторов	… может быть использована мошенниками для взлома систем банка …	… и кражи денежных средств	Это приведет к расходам по возмещению убытков	… и повлияет на изменение зависимых показателей	В конечном итоге плановый финансовый результат не будет достигнут



2 Этап 2. Разработка модели оценки киберрисков и мер по минимизации рисков.

Этап разработки модели включает в себя внесение в существующую финансовую/бюджетную модель:

- Неопределённости, вызванной киберрисками;
- Мер управления рисками.

При внесении неопределенности формируются параметры рисков – возможные диапазоны значений драйверов при реализации киберриска. Параметры риска задаются на основании нескольких предположений (сценариев):

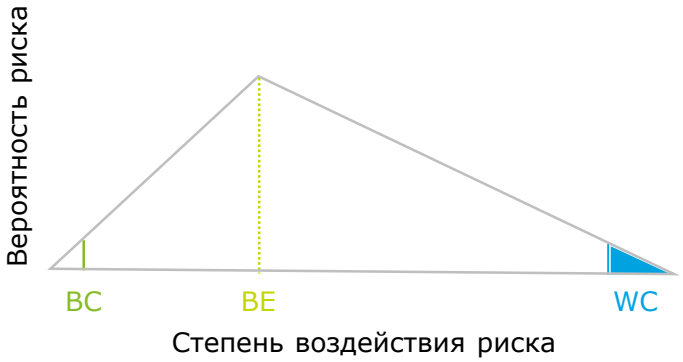
- Оптимистичный сценарий (best case – **BC**) представляет собой наиболее оптимистичный и при этом реалистичный исход событий;
- Ожидаемый сценарий (best estimate – **BE**) представляет собой наиболее вероятную ситуацию или наиболее ожидаемый исход;
- Пессимистичный сценарий (worst case – **WC**) представляет собой наихудший реалистичный вариант развития событий.

Пример:

Параметры риска «Недоступность систем»	BC	BE	WC
Количество инцидентов недоступности системы из за риск-фактора «уязвимость ПО», за год	1	2	5
Количество инцидентов недоступности системы из за риск-фактора «подключение к сети Интернет», за год	0	3	5
Величина потерь при реализации инцидента	$ 500	$ 1 000	$ 2 000
Распределение величины риска без учета мер	$ 500	$ 5 000	$ 20 000
Мера по минимизации вероятности реализации риск-фактора «уязвимость ПО»	Снижение количества инцидентов на 10%		
Мера по снижению последствий	Снижение величины потерь на 20%		
Распределение величины риска с учетом мер	$ 300	$ 3 600	$ 14 400

Параметры риска формируют распределение величины риска

График Распределения величины риска



Распределение различных рисков влияет на драйверы деятельности и включается в формулы расчета соответствующих ключевых показателей. На основании таких распределений для каждого риска модель прогнозирует диапазон колебаний ключевых показателей с учетом различных сценариев реализации рисков на основании введенных параметров при необходимом уровне уверенности (вероятности).

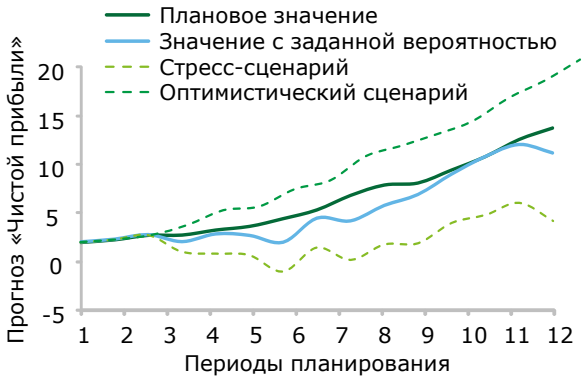
Этап 3. Анализ результатов оценки киберрисков.

3

- Определение величины ущерба от киберрисков (с учетом и без учета мер по минимизации риска);
- Ранжирование и приоритизация киберрисков;
- Анализ влияния рисков на показатели бизнеса (каждого риска в отдельности и совокупно) и определение вероятности достижения целевых значений показателей с учетом рисков.

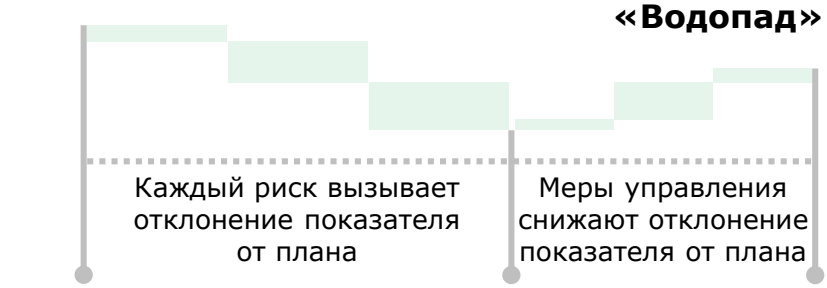
1 Модель позволяет прогнозировать значение показателя с учетом одного риска или группы рисков, с учетом мер по минимизации рисков и без учета.

Распределение «чистой прибыли» с учетом влияния киберрисков



2 Модель позволяет приоритизировать риски и мероприятия исходя из их влияния на ключевые показатели в форме диаграмм «Водопад» и «Торнадо».

«Водопад»

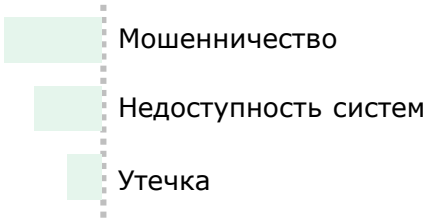


Плановое значение показателя «чистая прибыль»

Значение показателя «чистая прибыль» с учетом рисков

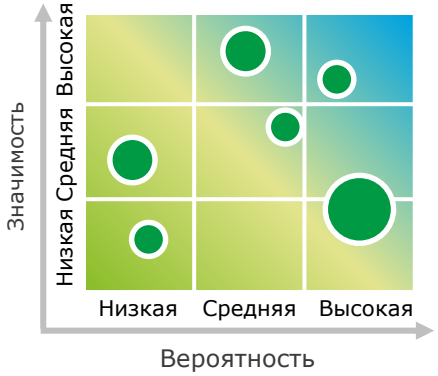
Значение показателя «чистая прибыль» с учетом рисков и мер

«Торнадо»



Воздействие киберрисков на отклонение показателя «чистая прибыль» от планового значения

3 Модель позволяет транслировать полученные оценки значимости риска на матрицу рисков исходя из заданных интервалов отклонения показателя от планового значения.



Диаметр окружности риска на матрице отображает степень управляемости риском: чем больше диаметр – тем ниже управляемость этим риском.

Deloitte.

Денис Липов

Партнер
Управление рисками

Тел.: +7 (495) 787 06 00
доб. 3071
Email:dlipov@deloitte.ru

Юлия Гончарова

Старший менеджер
Управление рисками

Тел.: +7 (495) 787 06 00
доб. 5086
Email: ygoncharova@deloitte.ru

Татьяна Будишевская

Директор
Управление рисками

Тел.: +7 (495) 787 06 00
доб. 1442
Email:budishevskaya@deloitte.ru