# Организация системы управления операционным риском в финансовых организациях

**Ольга Васильева, FRM**

**Москва, 2021**

# Содержание вебинара

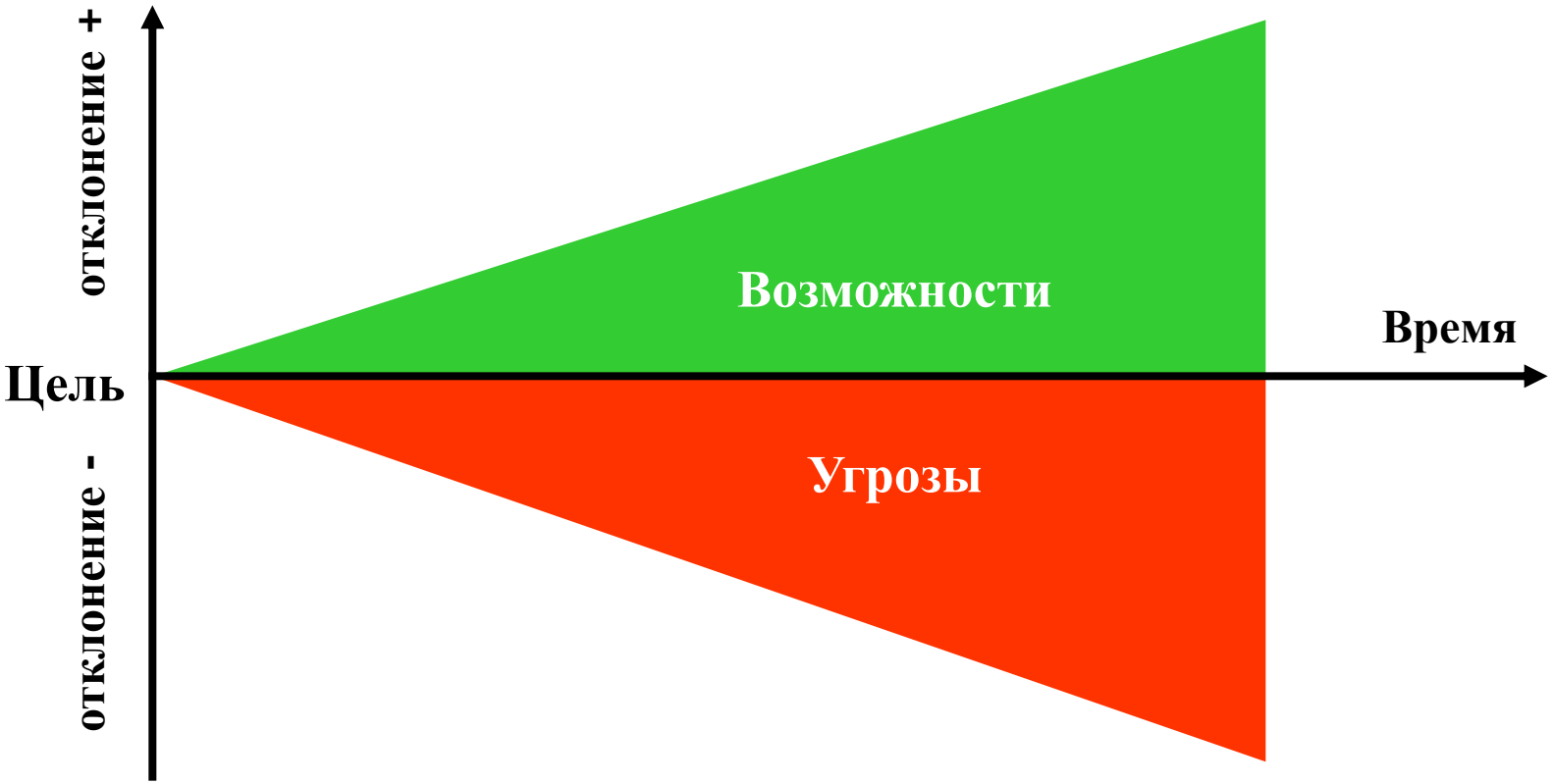
1. Понятие операционного риска
2. Элементы системы управления операционным риском
3. Участники системы управления операционным риском
4. База событий операционного риска
5. Отчетность по операционному риску
6. Новые требования Банка России для кредитных организаций
7. Основные ошибки при построении системы управления операционным риском

# 1. Понятие операционного риска

1. Что такое операционный риск?
2. Почему операционный риск самый важный, и в то же время самый недооцененный?
3. Как его идентифицировать?
4. Какие бывают виды операционных рисков?
5. Как их правильно классифицировать?

# Двойственный характер риска

Риск – это неопределенность будущего, выражающаяся в отклонении результата от ожиданий:




Будущее включает в себя угрозы и возможности

К сожалению, не все риски симметричны

# Цели управления риском

## «Выживание»

- Предотвращение неприемлемых потерь
- Безопасность условий труда
- Защита имущества
- Защита конфиденциальной информации
- Защита деловой репутации

## «Процветание»

- Повышение рыночной стоимости
- Стабилизация показателей прибыли
- Повышение кредитного рейтинга, снижение стоимости заимствований
- Снижение страховых премий и франшиз
- Справедливая оценка деятельности подразделений с учетом риска

# Цели управления риском


**Основное правило риск-менеджмента:**
стоимость управления риском не должна превышать возможных потерь от реализации данного риска

**Еще одно правило:**
не стоит пытаться управлять всеми рисками сразу, в первую очередь нужно управлять наиболее существенными из них

# Понятие операционного риска

**Операционный риск (ОР)** – это риск возникновения прямых и непрямых потерь в результате:

- несовершенства или ошибочных внутренних процессов организации
- действий персонала и иных лиц
- сбоев и недостатков информационных, технологических и других систем
- внешних событий

Операционный риск включает в себя правовой риск, но не включает стратегический и репутационный риски

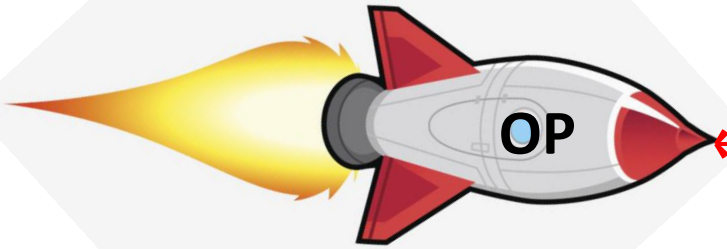
# Почему операционный риск самый недооцененный?

- Операционный риск самый «молодой», впервые появляется только в Базель II
- Отсутствие обязательной нормативной базы Банка России – только в 2020 вступило в силу Положение 716-П ««О требованиях к системе управления операционным риском в кредитной организации и банковской группе», для НФО таких требований пока нет
- Существенные операционные риски могут иметь длинный горизонт возникновения
- Эффект от управления операционным риском рассчитать сложно
- Потери от «чистого» операционного риска могут выглядеть незначительно на фоне потерь от прочих рисков

# Почему операционный риск самый важный?

Кредитный риск

Рыночный риск




Риск ликвидности

Стратегический риск
Репутационный риск

Потери от дефолтов заемщиков/контрагентов

Потери в результате деятельности на РЦБ

Потери в результате операционных сбоев

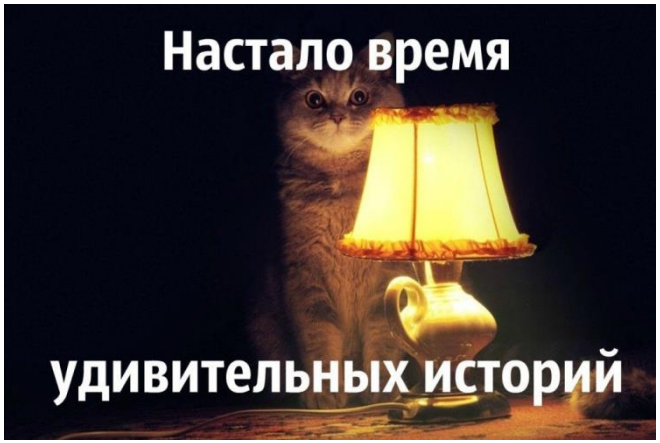
Потери от недостаточности ликвидности

Потери клиентов/бизнеса

# Почему операционный риск самый важный?

## Операционный риск

Некорректный ввод данных о сделке в систему




## Рыночный риск

Mizuho Securities. USD 223 млн
Продажа 620 тыс. акций J-Com за 1 иену вместо продажи 1 акции за 620 тыс. иен вследствие ошибки сотрудника. При этом в обращении находилось 14 тыс. акций

## Кредитный риск

Несоблюдение внутренних процессов, отсутствие контрольных процедур и разделения полномочий

Shoko Chukin Bank. USD 2,39 млрд
Внесение изменений работниками банка в данные кредитных заявок с целью их одобрения в рамках выполнения государственной программы по поддержке малого бизнеса (4,6 тыс. выявленных кейсов)

Barings PLC. USD 1,4 млрд
Совмещение Ником Лисоном должностей управляющего сингапурским филиалом и руководителя бэк-офиса. Осуществление операций с деривативами в нарушение одобренной руководством стратегии и сокрытие полученных убытков на созданном специальном счете

# Почему операционный риск самый важный?

Пожар в здании ПромстройНИИПроекта, в котором располагалось отделение Сбербанка, 2006


Сотрудницы прыгали из окон предпоследнего этажа, погибло 9 женщин

- ✓Формальный подход к выполнению мероприятий по ОНиВД
- ✓Не проводились тестирования модулей плана ОНиВД в форме учений
- ✓Запасной выход был перекрыт металлической решеткой, подъезд к дому заблокирован запаркованными автомобилями
- ✓Проверки пожарным надзором не проводились с 2001 года

Теракт 11 сентября 2001 года в башне Всемирного торгового центра Нью-Йорка

Удалось спасти большинство сотрудников JPMorgan Stanley (2687 человек), которые располагались на 29 этажах (с 44 по 73) Южной башни, благодаря организованным действиям во время эвакуации из горящего здания

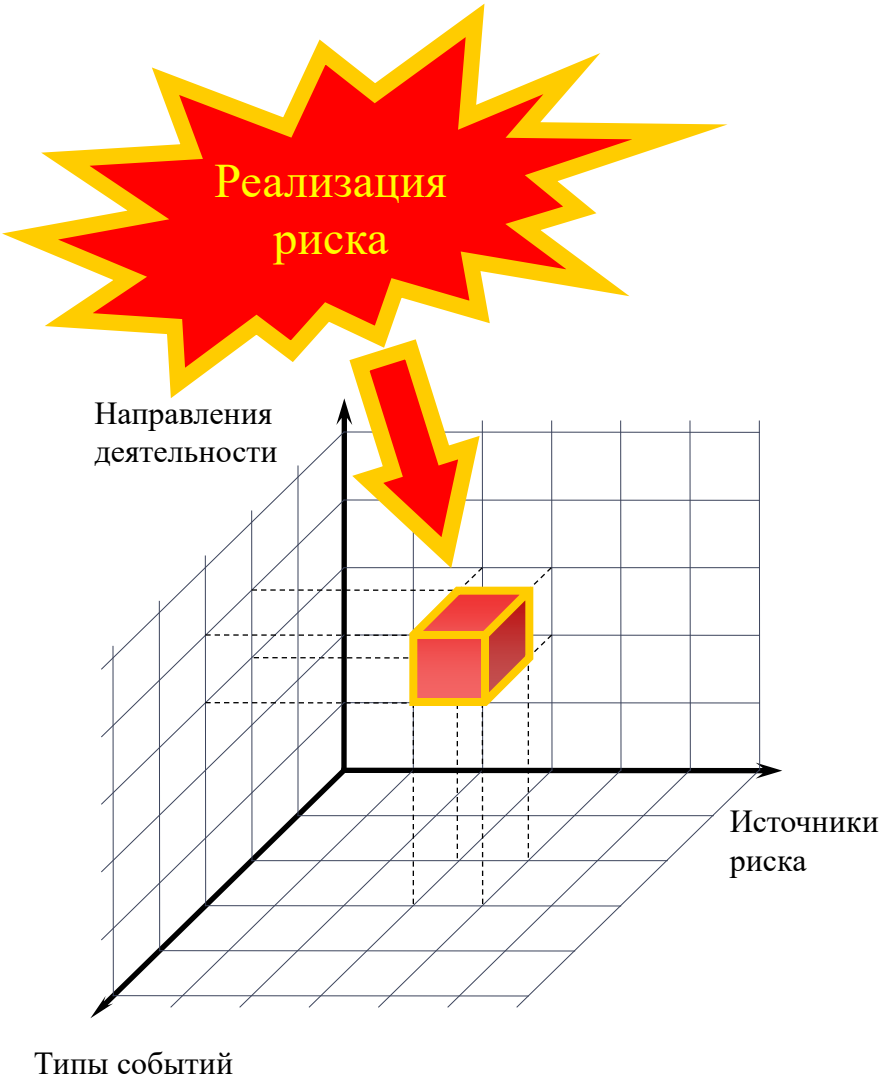
Глава службы безопасности регулярно проводил учения и научил сотрудников правильно вести себя в критической ситуации

# Состав операционного риска в рамках 716-П


В соответствии с 716-П отдельные виды ОР в могут управляться децентрализованно, специализированными подразделениями (не обязательно службой управления рисков)

При этом все подразделения должны придерживаться единой методологии

# Риск — всегда «где-то»



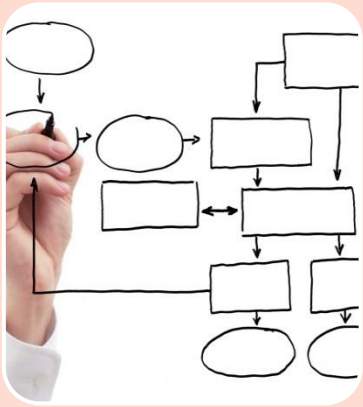

**Операционные риски классифицируются:**

- по источникам риска (почему?)
- по типам событий риска (что?)
- по объектам риска (где?)
- по видам убытков (сколько?)
- по иным классификаторам

**Классификация рисков позволяет:**

- строить аналитические отчеты в любых разрезах
- выявлять основные источники риска, которым подвержена организация
- выявлять наиболее подверженные риску объекты

# Источники операционного риска



## Персонал

- Квалификация
- Мотивация
- Загруженность
- Незаменимость
- Трудовые споры
- Ошибки
- Халатность
- Несанкционированные действия
- Противоправные действия

## Процессы

- Организация процессов, несоответствие масштабам поставленных задач
- «Избыточность» процессов
- Дублирование функций
- Ошибки распределения полномочий
- Неполная документированность

## Системы

- Недостаточная автоматизированность
- Недостаточная емкость систем, несоответствие масштабам поставленных задач
- Сбои и ошибки
- Качество данных

## Внешняя среда

- Внешнее мошенничество, в т.ч. кибер-мошенничество
- Природные явления
- Социально-политические события
- Техногенные катастрофы
- Изменения в области законодательства

# Типы событий операционного риска

| | |
|---|---|
| **Внешнее мошенничество** | • случаи преднамеренных противоправных действий третьих лиц |
| **Внутреннее мошенничество** | • случаи преднамеренной несанкционированной деятельности с участием хотя бы одного аффилированного с организацией лица (включая лиц, работающих на территории организации) |
| **Кадровая политика и безопасность труда** | • случаи несоблюдения трудового законодательства; иски (бывших) работников; убытки от несчастных случаев, произошедших с работниками, а также случаи всех видов дискриминации работников |
| **Клиенты, продукты и деловая практика** | • случаи нарушений законодательства; неисполнения возникающих из договоров обязательств перед клиентами, контрагентами и / или иными третьими лицами; нарушений обычаев делового оборота |
| **Ущерб материальным активам** | • обстоятельства непреодолимой силы, возникшие в результате стихийных бедствий, человеческих действий, нанесшие ущерб активам, повлекшие за собой срыв бизнес-деятельности полностью либо частично, и иные последствия |
| **Перебои в деятельности и системные сбои** | • случаи неработоспособности любых банковских компьютерных систем, аппаратуры или программного обеспечения, в том числе, по причине логических или структурных несоответствий, телекоммуникационных сбоев, нарушения электроснабжения и т. д. |
| **Исполнение, оказание услуг и управление процессами** | • случаи ненадлежащей организации деятельности, ошибок управления и исполнения, ошибок при вводе и обработке данных по операциям и сделкам, утери документов и т. п. |

# Объекты операционного риска

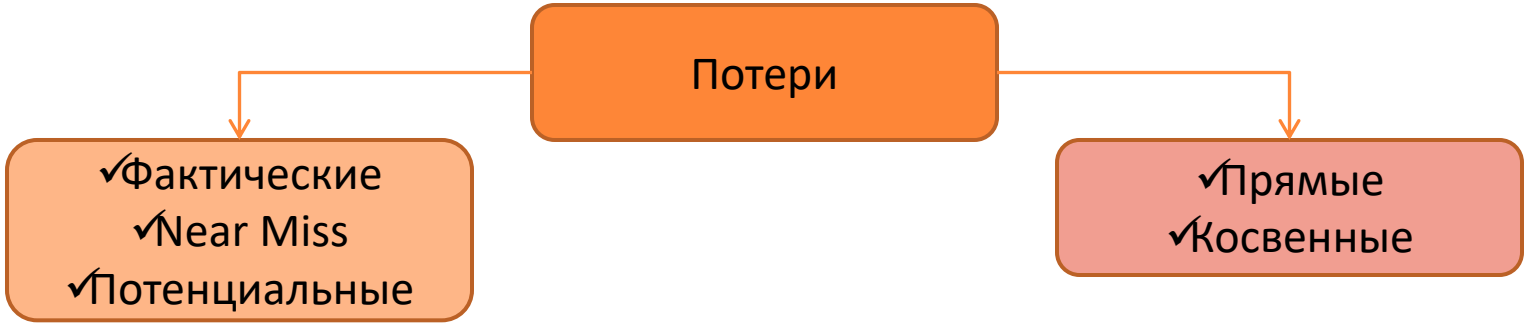
- Направления деятельности (фиксированы для кредитных организаций)

| |
|---|
| корпоративное финансирование |
| операции и сделки на финансовом рынке |
| розничное банковское обслуживание |
| коммерческое банковское обслуживание корпоративных клиентов |
| осуществление переводов денежных средств, платежей и расчетов через платежные системы |
| агентские и депозитарные услуги |
| управление активами |
| розничное брокерское обслуживание |
| обеспечение деятельности кредитной организации |

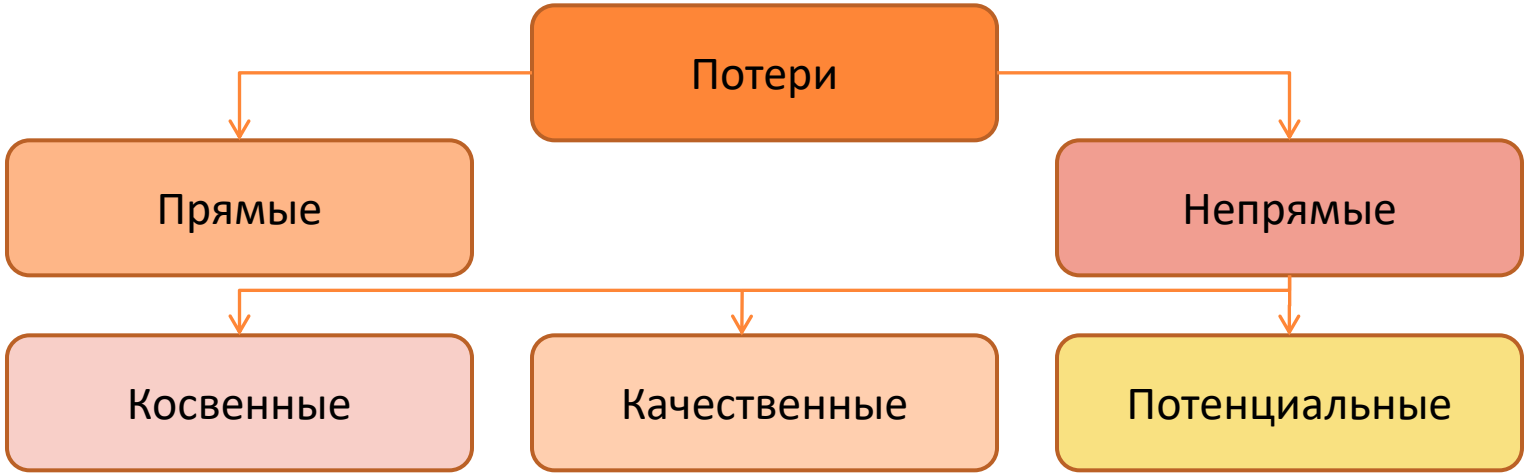
- Процессы
- Продукты
- Организационная структура
- ИТ-системы
- Иные объекты, аналитика по которым важна для организации

# Потери от операционного риска

«Классика»




«Потери по 716-П»



# Идентификация операционных рисков

# 2. Элементы системы управления операционным риском

1. Из каких элементов состоит система управления операционным риском?
2. От чего зависит успех функционирования системы управления операционным риском в организации?

# Цикл управления операционным риском

# Оценка операционного риска

Цель оценки – определить значимость каждого риска для дальнейшего выбора стратегии управления

Оценка

Проблема оценки – не все риски можно измерить количественно, в то время как единственная понятная для всех единица измерения – **деньги**

Количественная

Качественная

Расчет ожидаемых потерь

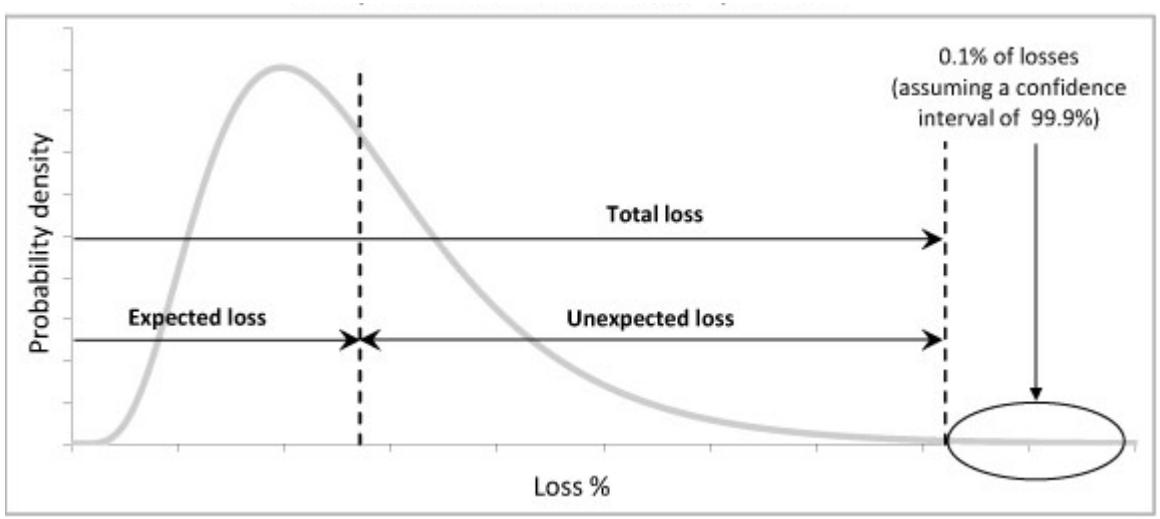
Расчет капитала (для банков)

Сценарный анализ, анализ «что если»

Самооценка

# Оценка операционного риска

- Ожидаемые потери – потери от ОР в результате реализации рисков, вероятность которых высока, а величина потерь низкая. Обычно покрываются за счет денежного потока, планируемых доходов/расходов, включаются в премию за риск
- Неожидаемые потери – потери от ОР в результате редких событий с значительным ущербом. Обычно покрываются собственными средствами (капиталом)
- Катастрофические потери – потери в результате реализации рисков, вероятность которых очень мала, а ущерб огромен. Для таких случаев разрабатываются планы обеспечения и непрерывности деятельности, используется страхование



# Оценка значимости операционного риска

Каждый риск оценивается по следующим параметрам:

- Вероятность наступления
- Серьезность последствий
- Эффективность контролей

Для каждого параметра должна быть установлена шкала измерения, например:

| Балл | Вероятность наступления |
|---|---|
| 0,2 | Вероятность реализации риска очень мала |
| 0,4 | Риск, скорее всего, не реализуется |
| 0,6 | О наступлении риска нельзя сказать ничего определенного |
| 0,8 | Риск, скорее всего, реализуется |
| 1 | Вероятность реализации риска очень высока |

| Балл | Эффективность контролей |
|---|---|
| 0 | Существующие контроли неэффективны |
| 0,2 | Существующие контроли малоэффективны |
| 0,4 | Об эффективности существующих контролей нельзя сказать ничего определенного |
| 0,6 | Существующие контроли эффективны |
| 0,8 | Существующие контроли полностью устраняют риск |

# Оценка значимости операционного риска

| Балл | Серьезность последствий | | | | |
|---|---|---|---|---|---|
| | Финансовые потери | Прерывание деятельности | Репутационные потери | Санкции со стороны регулирующих органов | Ущерб здоровью/жизни персонала |
| 1 | Менее 1 миллионов рублей (до 0,01% капитала) | Краткосрочное прерывание деятельности (на несколько минут) с последующим восстановлением | - | - | - |
| 2 | От 1 до 10 миллионов рублей (от 0,01% до 0,1% капитала) | Прерывание выполнения отдельных бизнес-процессов (далее - БП) на срок менее 4 часов | Единичные публикации в региональных СМИ, не оказывающие существенного влияния на деятельность | Возможное получение предписаний со стороны регулятора | - |
| 3 | От 10 до 50 миллионов рублей (от 0,1% до 0,5% капитала) | Прерывание выполнения отдельных БП на срок от 4 часов до 1 дня / прерывание деятельности Банка на срок менее 4 часов | Незначительное сокращение доли рынка для некоторых продуктов (рынков) / единичный уход персонала / освещение в региональных СМИ | Получение предписаний об устранении нарушений | - |
| 4 | От 50 до 100 миллионов рублей (от 0,5% до 1% капитала) | Прерывание выполнения отдельных БП на срок более 1 дня / прерывание деятельности Банка на срок от 4 часов до 1 дня | Сокращение доли рынка для некоторых продуктов (рынков) / частичный уход персонала / понижение рейтингов / освещение в национальных СМИ | Ограничение проведения / запрет на осуществление отдельных операций / изменение значений обязательных нормативов / предложение о докапитализации | Причинение ущерба здоровью персонала |
| 5 | Свыше 100 миллионов рублей (более 1% капитала) | Прерывание деятельности Банка на срок более 1 дня | Потеря доверия к организации / существенное сокращение доли рынка / массовый уход персонала / значительное понижение рейтингов / освещение в национальных и международных СМИ | Смена руководства / ввод временной администрации / приостановление деятельности / отзыв лицензии | Причинение ущерба жизни / здоровью персонала |

# Оценка значимости операционного риска

На основе данных оценок параметров рассчитывается значимость риска:

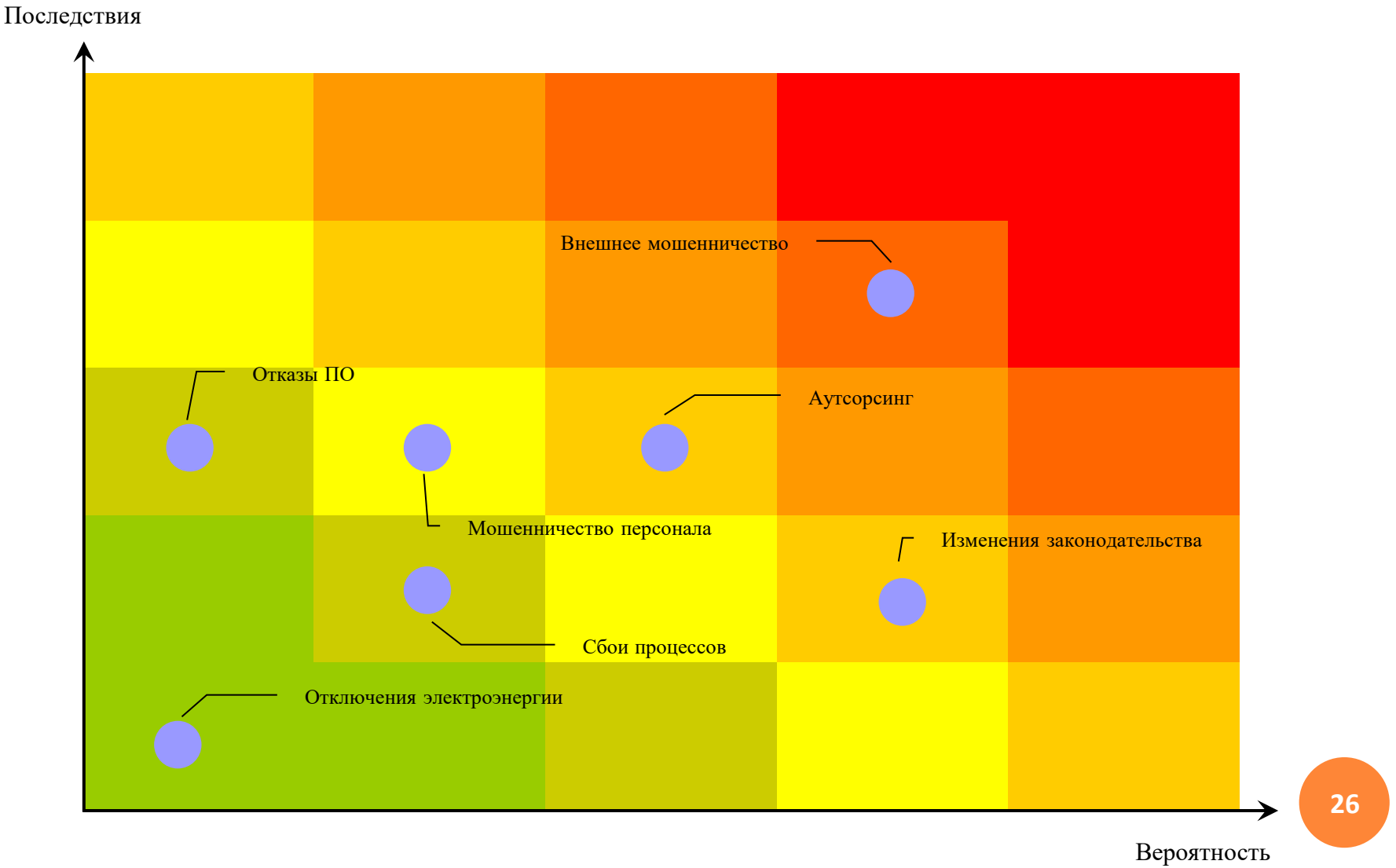
Итоговый балл =
Балльная оценка вероятности*
*Денежная оценка последствий от реализации риска*
*(1-Балльная оценка эффективности контроля)

Например:

| Значимость риска | Итоговый балл |
|---|---|
| Низкая | менее 1 млн. руб. |
| Средняя | От 1 до 10 млн. руб. |
| Высокая | более 10 млн. руб. |

Исходя из полученной значимости риска производится выбор стратегии управления данным риском

# Карта рисков (пример)



# Самооценка операционного риска

| | Тип риска *1* | Тип риска *2* | … | Тип риска *N* |
|---|---|---|---|---|
| Объект риска *1* | | ✓ | ✓ | |
| Объект риска *2* | ✓ | ✓ | | ✓ |
| … | | | | |
| Объект риска *K* | | ✓ | ✓ | ✓ |

Эксперты помимо правил проведения опроса должны понимать:

- ✓зачем проводится опрос
- ✓свою пользу от участия в опросе (опрос – не пустая трата рабочего времени)
- ✓«ненаказуемость» правды

Успех опроса зависит от выбора экспертов и их заинтересованности в участии!

# Самооценка операционного риска

**1.**
Тип риска может реализоваться на объекте?(Y/N)?

**2.**
Опишите типовой сценарий реализации данного типа риска для данного объекта

**3.**
Наблюдались ли случаи реализации данного сценария? Опишите, если да

**4.**
Оцените серьезность последствий и вероятность для данного сценария (качественно и. при возможности, количественно)

**5.**
Опишите существующие контроли для данного сценария

**6.**
Оцените эффективность контролей для данного сценария

**7.**
Опишите возможные мероприятия по управлению риском для данного сценария

**8.**
Задать ещё один типовой сценарий для объекта (Y/N)?

# Ключевые индикаторы риска (КИР)

КИР – количественный показатель, характеризующий динамику уровня риска

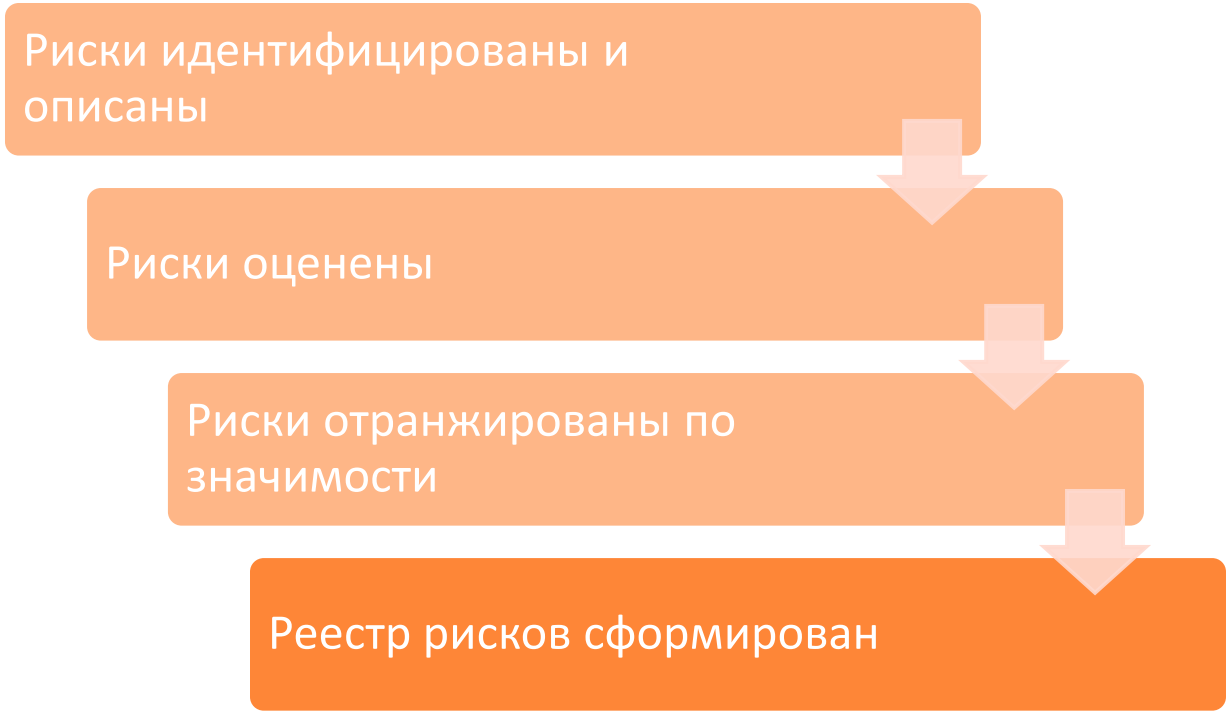
- ✓ опережающие
- ✓ текущие
- ✓ ретроспективные

- ✓ воздействия
- ✓ объемные
- ✓ агрегированные

- ✓ должны быть понятными и простыми для вычисления
- ✓ основываться на объективных данных
- ✓ расчет должен быть проверяемым
- ✓ должны иметь одинаковый набор атрибутов
- ✓ установленные «зоны» КИР должны соответствовать принятой шкале значимости ОР
- ✓ должны регулярно пересматриваться

Положение 716-П также требует устанавливать контрольные показатели уровня ОР

# Реестр рисков




- ✓ Приоритет в управлении – риски с высокой значимостью
- ✓ Разная значимость рисков – разный уровень принятия решений
- ✓ Реестр рисков – «живой» – информация меняется по мере выполнения мероприятий по управлению рисками и выявления новых рисков

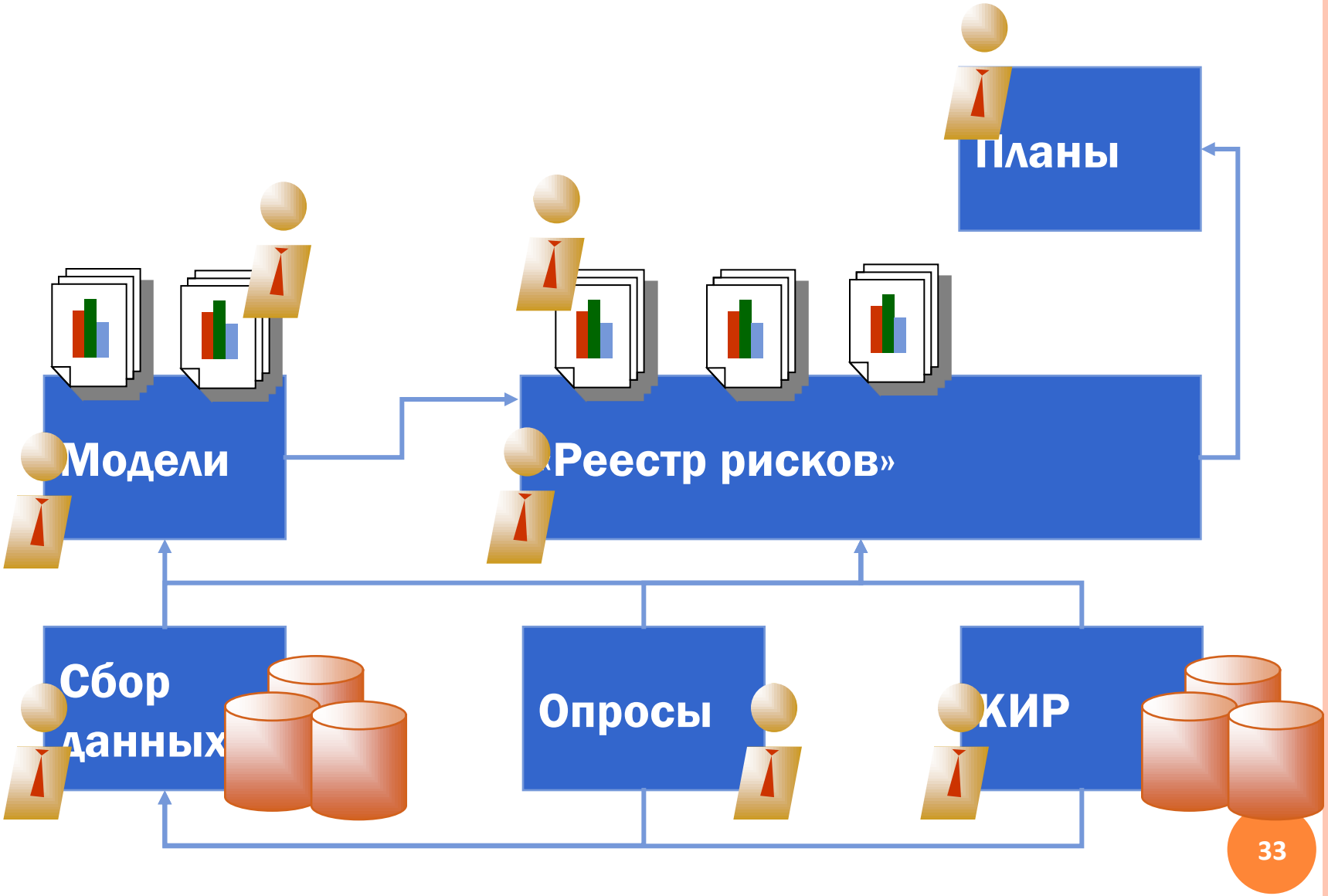
# Управление операционным риском

- Улучшения / реорганизация процессов
- Лимитирование
- Передача риска (страхование, аутсорсинг)
- Контрольные процедуры
- Планы ОНиВД
- Ограничение / избежание риска
- Принятие риска
- Внутренний контроль
- Капитал на покрытие ОР
- И пр.

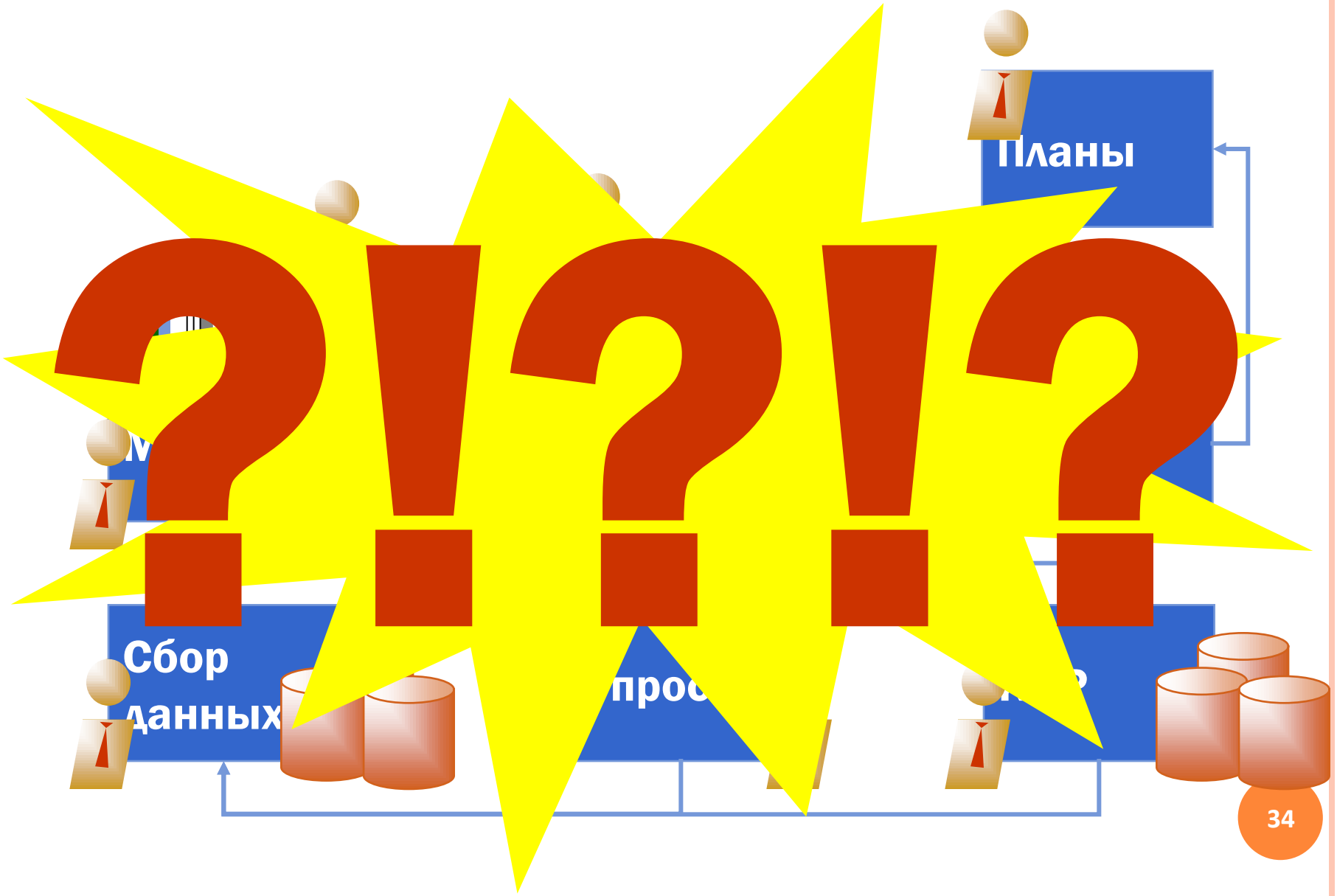
# Управление операционным риском

- Каким риском мы собираемся управлять?
- Каков текущий уровень риска?
- Каков целевой уровень риска?
- К каким объектам риска будет приложено управляющее воздействие?
- В какие сроки будут проводиться мероприятия?
- Какие ресурсы потребуются для управления?
- Кто ответственный за результат?

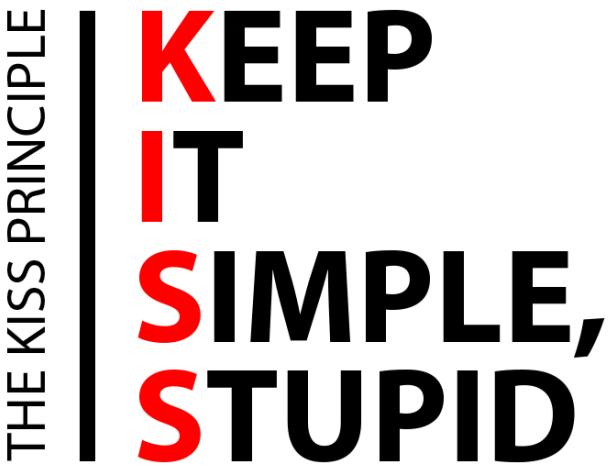
# Как работает СУОР?



# Как НЕ работает СУОР?



# Как работает СУОР?




**Будь проще!**

**Факторы успеха**

- полная поддержка высшего руководства
- мотивация сотрудников на участие в процессе
- минимальная дополнительная нагрузка на сотрудников
- обязательное обучение сотрудников
- доступные методические материалы
- удобная и понятная система взаимодействия

- позитивный имидж службы по операционным рискам
  - реальное взаимодействие, направленное на управление рисками и решение проблем, а не формальный сбор данных
  - неиспользование имеющейся информации о рисках в «карательных» целях

# 3. Участники системы управления операционным риском

1. Кто должен участвовать в управлении операционным риском?
2. Какие функции должно выполнять подразделение/служащий, ответственный за управление операционным риском в организации?

# Концепция «осознания рисков»

- Риск-менеджмент – это форма деловой ответственности на всех уровнях управления организации
- Высшее руководство должно быть осведомлено о возможных причинах потерь, для того, чтобы выработать комплекс превентивных и защитных мер
- Ответственность за предотвращение нежелательных рисков должна быть распределена между сотрудниками на всех уровнях управления в пределах их компетенции

# Решение главной проблемы

- Операционный риск — эндогенный по своей природе, следовательно…
- Необходимые богатые внутренние данные, следовательно…
- Необходимо извлекать данные из систем и получать их «на местах», следовательно…
- Необходимо наладить взаимодействия с сотрудниками на всех уровнях организации

# Взаимодействие — ключевое слово

- Высший менеджмент:
  - Управление риском на стратегическом уровне
- Риск-менеджмент:
  - Выработка и корректировка методологии
  - Контроль и аудит
- Линейный менеджмент:
  - Непосредственное управление риском в подразделениях банка
- Функциональные подразделения:
  - Содействие риск- и линейному менеджменту
- Сотрудники — важнейший элемент системы

# 3 линии защиты

| | |
|---|---|
| 1-я линия защиты: все подразделения | • выявление рисков<br>• минимизация рисков в текущей деятельности |
| 2-я линия защиты: риски | • методология<br>• координация работ<br>• свод и обработка информации |
| 3-я линия защиты: аудит | • осуществление текущего независимого контроля и регулярного аудита эффективности СУОР |

# Типичные роли риск-менеджера

## «Финансист риска»

- оценка риска
- оптимизация программ страхования
- расчет капитала

## «Внутренний контролер»

- контроль за соблюдением внутренних правил, методик
- анализ и устранение нарушений

## «Корпоративный советник»

- консультации для руководителей подразделений по вопросам управления рисками
- распространение полезной информации и опыта внутри организации

# Основные функции службы управления ОР

- Координация работ по построению СУОР
- Разработка и внедрение нормативной базы по управлению ОР
- Ведение реестра рисков, базы событий
- Оценка и мониторинг ОР
- Подготовка отчетности по ОР, доведение информации до руководства
- Методологическая поддержка подразделений по вопросам управления ОР
- Координация работ по управлению ОР
- Развитие культуры управления ОР
- *Подготовка планов ОНиВД*

# 4. База событий операционного риска

1. Почему важно вести базу событий операционного риска, и как это делать с пользой, а не для «галочки»?
2. Обязательно ли внедрять ИТ-решения для ведения базы событий операционного риска?

# Регистрация событий


- Данные регистрируются вручную или импортируются из ИТ-систем
- Данные подвергаются ручной очистке, верификации и классификации
- В процесс обработки данных включаются функциональные эксперты и линейные менеджеры
- Риск-менеджер осуществляет общую координацию процесса

# База событий ОР

Регистрационные данные

Даты, связанные с событием

Описание события

Классификация источников риска

Классификация объектов риска

Тип события

Связь с иными видами риска

Классификация потерь

Классификация возмещений

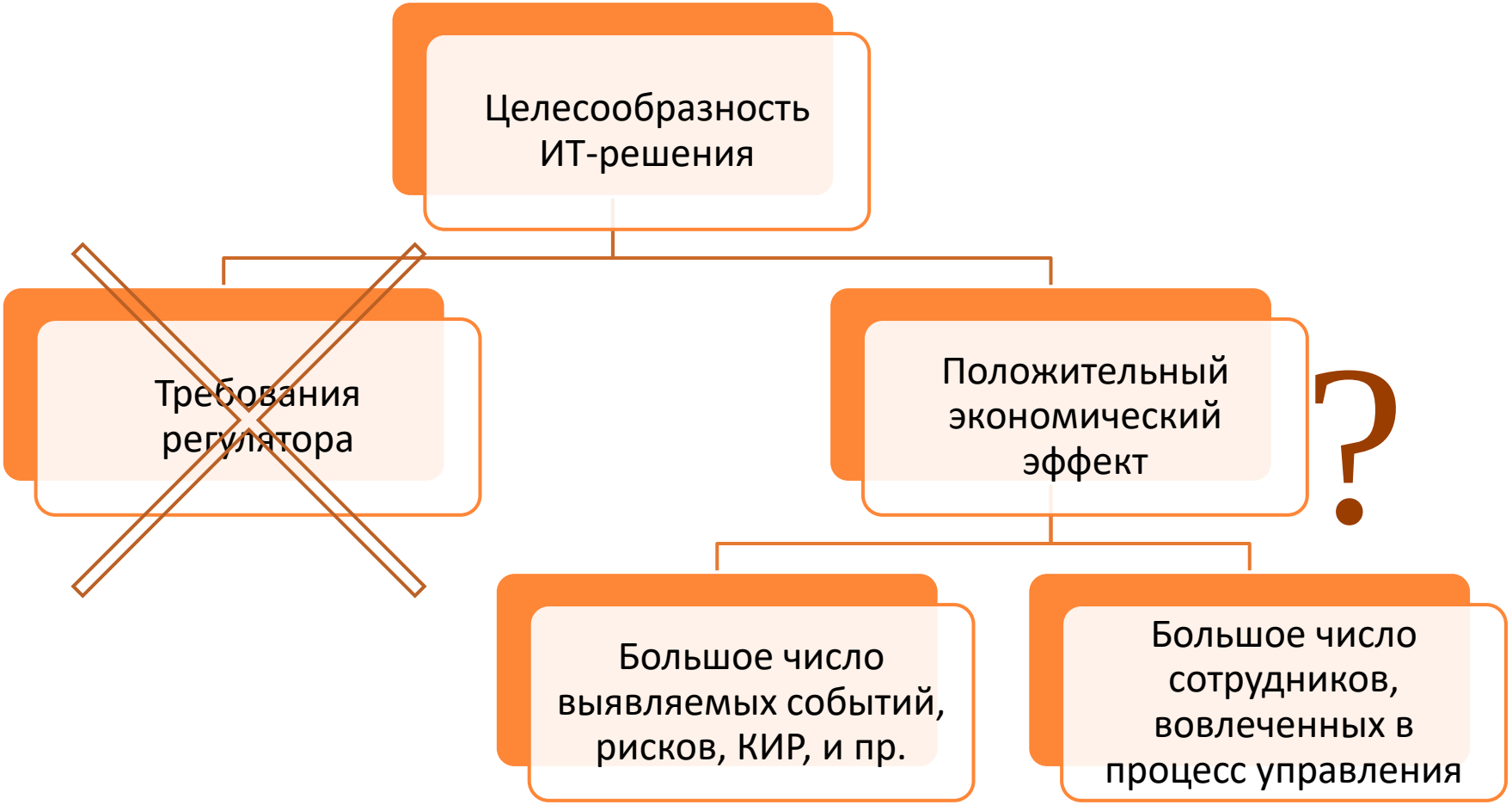
Статусы события

…

Планы по минимизации

База событий показывает уровень управления ОР в организации

# ИТ-решение – нужно ли?



# Преимущества ИТ-решения

- возможность интеграции и автоматического обмена информацией с доступными источниками данных в организации
- доступность ИТ-системы всем подразделениям
- возможность определения ролей пользователей
- возможность определения уровней конфиденциальности информации
- фиксация (логирование) всех действий пользователя в системе
- историчность данных
- невозможность удаления информации, внесенной в систему
- возможность автоматической переклассификации событий при внесении изменений в классификаторы
- уведомление пользователей о необходимых к совершению действиях в системе
- возможность планирования и отслеживания выполнения мероприятий по управлению риском
- возможность анализа данных и построения управленческой отчетности в любых разрезах
- формирование фиксированной отчетности на любую дату
- …

# 5. Отчетность по операционному риску

1. Как составить информативную и полезную отчетность по операционному риску?

# Отчетность по операционному риску

Периодичность предоставления:
•дневной
•месячный
•квартальный
•годовой

Форматы предоставления

Уровни предоставления:
•руководитель СУР
•бизнес-подразделения
•комитет по рискам
•правление
•совет директоров
•регулятор

Отчетность должна быть:
✓краткой
✓информативной
✓позволять принимать управленческие решения

# Отчетность по операционному риску

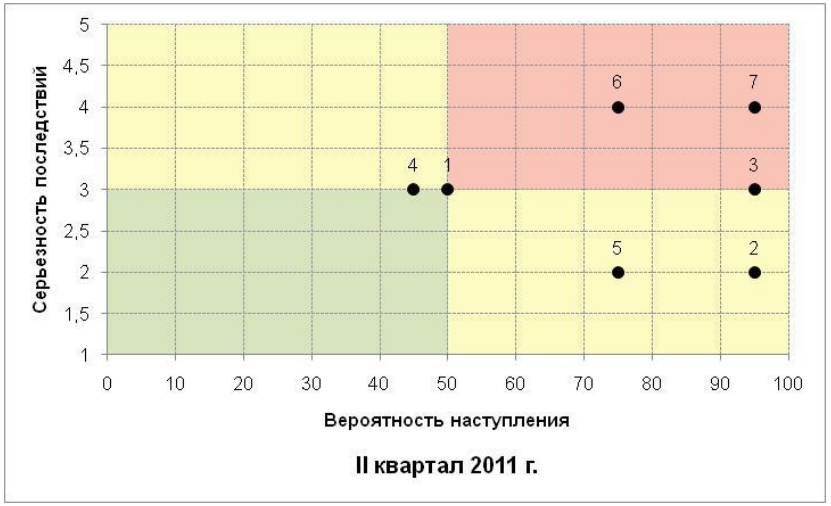
| Тепловая карта рисков в разрезе процессов на основе событий ОР, пример | Внутреннее мошенничество | Внешнее мошенничество | Кадровая политика и безопасность труда | Клиенты, продукты, деловая практика | Ущерб материальным активам | Перебои в деятельности и системные сбои | Исполнение, оказание услуг и управление процессами | Общий итог |
|---|---|---|---|---|---|---|---|---|
| **Процессы управления** | **0 / 0** | **0 / 0** | **1/ 0** | **1 / 0** | **0 / 0** | **1 / 0,3 млн. руб.** | **0 / 0** | **3 / 0,3 млн. руб.** |
| Процесс 1 | | | 1 / 0 | | | 1 / 0,3 млн. руб. | | 2 / 0,3 млн. руб. |
| Процесс 2 | | | | 1 / 0 | | | | 1 / 0 |
| **Основные процессы** | **2 / 10 млн. руб.** | **3 / 60 млн. руб.** | **0 / 0** | **0 / 0** | **0 / 0** | **3 / 0** | **9 / 0,8 млн. руб** | **17 / 70,8 млн. руб.** |
| Процесс 3 | 2 / 10 млн. руб. | | | | | | 4 / 0 | 6 / 10 млн. руб. |
| Процесс 4 | | 3 / 60 млн. руб. | | | | 3 / 0 | 5 / 0,8 млн. руб. | 11 / 60,8 млн. руб. |
| **Поддерживающие процессы** | **0 / 0** | **0 / 0** | **0 / 0** | **0 / 0** | **0 / 0** | **3 / 0** | **0 / 0** | **3 / 0** |
| Процесс 5 | | | | | | 3 / 0 | | 3 / 0 |
| **Общий итог** | **2 / 10 млн. руб.** | **3 / 60 млн. руб.** | **1 / 0** | **1 / 0** | **0 / 0** | **7 / 0,3 млн. руб.** | **9 / 0,8 млн. руб.** | **23 / 71,1 млн. руб.** |

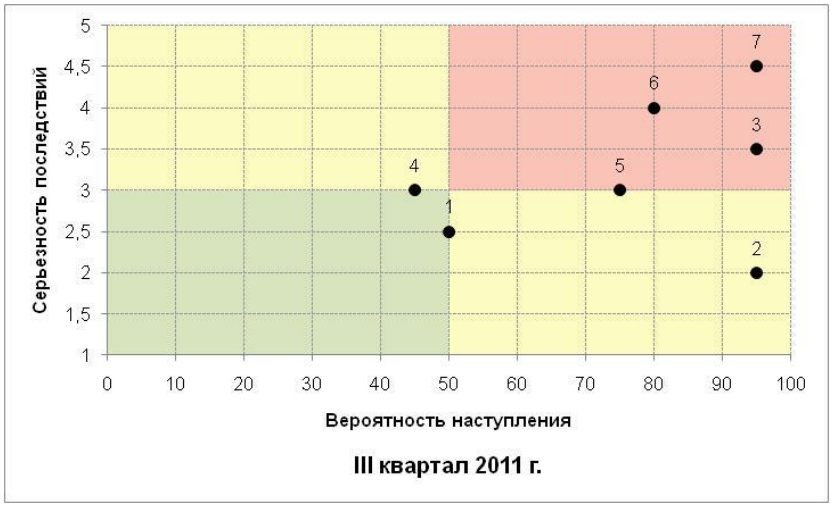


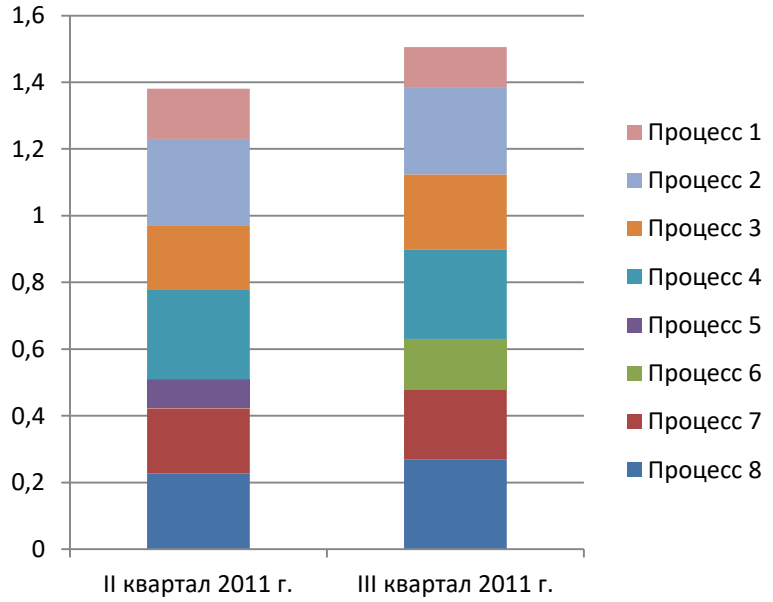
*Низкий риск* | *Средний риск* | *Высокий риск*

*x / y – число событий/величина потерь*

# Отчетность по операционному риску



# Отчетность по операционному риску

Вне зависимости от формата предоставления отчетность должна содержать данные:

- о понесенных потерях вследствие реализации ОР
- о крупнейших событиях и принятых мерах по минимизации
- о существенных рисках и планах по управлению ими
- данные, на основании которых требуется принятие управленческих решений

# Отчетность по операционному риску

- При этом данные отчетности должны быть полными и объективными:

Отчет 1:
- ✓Потери от взлома банкоматов за 2020 г. составили 17 млн. руб.

Отчет 2:
- ✓Потери от взлома банкоматов за 2020 г. составили 17 млн. руб.
- ✓При этом по каждому событию было получено страховое возмещение

Отчет 3:
- ✓Потери от взлома банкоматов за 2020 г. составили 17 млн. руб.
- ✓При этом по каждому событию было получено страховое возмещение
- ✓По полису страхования банкоматов на 2020 г. была уплачена страховая премия в размере 40 млн. руб.

# 6. Новые требования Банка России для кредитных организаций

1. Положение 716-П
2. Положение 744-П

# Положение 716-П

Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Разработано с целью:

- подготовки к внедрению нового стандартизированного подхода к оценке операционного риска для целей расчета норматива достаточности капитала
- формализации требований к риску информационной безопасности и информационных систем

Все КО должны привести систему управления операционным риском в соответствие требованиям Положения 716-П к **01.01.2022**

# Положение 716-П

- Глава 1. Общие положения
- Глава 2. Классификации, используемые в системе управления операционным риском
- Глава 3. Требования к процедурам управления операционным риском
- Глава 4. Требования к отдельным элементам системы управления операционным риском
- Глава 5. Требования к системе контрольных показателей уровня операционного риска
- Глава 6. Требования к ведению базы событий операционного риска
- Глава 7. Требования к управлению риском информационной безопасности
- Глава 8. Требования к управлению риском информационных систем
- Глава 9. Особенности применения норм в зависимости от вида банка
- Глава 10. Заключительные положения
- Приложение 1. Контрольные показатели уровня операционного риска
- Приложение 2. Подходы к расчету объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации операционного риска
- Приложение 3. Рекомендуемый перечень возможных мер, направленных на уменьшение негативного влияния операционного риска
- Приложение 4. Детализированная классификация типов событий операционного риска
- Приложение 5. Подходы к дополнительной классификации риска информационной безопасности

# Положение 744-П

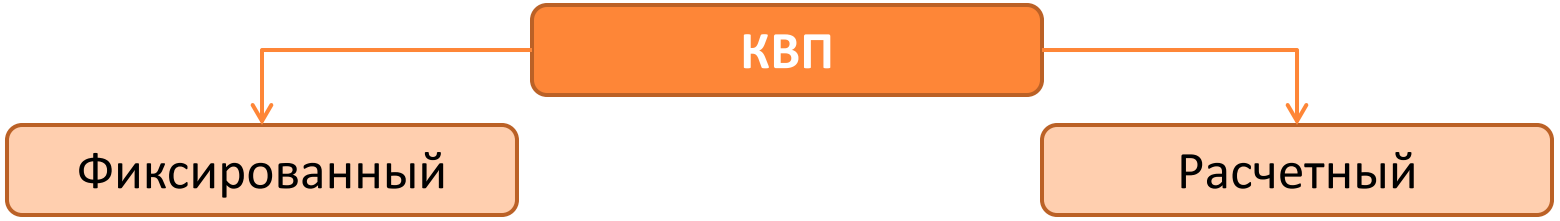
Положение № 744-П от 07.12.2020 «О порядке расчета размера операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением»

Размер ОР рассчитывается в соответствии с Базель III:

$$ОР = КБИ * КВП,$$

где *КБИ* – величина компонента бизнес-индикатора, зависит от размера КО и рассчитывается на основании форм отчетности 0409102, 0409127

*КВП* – коэффициент внутренних потерь:




$КВП = 1 + КНП$

где *КНП* – коэффициент неучтенных потерь
*ПП* – прямые потери

$КВП = КВП_{Б} + КНП$

$$КВП_{Б} = \ln\left(1{,}71828 + \left(\frac{ПП}{КБИ}\right)^{0{,}8}\right)$$

# 7. Основные ошибки при построении системы управления операционным риском

1. Какие типичные недостатки встречаются в организации систем управления операционным риском в финансовых организациях?

# Что может пойти не так?

При построении

- Руководство не заинтересовано в СУОР
- СУОР создается «для галочки»
- СУОР слишком «накручена»
- Подразделения не видят пользу от СУОР
- Отчетность неинформативна и не дает повода для принятия решений
- …

При проверке

- Неполное соблюдение требований регулятора
- Несогласованность документов между собой
- Несогласованность документов и действий
- Несоблюдение документов
- Неполнота собираемой информации о рисках
- Видимое отсутствие действий по управлению ОР
- Формальность процедур по управлению ОР
- …

# Спасибо за внимание!