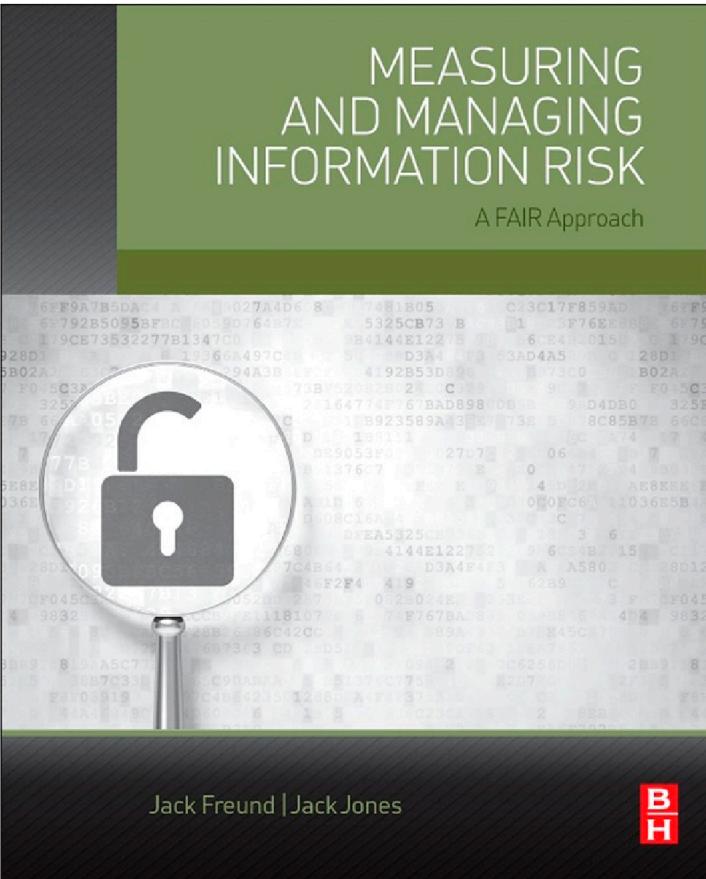


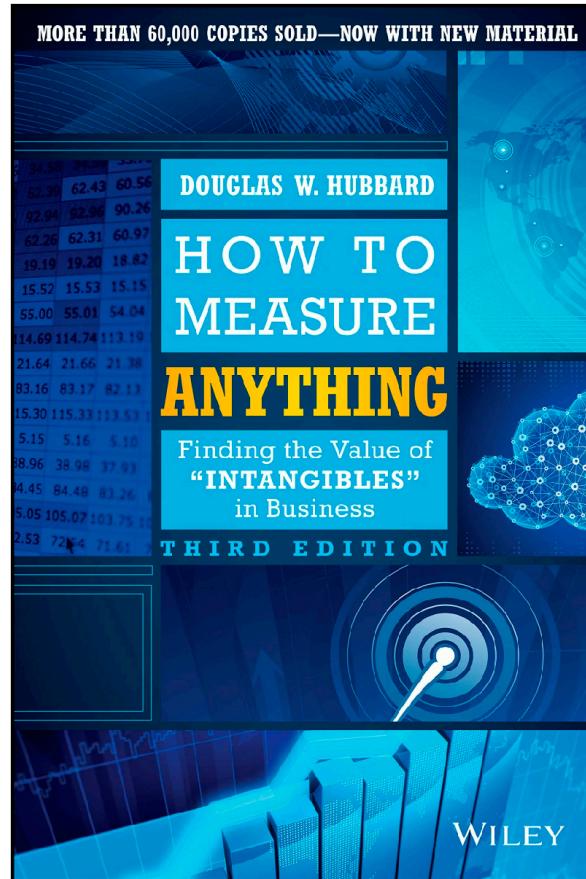
Применение data-driven подходов к управлению рисками в некредитных финансовых организациях

Основа подхода

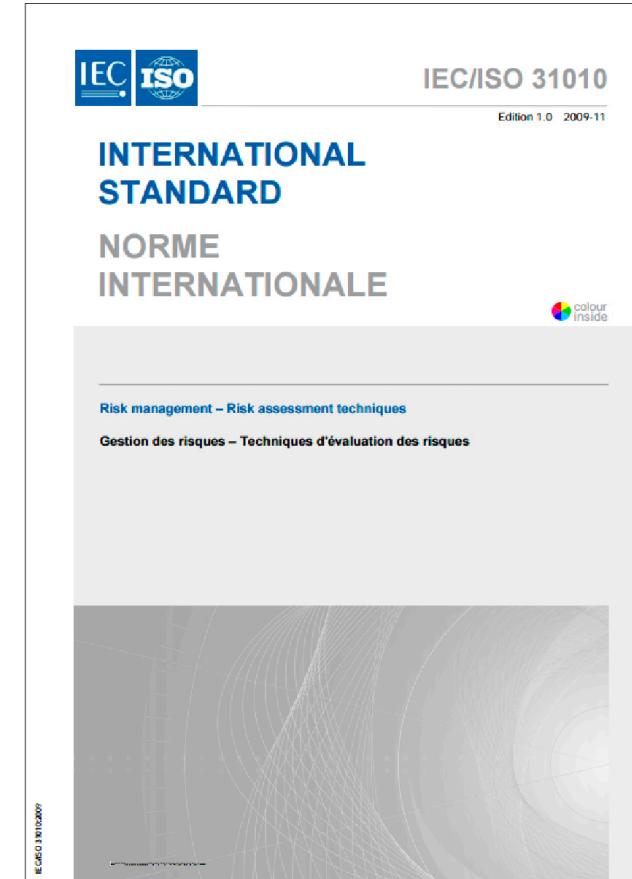
Measuring and Managing Information Risk



How to measure anything

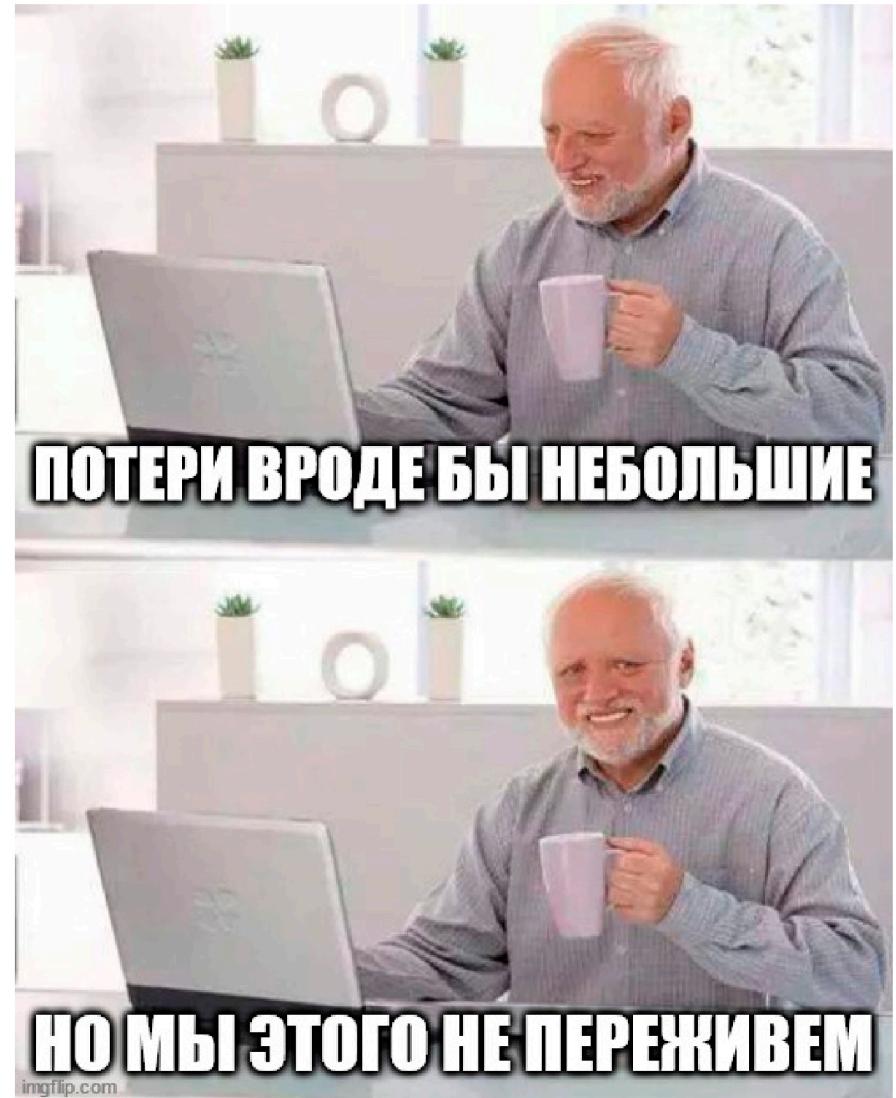


ISO 31010-2019



Оценка vs Управление

- ▶ хорошо выстроенный процесс управления рисками - важнее, чем идеально проведенный процесс оценки рисков
- ▶ контекст принятия решений может быть разным
- ▶ формат оценки рисков должен подходить под задачу принятия решений



Приятие решений, основанное на данных

Управление рисками ВСЕГДА начинается с понимания внутреннего и внешнего контекста организации, а не с поиска банка угроз под оценку рисков

Для того, чтобы ЛПР лучше понимал результаты анализа рисков, может быть удобным начинать с понимания событий потерь, свойственных для организации

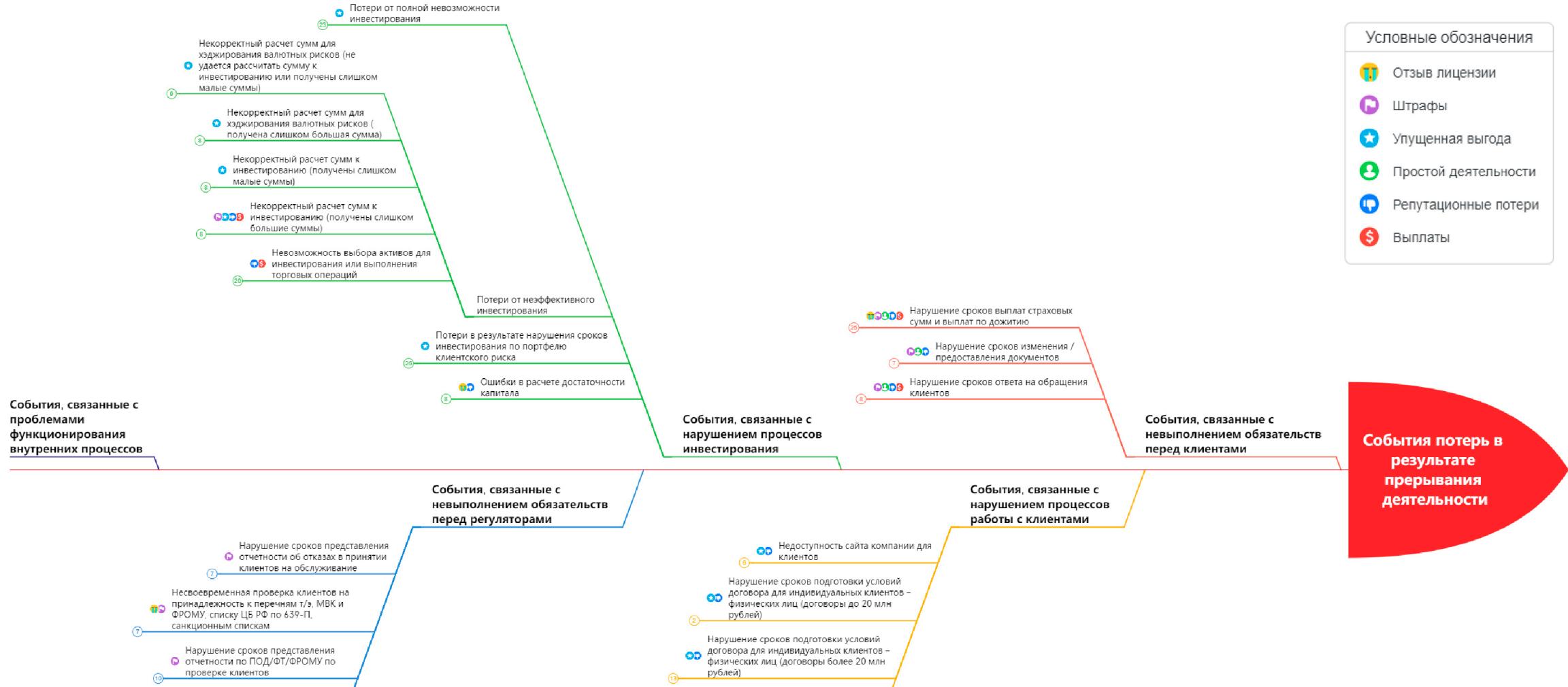
От понимания событий потерь приходит понимание активов, воздействий на активы и источников угроз, которые нужно рассматривать

Риски можно представлять как сценарии "источник угрозы - воздействие - актив"

Принятие решений, основанное на данных: какие данные у нас есть



Принятие решений, основанное на данных: события потерь



Принятие решений, основанное на данных: источники угроз

Клиенты и представители клиентов

Мотив финансовая выгода

Основное намерение кражи денег

Финансирование отсутствует

Предпочитаемые цели клиентские системы

Способности нет / минимальные

Полномочия

Взаимодействие с иными источниками угроз пользователь клиентских систем, веб-сайта

нет

Степень принятия собственных рисков низкая: компании известны их персональные данные, компания обрабатывает их финансовую информацию

Привилегированные работники

случайное воздействие, ошибка, финансовая выгода, месть

сбор данных для продажи, кражи денег, ненамеренное воздействие, изменение корпоративных политик, нанесение ущерба работодателю

отсутствует

системы, к которым работник имеет привилегированный доступ
системы, в которых тяжело отследить факт мошенничества

минимальные: обладают высокими общими навыками в сфере ИТ, но при этом не обладают навыками взлома

администратор отдельных систем

нет / могут финансироваться преступными группами

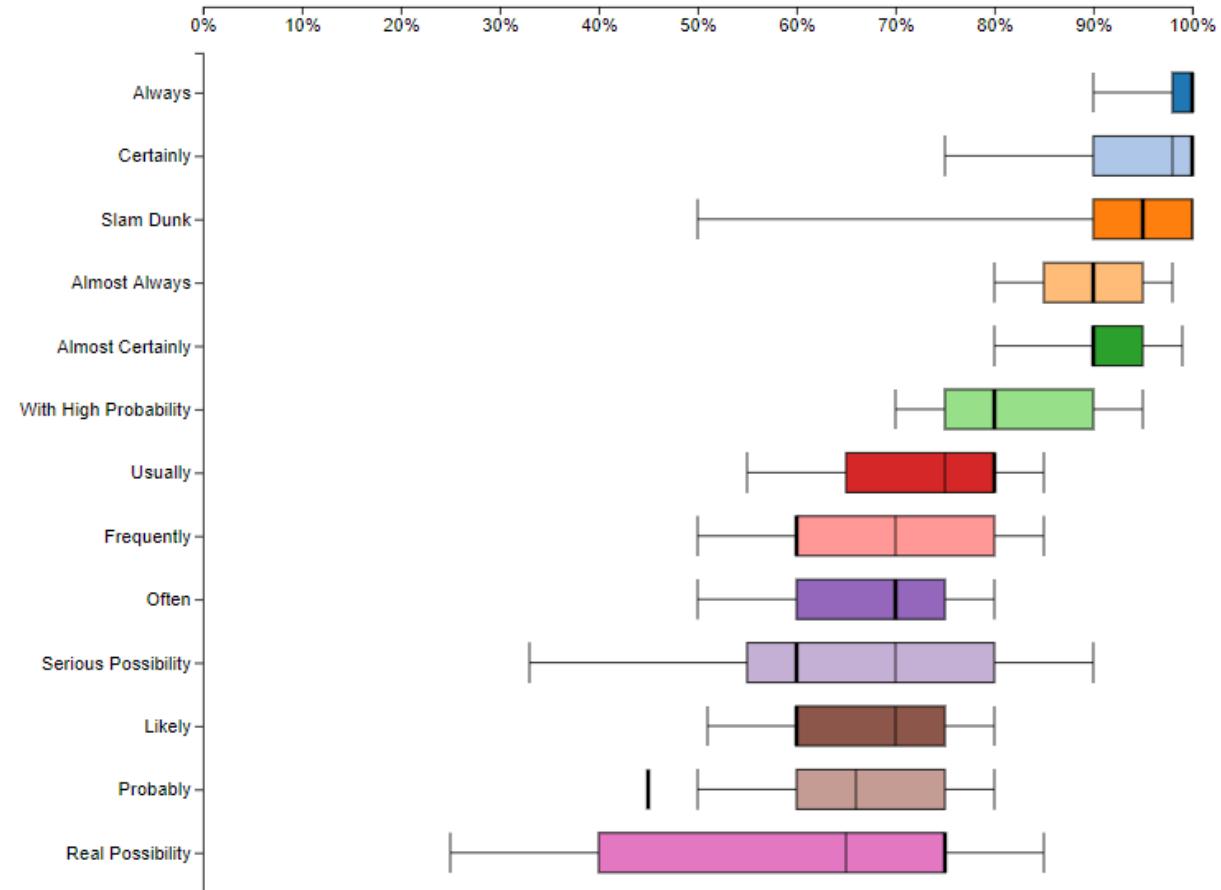
низкая: чаще всего достаточно дорожат местом работы и не готовы его потерять, при этом хорошо осведомлены в вопросах ИТ и понимают возможности нелегитимных действий

Принятие решений, основанное на данных: активы

Система	Описание последствий для бизнеса от нарушения свойств информации					
	Конфиденциальности		Целостности		Доступности	
	Кража без публикации	Публикация	Случайное изменение	Целенаправленное искажение	Недоступность системы / файлового ресурса	Уничтожение информации
собственные системы						
СЭД	- использование финансовых данных, ПДн клиентов, ВНД, замечаний к процессам и системам, коммерческой тайны конкурентами - снижение репутации	- штрафы за утечку ПДн клиентов - снижение репутации - использование финансовых данных, персональных данных клиентов, ВНД, замечаний к процессам и системам, коммерческой тайны конкурентами - раскрытие детальных данных о финансовой деятельности	- прямой риск финансовых потерь по инвестированию - санкции регуляторов за ошибки в представленных данных - некорректные решения по Убыткам - ошибки в переводах денежных средств - финансовые и операционные риски по хоз.деятельности - выплата неустойки контрагентам	- прямой риск финансовых потерь по инвестированию - санкции регуляторов - некорректные решения по Убыткам - перевод денежных средств мошенникам - финансовые и операционные риски по хоз.деятельности - выплата неустойки контрагентам - заключение договора на невыгодных условиях	- санкции регуляторов - невозможность проведения закупок - задержка в согласовании и подписании ВНД - увеличение длительности урегулирования убытков, заключения договоров с контрагентами, закупок - задержка поступления входящей корреспонденции - выплата неустойки - несвоевременная блокировка клиентов	- санкции регуляторов, аудиторов - невозможность проведения закупок - необходимость нового согласования и подписания ВНД - увеличение длительности урегулирования убытков, заключения договоров с контрагентами, закупок - задержка поступления входящей корреспонденции - выплата неустойки - несвоевременная блокировка клиентов
Jira	- использование коммерческой тайны, ПДн клиентов, информации о правоах заключениях контрагентами - срыв сделок - снижение репутации	- штрафы за утечку ПДн клиентов - снижение репутации - предписания регуляторов - срыв сделок, упущенная выгода - ущерб клиентам - отток текущих и потенциальных клиентов - резонанс в СМИ	- штрафы и предписания регуляторов - снижение репутации - упущенная выгода - некорректные выплаты, выплаты по неверным реквизитам - отток текущих и потенциальных клиентов - жалобы клиентов	- штрафы и предписания регуляторов - снижение репутации - срыв сделок, упущенная выгода - срыв сроков начала продаж нового продукта - нарушение сроков по договорам с клиентами - жалобы клиентов - невыгодные с юридической точки зрения действия бизнеса	- штрафы и предписания регуляторов - снижение репутации - срыв сделок, упущенная выгода - срыв сроков начала продаж нового продукта - нарушение сроков по договорам с клиентами - жалобы клиентов - остановка закупок	- штрафы и предписания регуляторов - снижение репутации - срыв сделок, упущенная выгода - срыв сроков начала продаж нового продукта - нарушение сроков по договорам с клиентами - жалобы клиентов - остановка закупок, необходимость инициирования части закупок заново

Проблема воспроизводимости и пути ее решения

probabilitiesurvey.com



Проблема воспроизводимости и пути ее решения

Работать с рисками можно
на разных уровнях детализации:



Проблема воспроизводимости и пути ее решения

- ▶ Самым частым ответом на вопрос об оценке параметра будет "я не знаю"
- ▶ Может помочь использование диапазонов оценок (оптимизм - ожидание - пессимизм) вместо точечных значений, чтобы у эксперта было поле для предположений и их обоснований
- ▶ Для оценки рисков достаточно точности в 80-90%
- ▶ Такие оценки можно впоследствии учитывать в стат. моделировании уровней рисков



Шкала доверия к оценке

Черновик

ИББ Доклад про data-driven подход к управлению рисками - Сообщение (HTML)

Файл Сообщение Вставка Параметры Формат текста Рецензирование Что вы хотите сделать?

Мы не можем отобразить подсказки прямо сейчас.

Кому... nina-best-designer@infosec.ru
 Копия...
Отправить
Тема ИББ Доклад про data-driven подход к управлению рисками

Нина, привет!

Хочу добавить в презентацию слайд про то, что всяческие наброски / **черновики тоже работают – если получается при их помощи донести основную мысль.** Типа что иногда имеет смысл не заморачиваться сильно над поиском каких-то данных, если их найти очень сложно.

Грубо говоря – иногда это требует полтора месяца гоняться за аналитиками, а в итоге оказывается, что мы могли сделать просто очень грубое предположение («либо вообще ничего не потеряем, либо потеряю миллиона полтора за год») – и на фоне потерь по другим рискам это было бы примерно одинаково информативно.

И если рассматривать такие грубые предположения как черновик (к которому мы вернемся, если увидим, что тут нужно снизить неопределенность) – то они могут помочь нам работать с рисками более эффективно

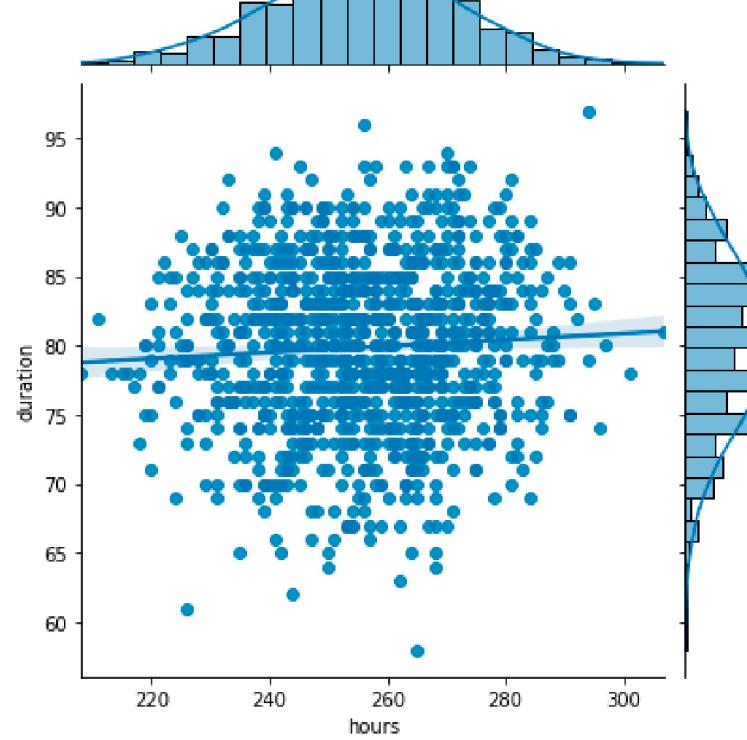
Как думаешь, как это лучше сделать?

С уважением, Евгений Сачков
Начальник отдела систем управления рисками
Департамент консалтинга и аудита

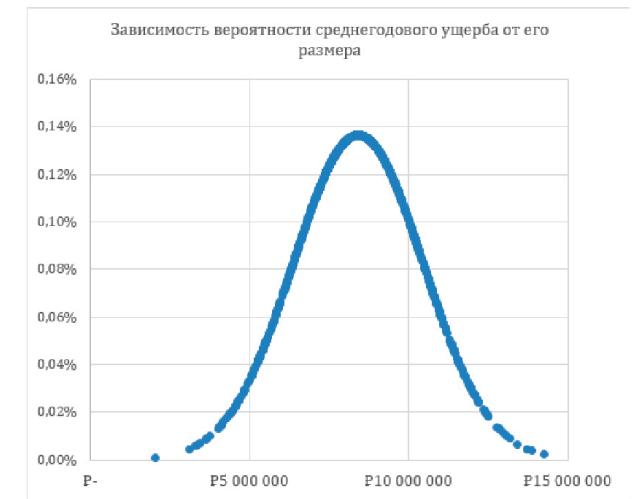
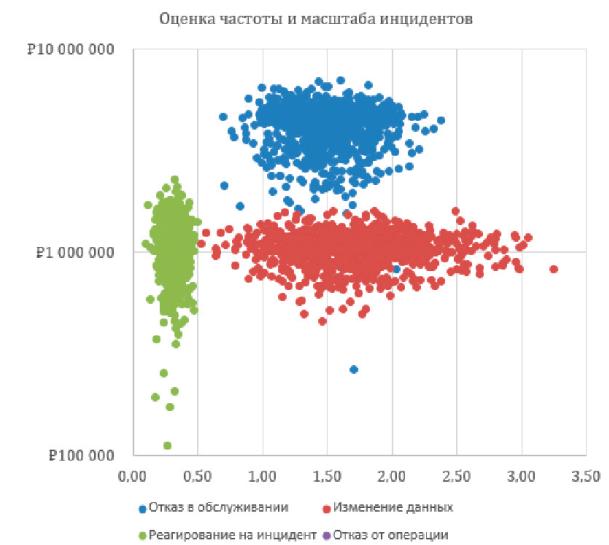
**Информзащита**
Системный интегратор

Телефон: +7 495 980 2345 (доб. 633)
e-mail: e.sachkov@infosec.ru

Приятие решений на данных: пример анализа событий потерь

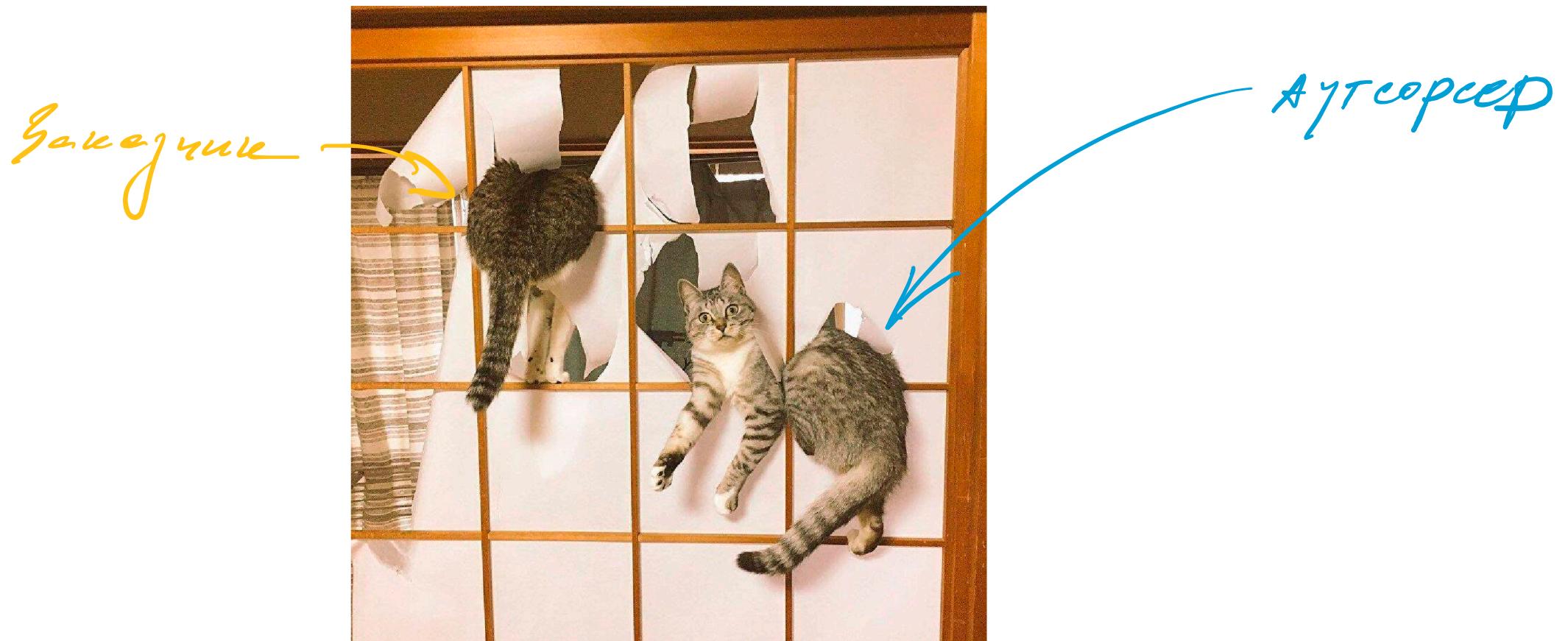


АБС Банка	Левая граница	Ожидаемое	Правая граница
Потери (инцидент)	2 447 905 ₽	6 505 092 ₽	9 245 667 ₽
Частота потерь	1,7	3,2	5,0
Отказ в обслуживании	264 956 ₽	4 381 510 ₽	6 959 157 ₽
Изменение/ подделка	455 768 ₽	1 055 968 ₽	1 596 684 ₽
Реагирование	110 827 ₽	1 107 468 ₽	2 276 166 ₽
Отказ от операции	- ₽	- ₽	- ₽



АБС Банка	Левая граница	Ожидаемое	Правая граница
Потери (за год)	2 046 277 ₽	8 421 305 ₽	14 270 227 ₽
Отказ в обслуживании	451 446 ₽	6 318 216 ₽	11 939 440 ₽
Изменение/ подделка	584 284 ₽	1 742 742 ₽	3 968 624 ₽
Реагирование	29 419 ₽	327 026 ₽	758 778 ₽
Отказ от операции	- ₽	- ₽	- ₽

Оффтоп: Можно ли аутсорсить деятельность по управлению рисками



Информационная безопасность **24x7x365**

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45

izsoc@infosec.ru

www.izsoc.ru

Системный интегратор

+7 495 980 23 45 

market@infosec.ru 

www.infosec.ru 

Центр противодействия мошенничеству

antifraud@infosec.ru

Сервисный центр

+7 495 981 92 22 

support@itsoc.ru 

www.itsoc.ru 

Пресс-служба

pr@infosec.ru