AKTIV.
CONSULTING

Как оценить финансовый ущерб от инцидента

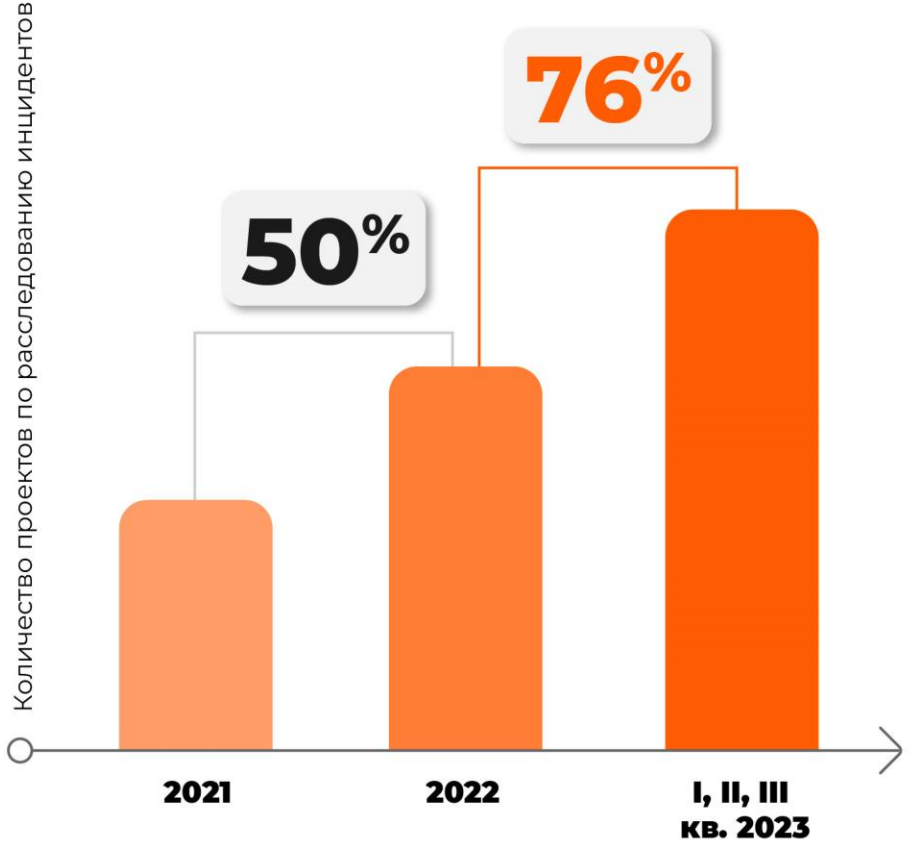
Сергей Шлёнский

Ведущий специалист
по информационной
безопасности

План вебинара

1. **Текущая** ситуация
2. Что является **недопустимым** событием
3. Для чего необходимо **рассчитывать ущерб** от инцидента
4. **Примеры** инцидентов и их последствия
5. **Уровни зрелости** организации
6. Методы **измерения рисков**
7. Прямой и косвенный **ущерб**
8. **Ранжирование** ущерба
9. Что такое **риск-аппетит** и толерантность к рискам
10. **Как считать** будущие потери

Текущая ситуация с инцидентами ИБ в Российской Федерации



Число кибератак на российские компании за прошедший год выросло **в 2,5 раза.**

Следует также отдельно отметить рост числа хорошо подготовленных целенаправленных атак – по сравнению с 2023 годом рост примерно **на 60%.**

Что является недопустимым событием

Недопустимое событие* — событие в результате кибератаки, делающее невозможным достижение операционных и (или) стратегических целей организации или приводящее к значительному нарушению ее основной деятельности.

Для каждой организации существуют такие события, наступление которых может иметь **катастрофические последствия** *(остановка производства, подмена контента («дефейс»), полная или частичная потеря данных и т.д.).*

* Методические рекомендации по формированию перечня недопустимых событий... (Минцифры)

Для чего необходимо считать ущерб?

Для учета в обязательной финансовой отчетности *(при наличии требований)*

Для расчета страхового возмещения

Для оценки затрат на деятельность в области ИБ

Для выплат компенсации клиентам и партнерам

Для сравнения с... <кем-то по отрасли>

Насколько все может быть серьезно

Атака на трейдинговую систему одного крупного регионального банка, в результате которой курс рубля в течение 14 минут менялся на биржевых торгах более чем на 15%.
В течение этого периода волатильности курс колебался от 55 до 66 рублей за $1.

Финансовые потери банка оценивались от 244 до 500 миллионов рублей

Кейс Sony Pictures

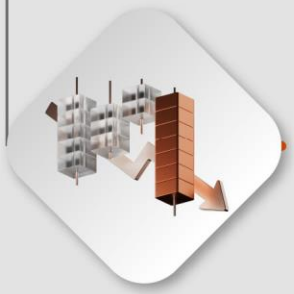
Кража сценариев

Кража копий новых фильмов

Отказ от премьеры фильма «Интервью» *(из-за угроз со стороны хакеров)*

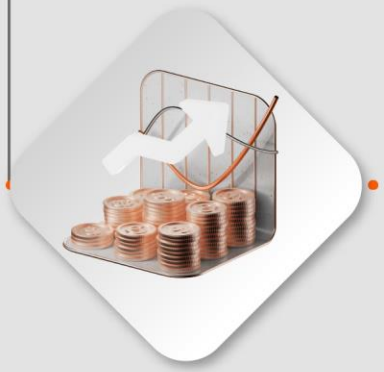
Уровни зрелости оценки ущерба от инцидентов ИБ

Компания **затрудняется оценить ущерб** от инцидента *(в том числе потенциального)*

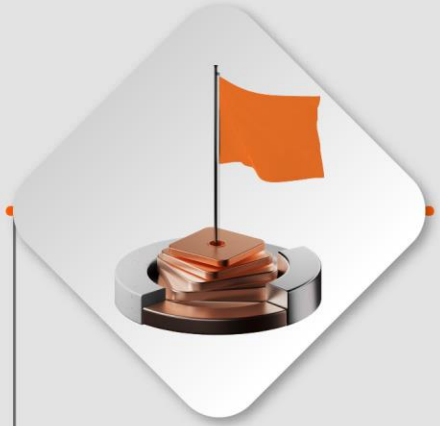


Компания использует **количественную интерпретацию** качественной оценки *(«метод светофора»)*

Компания **может оценить ущерб** количественными методами *(рублем)*



Компания **учитывает риск** – аппетит в повседневной операционной деятельности



Компания **моделирует сценарии** и определяет недопустимые события

AKTIV.CONSULTING

Фреймворки и методологии риск-менеджмента

Фреймворк «**NIST Risk Management Framework**»

Стандарт **ISO/IEC 27005** *(Менеджмент риска ИБ)*

Серия стандартов **ISO/IEC 31000**

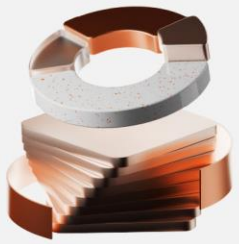
ГОСТ Р ИСО/МЭК 31010 *(Менеджмент риска. Методы оценки риска)*

ГОСТ Р 57580.3 *(управление риском инф. угроз и опер. надежности)*

Методологии *(Монте-Карло, FAIR, FRAP, BIA, FMEA, CRAMM...)*

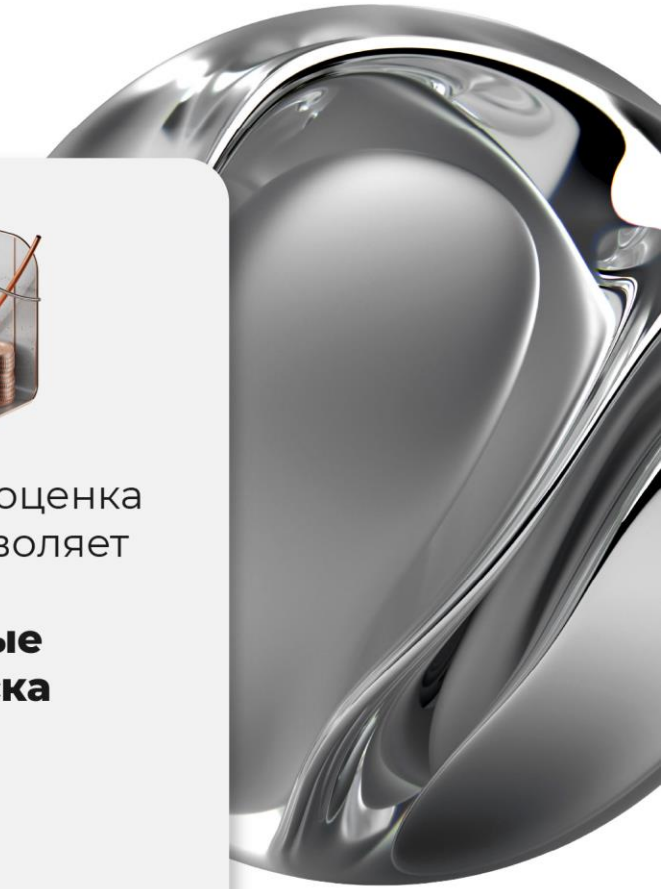
Типовые сложности оценки рисков (качественная оценка рисков)

Качественная оценка рисков **более субъективна,** так как основана на мнении экспертов и не всегда может быть объективной.



Качественный подход не позволяет получить **точные количественные оценки вероятности** и последствий риска.

Качественная оценка рисков не позволяет предвидеть **потенциальные потери от риска** в денежном выражении с приемлемой точностью.



Как обычно измеряют риски / угрозы ИБ?

Вероятность реализации / потенциальный ущерб	**Почти нереально**	**Маловероятно**	**Возможно**	**Вероятно**	**Очень вероятно**
Катастрофически	**6**	**7**	**8**	**9**	**10**
Значительно	**5**	**6**	**7**	**8**	**9**
Умеренно	**4**	**5**	**6**	**7**	**8**
Незначительно	**3**	**4**	**5**	**6**	**7**
Несущественно	**2**	**3**	**4**	**5**	**6**
	Принять (уровень = 2,3)	Мониторить (уровень = 4,5)	Управлять (уровень = 6)	Избегать / устранять (уровень = 7)	Немедленно избегать / устранять (оценка = 8,9,10)

Недостатки «светофора»

Зависимость
от доверия
к эксперту

Невозможность
провести оценку
для редких событий

Зависимость
от **квалификации эксперта /**
экспертов, отсутствие
их достаточного количества

Влияние на мнение
экспертов
заинтересованными
лицами

Психология
восприятия
рисков

Типовые сложности оценки рисков (количественная оценка рисков)

Для проведения количественной оценки рисков необходимо иметь **достаточный объем данных и знания** в области статистики и математического моделирования

Для проведения количественной оценки рисков необходимо собрать и обработать **большой объем данных**

Количественная оценка рисков не всегда может **учесть все факторы,** которые могут повлиять на вероятность и последствия риска

Экономический ущерб от инцидента

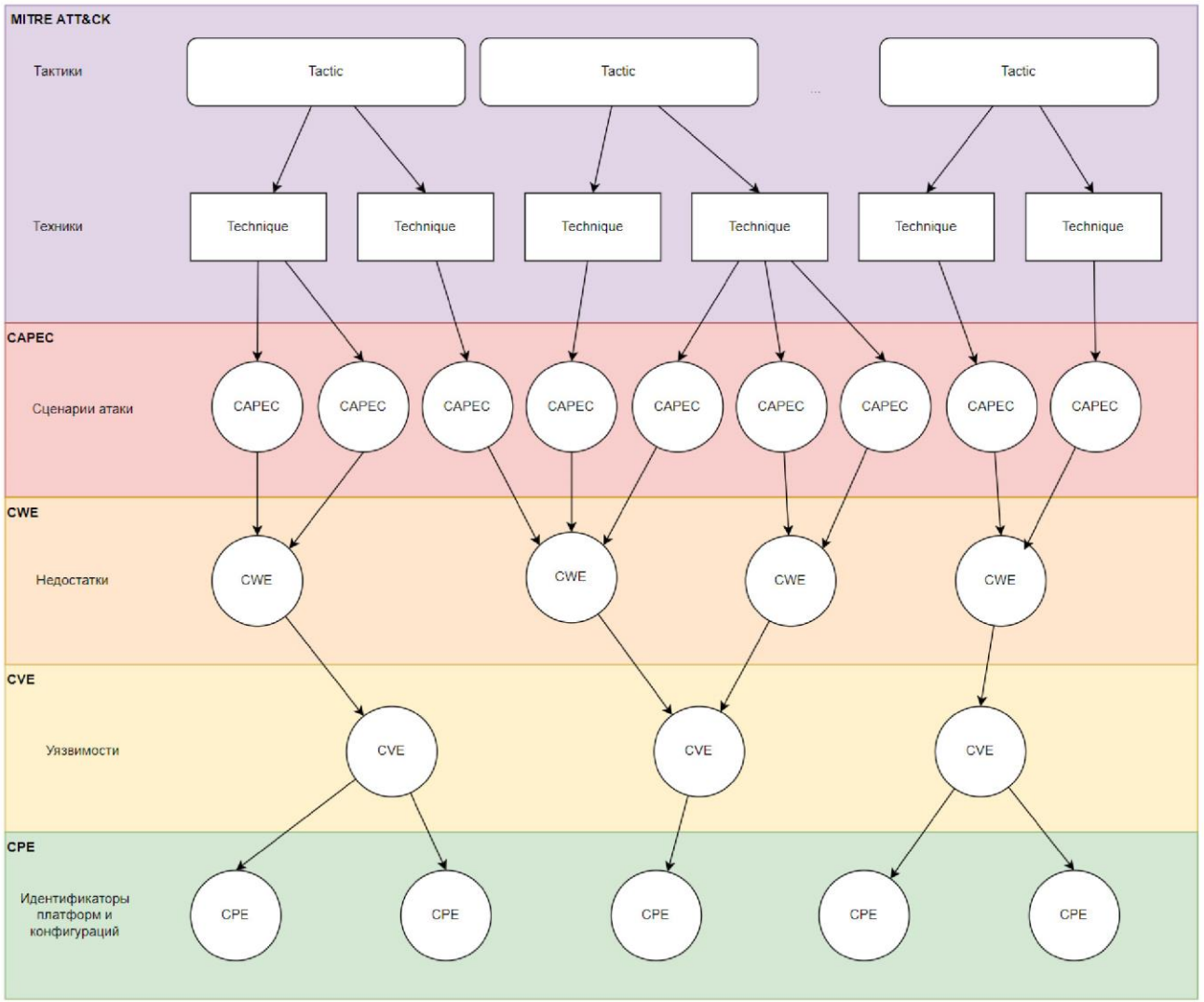
У = Упр. + k * Ук.

У – экономический ущерб от инцидента
Упр. – прямой экономический ущерб

k – коэффициент приведения разновременных затрат, зависящий от длительности последствий

Ук. – косвенный экономический ущерб *(вынужденные затраты, потери, убытки, обусловленные вторичными эффектами)*

Сценарный анализ: общий подход



Приложение №14 СТО БР 1.5-2023 *(реагирование на инциденты ЗИ и ОН (общепризнанные мировые подходы)*

Примеры методов оценки потерь

1. Оценка потенциальных прямых потерь
(отражаемые на счетах расходов и убытков в бух. учете)

A. Группа методов экспертной оценки различные методы экспертной оценки на основе сценарного анализа

2. Оценка потенциальных косвенные потерь
(не отраженные в бух. учете, но косвенно связанные, в т. ч. определяемые расчетными методами в денежном выражении)

B. Группа регуляторных методов:

- «расчет ожидаемых потерь» по 652-П
- «расчет на основании доли капитала» по РС БР ИББС-2.2

Составные части расчета ущерба

- 1-3 ИТ
- 4-6 HR
- 7-8 ИТ+Бизнес

1. Время простоя вследствие атаки
2. Время восстановления после атаки
3. Время повторного ввода потерянной информации
4. Зарплата обслуживающего персонала
5. Зарплата сотрудников атакованного узла или сегмента
6. Численность обслуживающего персонала / сотрудников атакованного узла / сегмента
7. Стоимость замены оборудования или запасных частей
8. Объем продаж, выполненных с помощью атакованного узла или сегмента

Ущерб может быть нормой для компании

Риск – аппетит – уровень риска, который организация готова принять для достижения бизнес-целей

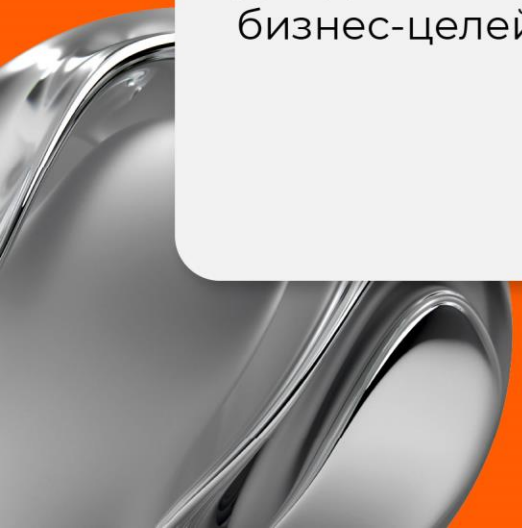
Толерантность к рискам – количественное значение, которое указывает на максимально допустимую величину конкретного риска

Эти понятия не следует путать.

Толерантность к рискам – уровень риска, который компания может вынести без серьезного ущерба.

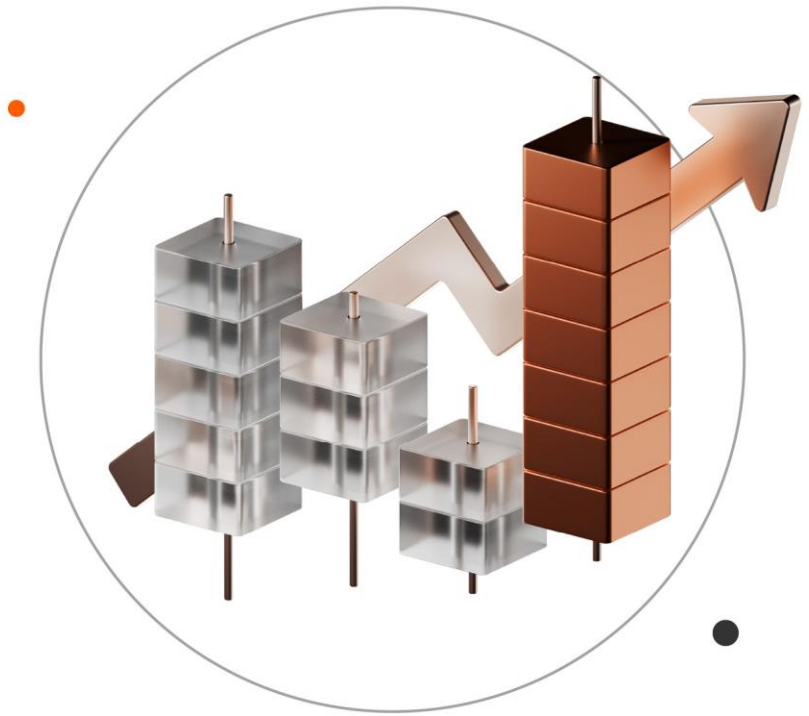
Риск – аппетит определяет какие риски компания готова принимать, чтобы достичь своих бизнес –целей.

Единой формулы расчета нет: многое зависит от конкретной организации и ее стратегии управления рисками.



Ранжирование ущерба

- Не любой финансовый ущерб значим для организации или ее подразделений или бизнес-проектов
- Важно ранжировать весь ущерб, разбив его на диапазоны от незначительного до катастрофического (риск-аппетит)
- Определяется менеджментом организации
- Чем подробнее ранжирован потенциальный ущерб, тем доступнее оценка инвестиций в ИБ и возможность ее обоснования для руководства.



	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Финансовый ущерб на более чем Y млн. руб.	**0,1 млн.**	**0,5 млн.**	**1 млн.**	**5 млн.**	**10 млн.**

Как считать будущие потери?

Автоматизация управления рисками – переход от ручного сбора данных к их автоматическому анализу, что сокращает время на обработку информации и уменьшает вероятность человеческой ошибки.

Оценка ущерба обычно базируется на прошлых периодах.

Метод Монте-Карло позволяет смоделировать тысячи «экспериментов» и получить распределение вероятных ущербов.

Смысл метода Монте-Карло в том, чтобы использовать данные случайных событий, чтобы на их основе получить более-менее точные результаты каких-то других вычислений.

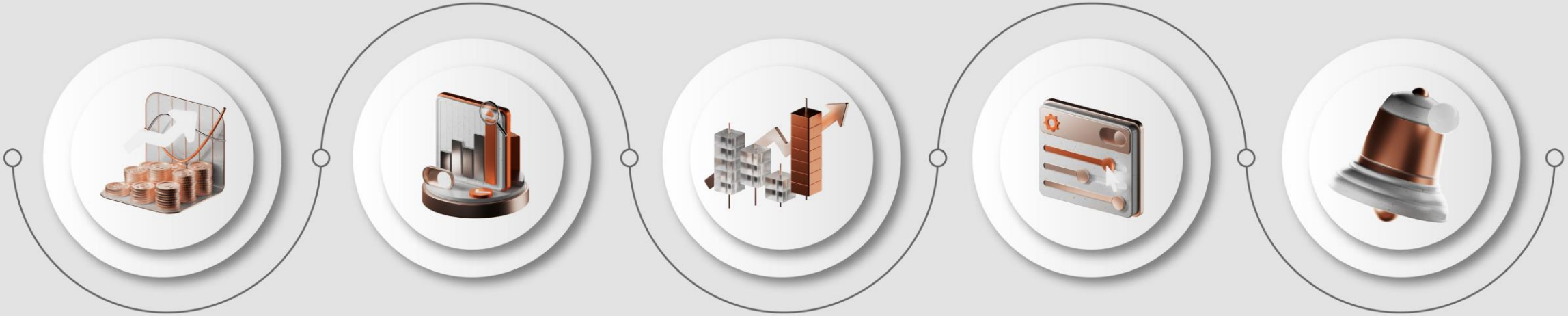
Они не будут идеально и математически точными, но их уже будет достаточно, чтобы с ними полноценно работать. Иногда это проще и быстрее, чем считать всё по точным формулам *(пример такого вычисления — построение маршрута в навигаторе).*

Как считать будущие потери?

Декомпозиция риска по FAIR (Factor analysis of information risk) – метод выделения переменных (факторов), оказывающих влияние на тот или иной показатель.

Предназначен для проведения **количественного анализа рисков,** предлагающий модель построения системы управления рисками на основе экономически эффективного подхода, принятия информированных решений, сравнения мер управления рисками, финансовых показателей и точных риск-моделей.

Итоги



1

Ущерб
от инцидентов
может и должен считаться

2

Его реальный
размер обычно
выше первичных оценок

3

Декомпозиция
помогает
разбить расчет на части

4

Многие исходные
данные
находятся у бизнеса

5

До инцидентов
лучше
не доводить

Анонс вебинара

19 июня 2025 года

Оптимальный бюджет по ИБ. Как?

Ольга Копейкина

Ведущий консультант
по информационной безопасности
AKTIV.CONSULTING

AKTIV.CONSULTING

AKTIV.
CONSULTING

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Сергей Шлёнский

Ведущий специалист
по информационной
безопасности

shlenskiy@aktiv.consulting