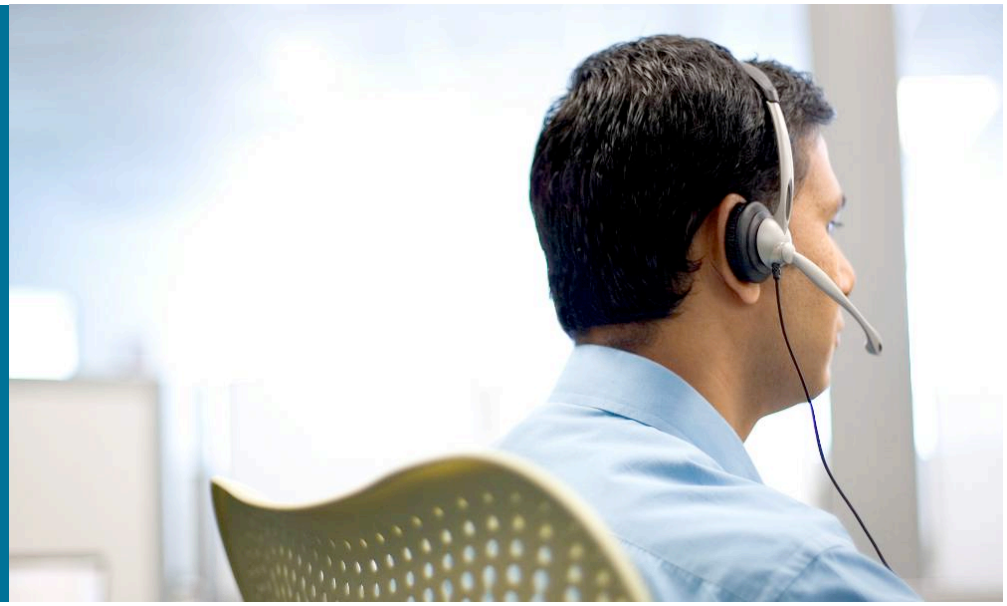
Как посчитать эффективность ИБ?

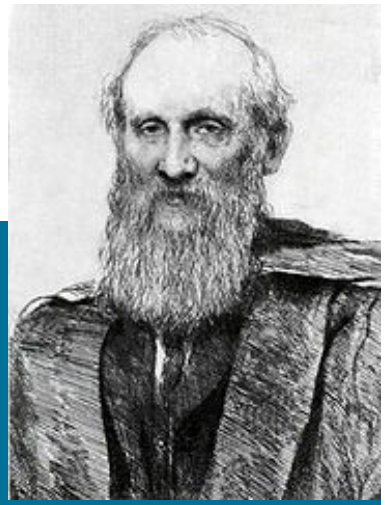


Алексей Лукацкий

Бизнес-консультант по безопасности

“Если вы можете измерить то, о чем говорите, и выразить это в цифрах, вы что-то знаете об этом предмете. Но если вы не можете выразить это количественно, ваши знания крайне ограничены и неудовлетворительны.”

Лорд Кельвин (Уильям Томсон), британский физик



Что говорит и думает руководство?

- Он спрашивает: «Каков уровень риска?»

  Он думает: «Чем нам это грозит?»

- Он спрашивает: «Соответствуем ли мы требованиям?»

  Он думает: «Не накажут ли нас?»

- Он спрашивает: «Почему так дорого?»

  Он думает: «А может лучше кофе или туалетной бумаги купить?»

- Знания CISO/CIO не совпадают с восприятием CxO

  Любой вопрос подразумевает измерение ИБ!

Что мы измеряем в ИБ?

1. Уровень опасности или сколько мы потеряем?
2. Сколько денег на ИБ достаточно?
3. Мы достигли цели?
4. Насколько оптимально мы движемся к цели?
5. Сколько стоит информация?
6. Насколько мы соответствуем стандартам или требованиям?
7. Какая из мер защиты выгоднее/лучше?
8. Как мы соотносимся с другими?
9. …

Зачем нужно измерять безопасность

1. Демонстрация результатов своей работы
2. Выполнение требований стандартов
3. Обоснование инвестиций
4. Согласование SLA
5. Быть бизнес-партнером

Но ИБ мало кто измеряет!

Проблема измерений ИБ

Почему мы отказываемся измерять?

- Это нематериально, а значит неизмеримо
- «Чтобы оценить этот показатель, нужно потратить миллионы рублей. А менее масштабный проект дает большую погрешность»
- Отсутствуют методы измерения
- «С помощью статистики можно доказать все, что угодно»
- Важные для предприятия проекты пропускаются в пользу слабых только потому, что во втором случае методы оценки ожидаемого эффекта всем известны, а в первом нет

Проблемы измерений

- Принятие решений часто требует количественной оценки предполагаемых нематериальных активов или вопросов
- Многие считают такую оценку невозможной, а нематериальное неподдающимся измерению
  - Именно это часто является причиной отказа от многих проектов (предубеждение пессимизма)
- Раз это невозможно, то мало кто пытается это сделать
- Но
  - Если какой-либо объект/явление можно наблюдать тем или иным образом → существует метод его измерения

Развенчание мифа

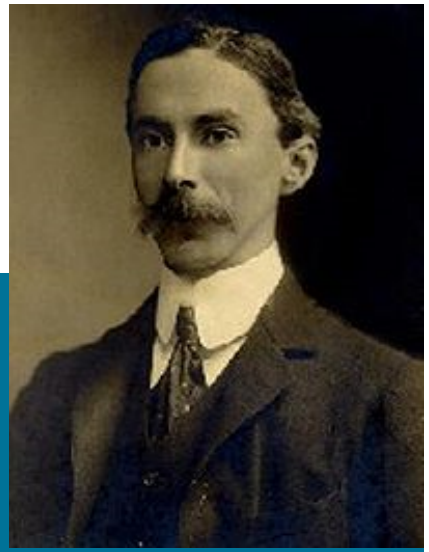
- Если что-то лучше
- ⇒ Есть признаки улучшения
- ⇒ Улучшение можно наблюдать
- ⇒ Наблюдаемое улучшение можно посчитать
- ⇒ То, что можно посчитать, можно измерить
- ⇒ То, что можно измерить, можно оценить
- …и продемонстрировать!

Что такое измерение?

- Измерение – это определенность, точная величина?
  - Количественное выражение чего-либо
  - Расчет точной стоимости чего-либо
  - Сведение к одному числу
- Измерение – это совокупность снижающих неопределенность наблюдений, результат которых выражается некоей величиной!
  - → Измерение – это не только полное, но и частичное сокращение неопределенности

“Как это не парадоксально, но всякая точная наука основывается на приблизительности. Если кто-то говорит вам, что точно знает что-то, можете смело делать вывод: вы разговариваете с человеком, не имеющим понятия о точности.”

Бертран Рассел, британский математик и философ



О неопределенности

- Информация (по Шеннону) – это снижение неопределенности
- Многие решения принимаются в условиях неопределенности
- Снижение неопределенности (даже незначительное) способствует принятию более удачных решений
- Снижение дает вполне определенный эффект

  Эффект может многократно превышать затраты на измерение эффекта (оценку эффективности)

Количественное измерение?

- Измерение – это не всегда количественная оценка в традиционном понимании этого слова

  Произойдет ли сбой?

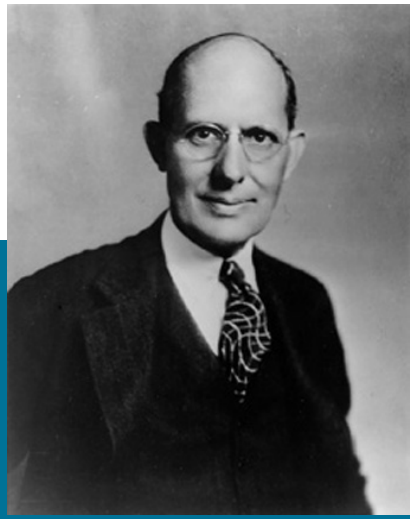
  Получим ли мы сертификат соответствия?

  Число сигнатур атак в IDS#1 больше чем в IDS#2 (не важно насколько)

  Продукт #1 имеет 4 балла в тестах, а продукт #2 – 2 балла (2 балла не обязательно вдвое меньше, чем 4 балла; а 2 системы, имеющие по 2 балла, не обязательно будут также эффективны, как одна система с 4-мя баллами)

Вернемся к безопасности

“Правильно поставленная проблема уже наполовину решена.”



Чарльз Кеттеринг, американский изобретатель

Определите объект измерения!!!

- Самое важное – определить объект измерения!
- Что для вас информационная безопасность?
  - Снижение числа вредоносных программ?
  - Получение аттестата PCI Council?
  - Снижение числа запросов в Help Desk по поводу забытых паролей?
  - Снижение числа утечек конфиденциальной информации?
  - Защита от наездов регуляторов?
- Что конкретно вы имеете ввиду?!
- Определитесь с объектом измерения и половина работы по измерению будет проведена!

Что такое эффективность?

- Мало кто может сказать, что такое эффективность – большинство может сослаться на разрозненные наблюдения, которые ассоциируются у них с эффективностью
  - Число эпидемий стало меньше
  - Заказчики стали меньше звонить в Help Desk по поводу недоступности сайта
  - Пользователи стали реже заносить вредоносные программы на флешках
  - Руководство не жалуется, что не может «достучаться» до корпоративной ИС из командировки
  - Сервер AD ни разу не «упал» в этом месяце

Что такое эффективность?

- Эффективность – это поддающийся количественному определению вклад в достижение конечных целей
- Важно в конкретном случае детализировать понятие «эффективность» (объект измерения)
- Прежде чем оценивать эффективность, необходимо понять, определить и зафиксировать цели, эффективность достижения которых мы измеряем!!!

Монетарные и нефинансовые метрики информационной безопасности

Функции и процессы любой компании

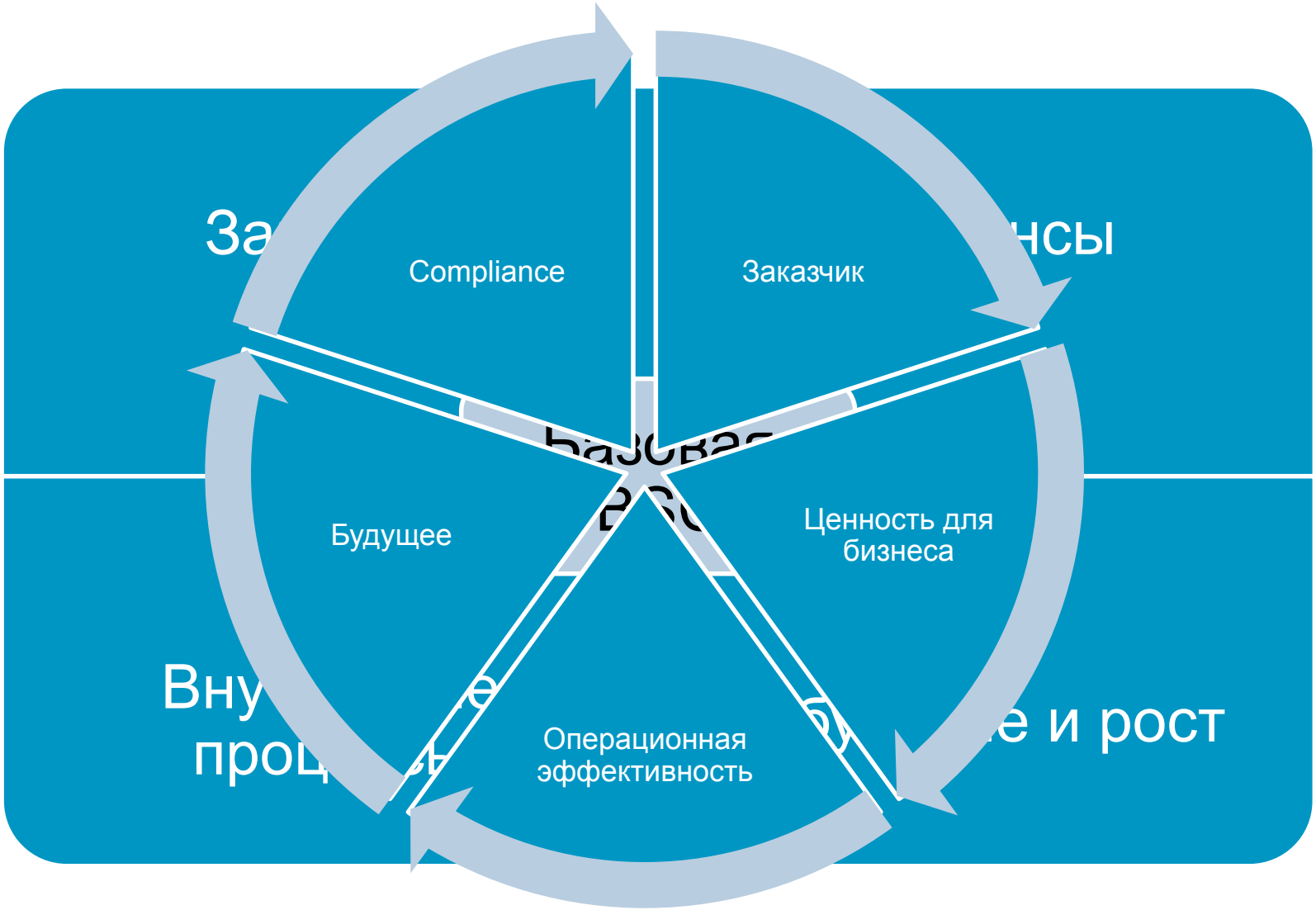
Могут ли быть нефинансовые метрики?

- ИБ не относится к первой категории функций предприятия
  - Финансовые метрики сложно применять в этом случае, т.к. ИБ напрямую не генерит бизнес
- ИБ чаще всего относится ко второй категории функций
  - Возможность использования финансовых метрик зависят от оцениваемого процесса
  - Некоторые проекты ИБ могут помочь оптимизировать издержки
- Управление ИБ – это всегда третья категория функций
  - Финансовых метрик может вообще не быть
  - Исключение может составлять экономия на персонале за счет более эффективного управления

Могут ли быть нефинансовые метрики?

- Классические финансовые метрики определяют балансовую стоимость предприятия, его доходы и расходы
- Рыночная стоимость, капитализация определяются в т.ч. и нефинансовыми показателями
  - Уровень корпоративного управления
  - Наличие бренда
  - Прозрачность
  - Эффективность управления
  - И т.д.
- Не зря появляется такое понятие, как система сбалансированных показателей (Balanced scorecard, BSC)

Security balanced scorecard



Всегда ли выгода измеряется деньгами

- Бизнес инвестирует в проекты, приносящие отдачу
  - Отдача не обязательно носит денежный характер

Критерии
• Бизнес-ориентированный • Связанный с приоритетами/целями компании • Измеримый в метриках, понятных бизнесу • Приносящий ценность или отдачу (желательно финансовую) • Оптимальный (цель не любыми средствами) • Выполненный в срок • Не нарушающий законодательство

Примеры
• Снижение TCO • Защита взаимоотношений • Рост доверия • Соответствие требованиям • Ускорение выхода на рынок • Географическая экспансия • Снижение бизнес-рисков • Снижение текучки клиентов/партнеров • Рост лояльности клиентов/сотрудников • Оптимизация процессов • Интероперабельность и интеграция • Стандартизация • Рост качества • Оптимизация затрат (на внедрение, эксплуатацию, поддержку и т.п.) • Повторное использование • Масштабируемость

Метрики информационной безопасности

Что такое «метрика безопасности»?

- Метрика безопасности – способ применения количественного, статистического и/или математического анализа для измерения «безопасных» стоимости, преимуществ, удач, неудач, тенденций и нагрузок
  - Отслеживание статуса каждой функции безопасности
- Метрики – это не столько цифры, сколько факт достижения поставленных целей, выраженный количественно
- KPI, KRI, PI = метрика

KPI, KRI, PI и CSF

- KPI – Key Performance Indicator
- KRI – Key Result Indicator

  Не путать с Key Risk Indicator
- PI – Performance Indicator
- CSF – Critical Success Factors

Классификация метрик информационной безопасности

О метриках

- Существуют различные классификации метрик ИБ
- Например, метрики

  оценивающие эффективность реализации политики безопасности

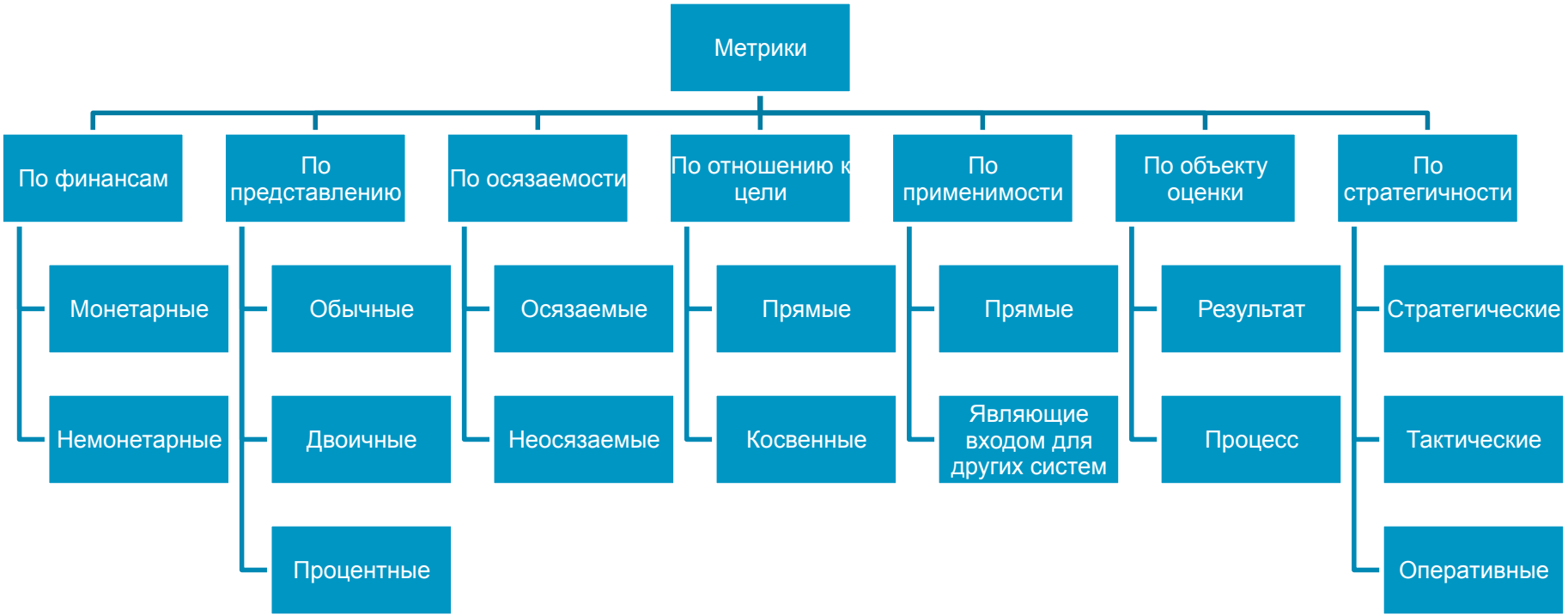
  оценивающие эффективность процесса обеспечения безопасности (насколько оправданы затраты)

  оценивающие влияние безопасности на бизнес
- Например, каждая система может создавать 2 типа метрик

  Показывающие достижение целей в системе

  Являющиеся входным параметром для систем более высокого уровня
- Использование метрик зависит от уровня зрелости процессов ИБ

Таксономия метрик ИБ



Иерархия метрик
в масштабе службы ИБ

Иерархия метрик
в масштабе предприятия

Метрики безопасности

- Метрики эффективности реализации

  Пример (один источник данных): число неудачных попыток аутентификации

  Пример (несколько источников данных): число инцидентов безопасности по причине некорректной настройки подсистемы контроля доступа

- Метрики эффективности процесса ИБ

  Пример: число специалистов, требуемых для реагирования на инциденты

- Метрики оценки влияния на бизнес

  Пример: стоимость обработки звонка в Help Desk по поводу смены пароля или время простоя бизнес-пользователя в результате вирусной эпидемии

Стратегические/тактические метрики

- Стратегическая метрика – показатель правильности выбранного пути
  - Отклонение от него не требует немедленной реакции
  - Стандартный срок действия метрики – 3 года
  - Требуется понимание образа мыслей топ-менеджеров
  - Никаких деталей – только высокоуровневые индикаторы
- Отраслевых стратегических метрик в ИБ нет
  - В отличие от других отраслей
  - Исключая число выданных сертификатов и лицензий

Стратегические отраслевые метрики

- Здравоохранение

  Коэффициент трудовой занятости, общее число госпитализированных и выписанных, показатель рождаемости и смертности и т.п.

- Промышленность

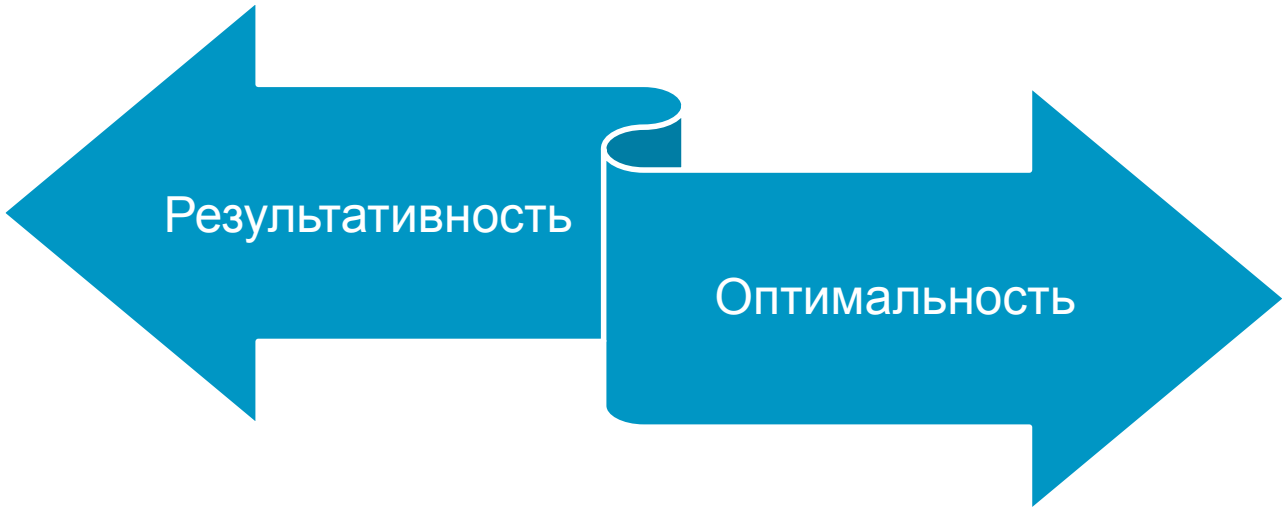
  Число аварий на производстве, число дефектов на устройство, среднее отклонение от допуска и т.д.

- Ритейл

  Объем продаж на квадратный метр, продажи на одного покупателя, число покупок на одного покупателю и т.д.

Результат любой ценой?

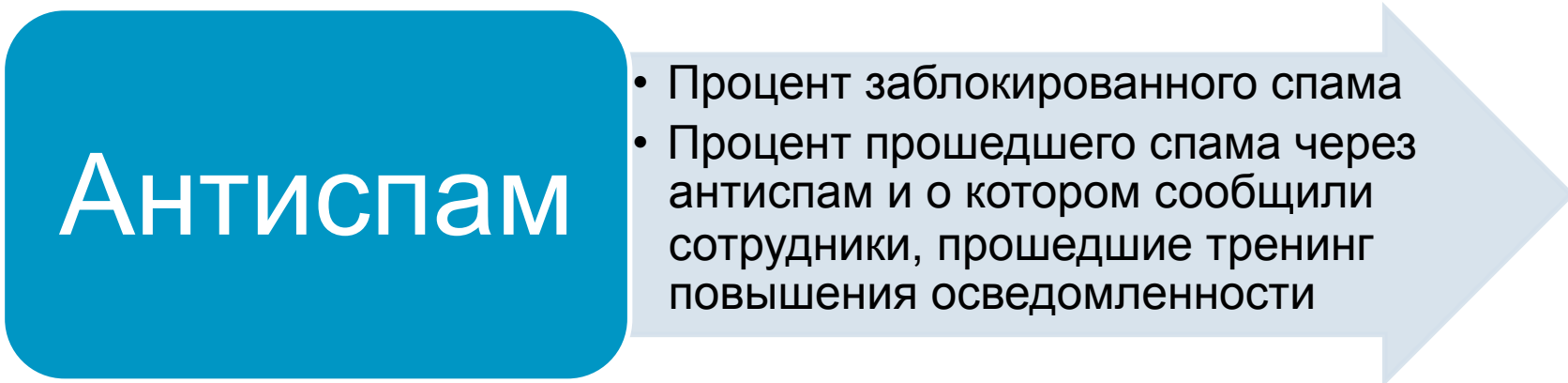
Efficiency vs. Effectiveness



- Сначала мы обычно оцениваем достижение цели как таковой (результат)
  - Но интересно ли нам достижение цели любыми средствами?

Метрики на результат и процесс

- Метрики, нацеленные на результат
  - Наиболее привычные для служб ИБ
  - Чаще всего выдаются системами защиты
- Метрики, нацеленные на процесс
  - Сложнее оцениваются
  - Требуют взаимодействия с людьми



Как выбирать метрики ИБ

Выбор метрик

- Не используйте метрики, создающие «видимость» улучшения, без самого улучшения для бизнеса
  - Например, число обнаруженных вирусов или устраненных уязвимостей
- Если измерение не дает ничего с точки зрения бизнеса, то это плохое измерение
  - Измерение ради научных целей интересны, но не нужны в деле
- Метрика должна быть релевантной, измеримой в адекватных терминах и, желательно, ассоциированной со стоимостью
  - Время/стоимость простоя пользователя в месяц
  - Не идеальна, но соответствует требованиям
  - Можно также учесть время, в который происходит простой, роль пользователя, который простаивает и т.д.

Выбор метрик (продолжение)

- Точность метрики менее важна, чем ее качественная связь с бизнесом и его целями
- Метрики должны быть применимы ко всему предприятию
  - Если мы хотим донести до топ-менеджмента всю важность ИБ
  - Локальные метрики допустимы на уровне отдела или для собственных задач
- Измерения должны быть повторимыми
- Не бывает универсальных метрик
  - У каждого предприятия свои особенности и свои метрики
- Не используйте сложных в вычислении метрик
  - Это снижает доверие к результатам и увеличивает время

Принципы выбора метрик

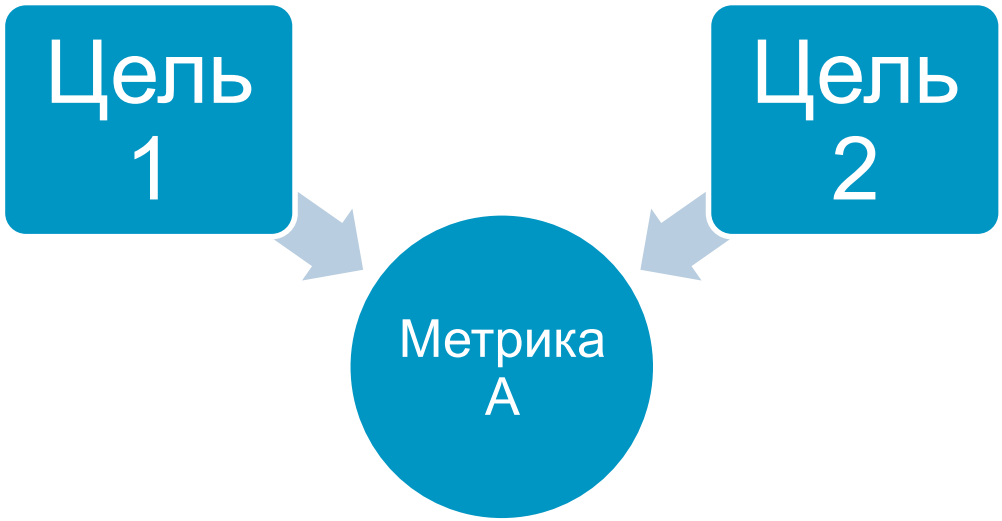
- SMART – **S**pecific, **M**easurable, **A**chievable, **R**elevant, **T**imely
  - Как можно конкретнее, без двойных толкований, для правильной целевой аудитории
  - ROSI vs. удовлетворенность клиента
  - Зачем выбирать цель, которая недостижима?
  - Соответствие стратегическим целям, а не «вообще». При внедрении проектного подхода к ИБ, правильной метрикой будет число проектов, завершенных в срок, а не просто число стартовавших проектов
  - Своевременность и актуальность метрик

Принципы выбора метрик

Характеристика	Пример хорошей метрики	Пример плохой метрики
Конкретная	Число неудачных попыток входа в систему в неделю на одного сотрудника	Число неудачных попыток входа в систему
Измеримая	Уровень лояльности внутренних клиентов	Доход от внедрения системы защиты
Достижимая	Число инцидентов в текущем квартале < 5	Отсутствие инцидентов ИБ за текущий квартал
Релевантная	Число проектов завершенных в срок	Число запущенных проектов
Актуальная	Число пропатченных ПК в этом году	Число пропатченных ПК в прошлом году

Выбор метрик (окончание)

- Нельзя допускать появления кросс-метрик, одинаково подходящих для оценки двух разных целей
  - Особенно противоположных целей



Как выбирают метрики?

1. Метрики обычно выбираются исходя из корпоративных целей (в 65% случаев)
2. Анализ существующих отчетов, из которых вычленяются чаще всего используемые для оценки деятельности показатели
3. Индивидуальные интервью
4. Карты бизнес-процессов
5. Специальные сессии определения KPI
6. Групповые интервью
7. Стратегические карты
8. Опросы (в 23% случаев)

Пример: какой антивирус лучше

- Исходные данные
  - Symantec Antivirus обнаруживает 100K+ штаммов вирусов
  - Антивирус AntiDIR обнаруживает только один вирус DIR
- Задача – определить какой антивирус лучше?

Пример: значимость метрик

- Измерение числа спам-сообщений в общем объеме почты
  - Как это важно для предприятия и для бизнеса?
  - Что изменится, если спама будет 70%, а не 50%
- Обнаружение шпионского ПО
  - Обнаружение 50% всех spyware, встречающихся в диком виде
  - Обнаружение 95% spyware, которые могут встретиться в компании (даже если это будет 10% от всех spyware)
- Число вирусов, а следовательно и атак, бесконечно. Поэтому бессмысленно опираться на конечное число обнаруженных вирусов и уязвимостей
  - Что такое тысяча или даже миллион по сравнению с бесконечностью

Пример: дорога на Луну

- Задача: Я хочу добраться до луны
- Решение: насыпать холм до луны
  - Каждый день холм растет на 10 м
  - Каждый день я становлюсь на 10 м ближе к цели
  - Для достижения цели потребуется 38440000 дней
- Можно наблюдать процесс достижения цели!!!
- Но… цель недостижима, т.к. Земля движется вокруг своей оси, солнца, галактики… и расстояние/ направление от холма до Луны постоянно изменяется

Выбор метрик

- Будьте осторожны в выборе метрик
  - Сотрудники будут оптимизировать свою деятельность, чтобы метрики говорили в их пользу
  - Это допустимо, если от этого выиграет бизнес

Пример: число звонков в Service Desk

- Задача: оценить время реагирования на звонок об инциденте
- Поощрение за снижение времени реагирования
  - Сотрудники могут класть трубку сразу после звонка!
- Поощрение за число разрешенных инцидентов
  - Сотрудники будут самостоятельно пытаться закрыть инцидент, не эскалируя его правильному специалисту
  - Увеличение длительности звонков и ожидания клиентов на линии
  - Меньше доступных специалистов – ниже удовлетворенность
- Комбинируйте метрики
  - Время реагирования на звонок + длительность звонка

Пример: контроль доступа в Интернет

- Задача: оценить эффективность системы контроля доступа

Видимая оценка	Скрытая оценка
• 1,5 часа в день на «одноклассниках» • 200 сотрудников • 6600 часов экономии – 825 чел/дней • $18750 в месяц (при зарплате $500) • $225000 в год экономии	• Блокирование доступа не значит, что сотрудники будут работать • Работа «от» и «до» и не больше • Ухудшение псих.климата • Потери $150000 в год

Считать можно все!

Метрика	Частота измерения	Единица измерения
Удачная аутентификация	квартал	секунда
Неудачная аутентификация	квартал	секунда
Стоимость обработки звонка в Help Desk о смене пароля	квартал	долларов на звонок
Время регистрации в системе	квартал	минут в день
Добавление/удаление учетной записи	квартал	долларов за событие
Инцидент, произошедший из-за некорректной настройки системы контроля доступа	квартал	инцидент

Считать можно все!

Метрика	Частота измерения	Единица измерения
Стоимость системы защиты в расчете на одного сотрудника (собственного или по контракту)	6 месяцев	долларов на сотрудника
Число узлов КИС, на которых были протестированы механизмы защиты	ежегодно	процент
Время между обнаружением уязвимости и ее устранением	квартал	час
Число прикладных систем, для которых реализовано требование разделения полномочий между операциями А и Б	6 месяцев	процент
Число лэптопов с внедренной подсистемой шифрования важных и конфиденциальных документов	квартал	процент

Считать можно все!

Метрика	Частота измерения	Единица измерения
Число систем, для которых план реагирования на инциденты был протестирован	квартал	процент
Число задокументированных изменений ПО	6 месяцев	процент
Число систем с установленными последними патчами	месяц	процент
Число систем с автоматическим антивирусным обновлением	6 месяцев	процент
Число сотрудников, прошедших через тренинги по повышению осведомленности	ежегодно	процент
Число систем с разрешенными уязвимыми протоколами	6 месяцев	процент

Что обычно считают?

Какие данные собирает ваша организация?	%
Обнаруженных вирусов в файлах	92,30%
Обнаруженных вирусов в почте	92,30%
Неудачный пароль при входе в систему	84,60%
Попытка проникновения/атаки	84,60%
Обнаруженный/отраженный спам	76,90%
Доступ к вредоносным сайтам	69,20%
Неудачное имя при входе в систему	69,20%
Обнаруженных вирусов на сайтах	61,50%

Что обычно считают?

Какие данные собирает ваша организация?	%
Внутренняя попытка НСД	61,50%
Нарушение со стороны администратора	61,50%
Удачное проникновение	53,80%
Раскрытие информации	38,50%
Пропущенный спам	38,50%
Ложное обнаружение спама	30,80%
Другое	23,10%

Источник: http://www.csoonline.com/analyst/report2412.html

Сколько метрик ИБ достаточно?

Количество метрик

- Надо понимать разницу между KPI и PI

  Обычно для измеряемого процесса / приложения / подразделения не должно быть больше 7-ми ключевых метрик

  Низкоуровневых метрик может быть больше, но их число не должно быть самоцелью

  На уровень топ-менеджмента также не должно выноситься более 7-ми метрик

- Verizon использует всего одну метрику для топ-менеджмента - индекс риска актива

  Опирается на данные анализа защищенности, транслированные в бизнес-язык

Пример бизнес-ориентированных метрик ИБ

Транзакция

- Транзакция – это ключевое понятие на современном предприятии
- Обычно оно выпадает из поля деятельность служб ИБ, т.к. транзакция является обычным и легитимным событием
- Это не только финансовое понятие

  Сетевые потоки (flow)

  Сессии

  Сообщения

  Операции приложений (немного выпадает из традиционного восприятия транзакций, но относится к ним же. Правда, и измеряется сложнее)

Бизнес-метрики ИБ

Метрика	Формула	Комментарий
Transaction Cost	Совокупная цена средств ИБ / число транзакций	Снижение данного показателя может войти в конфликт с минимально необходимым уровнем защиты
Controls per transaction (CPT)	Число технических защитных мер / число транзакций	Интересна в совокупности с другими метриками. Например, при одинаковом количестве инцидентов для разных приложений больший CPT говорит о переборе защитных мер. Транзакции можно поменять на подразделения или филиалы

Бизнес-метрики ИБ (продолжение)

Метрика	Формула	Комментарий
Security to IT Cost Ratio (STC)	Цена ИБ / цена ИТ	Показывает соотношение затрат на ИБ от ИТ бюджета. При оценке в совокупности с метриками по инцидентам позволит оценить оптимальный уровень затрат на ИБ от ИТ-бюджета. Если STC снижается, а инциденты растут, то защита неэффективна. Cost можно заменить на Value - STV (если можно оценить не просто стоимость, сколько ценность)
Transaction Value	Total Security Value / Total Transaction	

Бизнес-метрики ИБ (продолжение)

Метрика	Формула	Комментарий
Cost per Control (CPC)	Цена технических мер защиты / число контролируемых средством защиты элементов (число соединений для МСЭ, число сканируемых узлов для сканера…)	Снижение CPC может привести к росту CPT
Loss to Value Ratio (LTV)	Совокупные потери / ценность ИБ	Чем меньше, тем лучше. Однако при падении LTV и росте STV/STC это уже не очень хорошо

Бизнес-метрики ИБ (продолжение)

Метрика	Формула	Комментарий
Control Effectiveness Ratio (CER)	(100% хорошие / пропущенные/ события + 100% плохие / блокированные/ события) / общее число событий	Выше CER – эффективнее система защиты. Однако надо понимать, что данная метрика должна рассматриваться в контексте предприятия, а не оторвано от него. Просто измерять CER можно для сравнения различных продуктов, но сама по себе данная метрика не говорит, снижает ли риски данная защитная мера. Иными словами, данная метрика оценивает, насколько защитная мера делает то, что должна делать, а не то, как она это делает в конкретной ситуации. Если CER высок, а число инцидентов не уменьшается или растет, то выбрана неадекватная защитная мера (которая сама по себе может быть очень эффективной)

Бизнес-метрики ИБ (продолжение)

Метрика	Формула	Комментарий
Incident per Million (IPM)	Число инцидентов / число транзакций * миллион – частота инцидентов	Важно определить, что такое инцидент. Вместо миллиона можно взять более реальный для бизнеса порядок транзакций. Инцидент может произойти по причине неэффективной защитной меры, пропустившей инцидент, или по причине отсутствия защитной меры. Чем ниже, тем лучше. Необходимо учитывать, что в ряде случаев этот показатель может быть достаточно высоким, т.к. в ряде случаев экономически невыгодно защищать транзакции

Бизнес-метрики ИБ (окончание)

Метрика	Формула	Комментарий
Incident Prevention Rate (IPR)	1 – (число инцидентов / (100% предотвращенные инциденты + число инцидентов))	CER – важная метрика, но гораздо важнее число пропущенных инцидентов. Чем выше, тем лучше
Risk Aversion Ratio (RAR)	Хорошие отброшенные / число инцидентов	Показывает насколько организация готова бороться с реальными инцидентами. RAR – уровень терпимости организации к риску. Он ни плох, ни хорош

Пример: оценка системы защиты e-mail
Технические метрики

- % обнаруженного спама от общего числа писем
- % писем с вредоносными программами или фишингом от общего числа писем
- % необнаруженного спама/вредоносных программ/фишинга
- % ложного обнаружения спама/вредоносных программ/фишинга
- Число предотвращенных утечек информации
- Число/стоимость/длительность звонков в службу поддержки по поводу недошедших писем

Пример: оценка системы защиты e-mail
Псевдотехнические метрики

- Цена/длительность лечения зараженной почты
- Число вирусов/спама/утечек в исходящей почте
- % пользователей, прошедших тренинг по использованию и защите электронной почты
- % пользователей, сообщивших о пропущенном спаме/вредоносной программе/фишинге
- Рейтинг успешности повышения осведомленности в области использования и защиты электронной почты
- % внутренних нарушителей, отправивших спам/вредоносную программу/конфиденциальную информацию

Пример: оценка системы защиты e-mail
Псевдобизнес метрики

- Наличие политики использования и защиты электронной почты
- Число зашифрованных сообщений
- Потери от вирусов/спама/утечек/фишинга
- Сэкономленное время сотрудников
- Затраты на Интернет-трафик для удаленных офисов/ мобильных работников

Оценка системы защиты e-mail

Исходные данные	Значение	Метрика	Значение
Ценность (value)	1.000.000	**Transaction Value**	0,0025
Цена решения	250.000	**Transaction Cost**	0,000625
Цена средств защиты	20.000		
Потери на инцидент	300	**Cost per Control**	0,000023529
Число транзакций	400.000.000		
		Control per Transaction	2.13
Проверенных IP	300.000.000		
Антиспам	400.000.000	**Security to Value Ratio**	2%
Антивирус	150.000.000	**Loss to Value Ratio**	15%
Хороших писем разрешено	80.000.000	**Control Effectiveness Ratio**	95%
Плохих писем запрещено	300.000.000	**Incident per Million**	1,25
Хороших писем запрещено	200.000	**Incident Prevention Rate**	99,9998%
Плохих писем разрешено	500	**Risk Aversion Ratio**	400

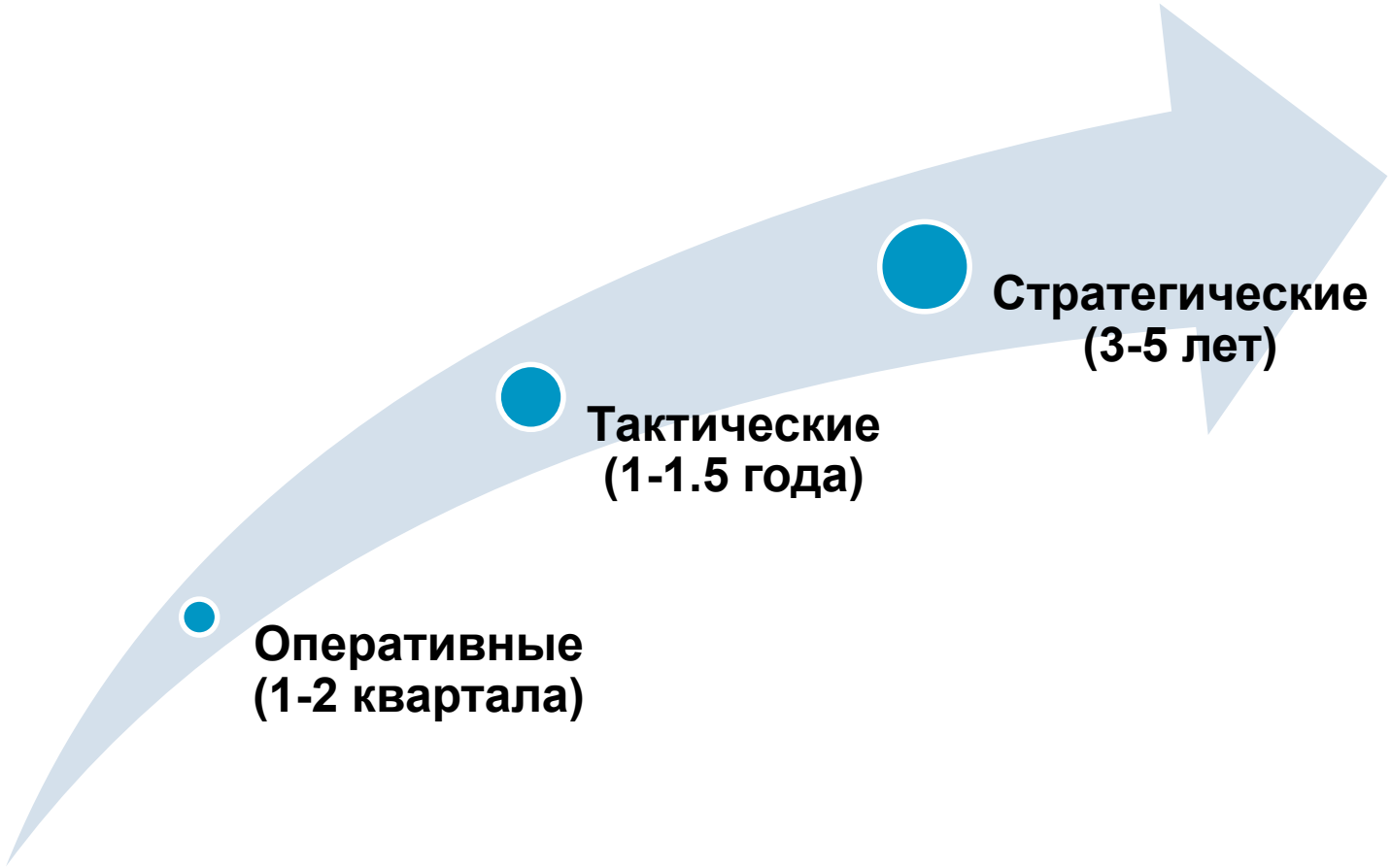
Как объединить все в одну метрику?

	Градация уровней					Пример расчета			
	1	**2**	**3**	**4**	**5**	**Значение**	**Уровень**	**Вес**	**Рейтинг**
Число уязвимостей на ПК (в среднем)	100	75	50	25	0	34	4	25	100
Число инцидентов ИБ	>5	5	3-4	1-2	0	2	4	25	100
Число непропатченных ПК	100%	75%	50%	25%	0%	65%	3	25	75
Объем спама	<80%	80%	90%	95%	>95%	24%	1	25	25
Совокупный рейтинг									**300**

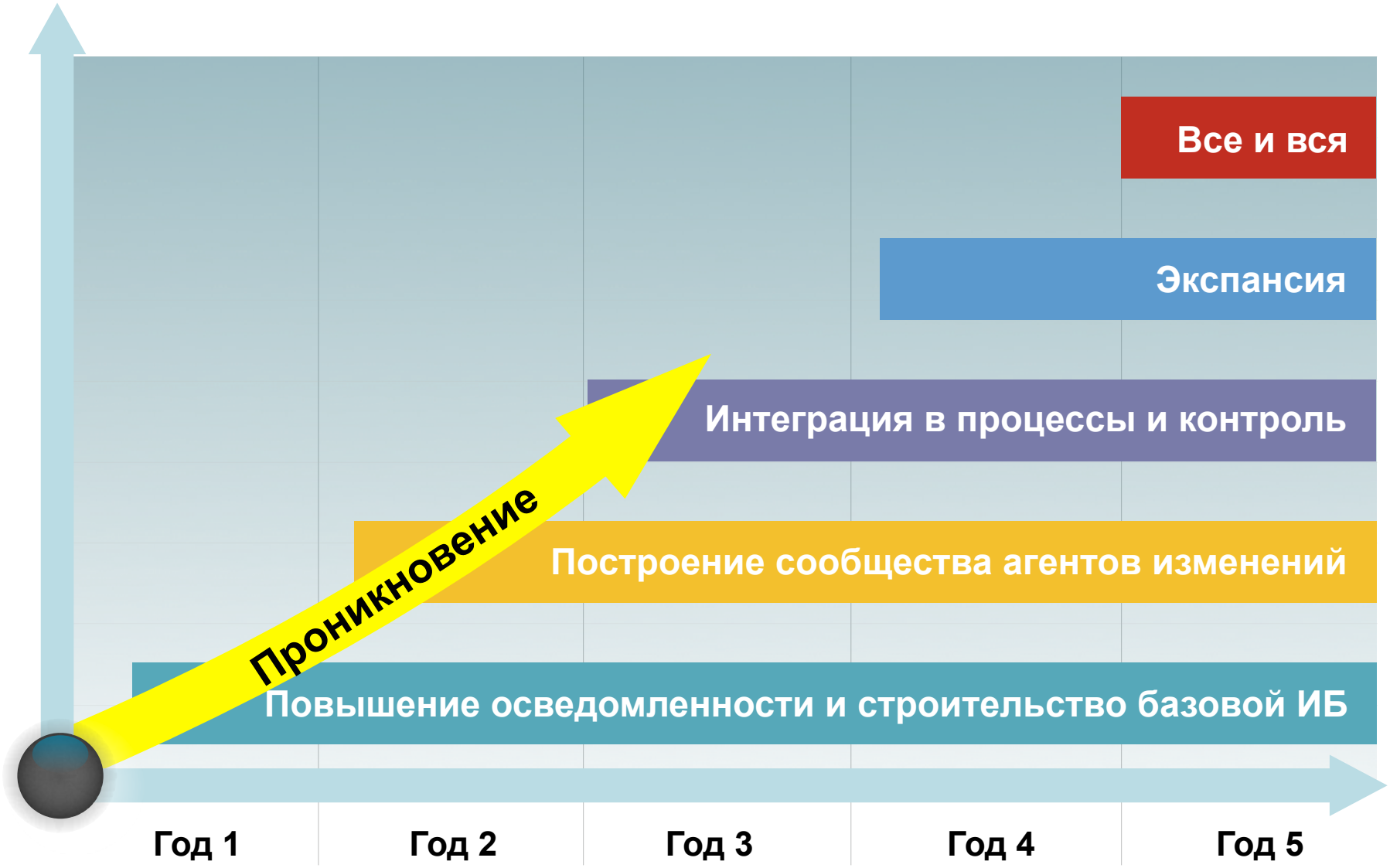
- Задача: повысить индекс до максимальных 500

Метрики информационной безопасности и фактор времени

Сколько нужно времени?



На все нужно время

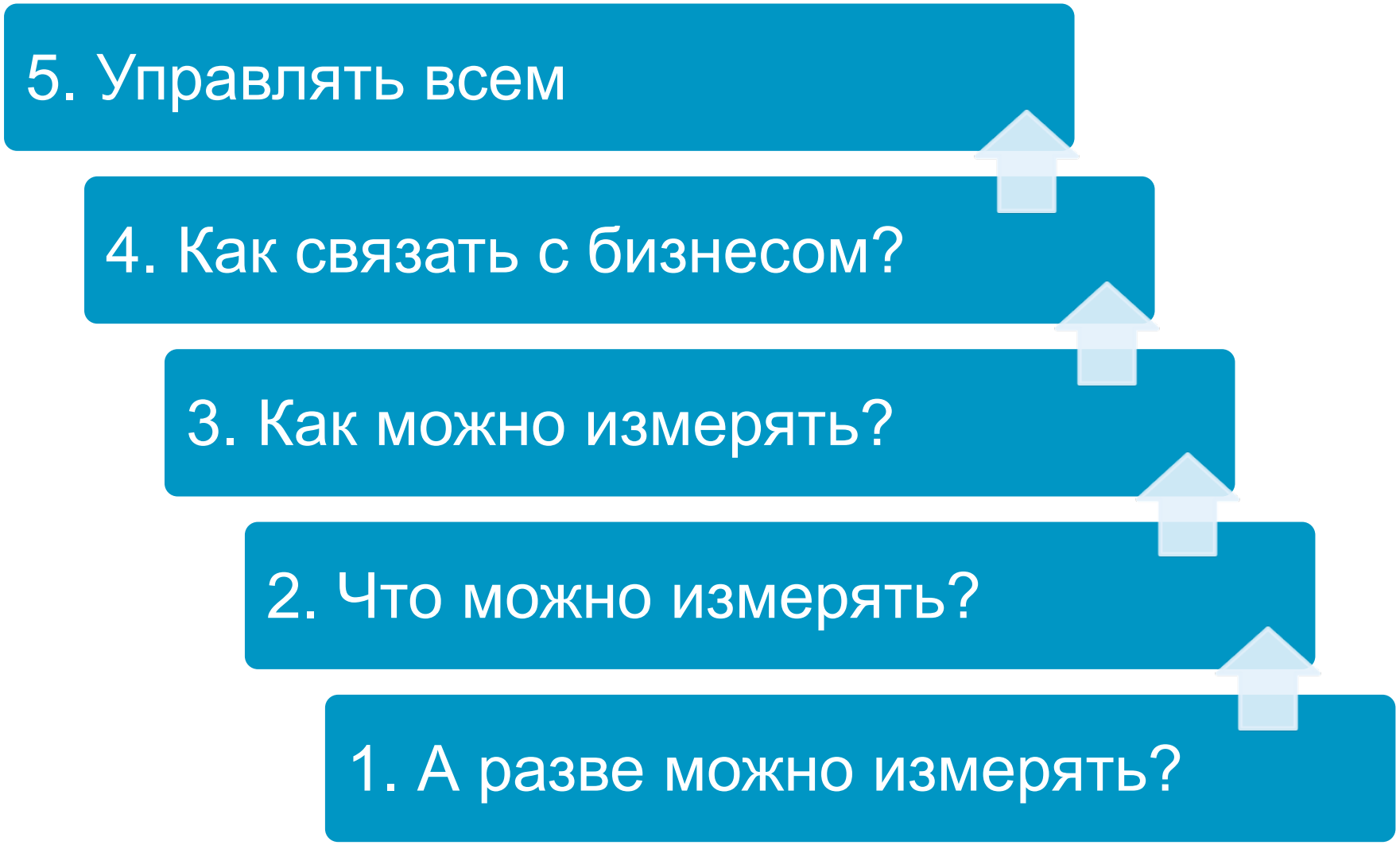


Программа управления оценкой эффективности информационной безопасности

Программа управления оценкой эффективности

- Выбор метрик и формирование базы – это только начало оценки эффективности
- Необходима целая программа управления данным процессом
  - Регулярный, непрерывный, всеохватывающий процесс
- Не пытайтесь съесть слона целиком – нужно поэтапное внедрение
  - Начните с одного бизнес-приложения (АБС), подразделения (работы с клиентами), бизнес-процесса (Интернет-банкинг), части инфраструктуры (например, Интернет-периметра)

Модель зрелости программы метрик



Методы измерений

Подходы к измерению

Тип	Используется для…	Ограничения
Сверху-вниз	Программы и оценки развития	Сложно оценивать до деталей Очень много компонентов
Оценка разрыва	Поиск пробелов	Обнаружение слабых мест не помогает в их приоритезации
На базе стандартов	Общая оценка программы для due diligence, compliance Оценка статуса программы и улучшений	Многие стандарты не имеют механизмов для измерений и метрик для оценки их использоания
По сравнению с предыдущим состоянием	Демонстрация развития	Сравнение с предыдущим состоянием не показывает достижения поставленных целей

Подходы к измерению

Тип	Используется для…	Ограничения
По сравнению с другими	Программы сравнения	Не существует универсальных или вендор-независимых сравнений
По отношению к критичности для бизнеса	Ранжирование внимания	Трудно выполнимо без глубоких знаний предприятия
Временная динамика по графу атак	Многосценарные ситуации и имитационный анализ	Дорого и тяжело для многосценарных систем Для малосценарных систем результат ограничен качеством и точностью модели
По сравнению со списком пунктов	Произвольная выборка, чтобы быть уверенным, что ничего не упущено	Отсутствуют общепринятые списки для ИБ

Подходы к измерению

Тип	Используется для…	Ограничения
Метрики программы	Общая оценка программы и изменения с течением времени	Сложно составить список критериев. Они должны применяться в контексте
Метрики ROI	Привязка финансовой метрики к ИБ	Практически неприменимо в области ИБ
Метрики производителей	Измерение производительности продуктов в выбранном сегменте	Вендоры фокусируются на метриках, показывающих свое лидерство по отношению к конкурентам, а не на компании
Метрики оценки рисков	Использование в общей стратегии управления рисками	Основаны на математических моделях, не всегда учитывающих вопросы ИБ

Подходы к измерению

Тип	Используется для…	Ограничения
Метрики на основе опросов	Сравнение выбранных граней программы ИБ	Основан на ненадежных данных, от которых сложно ожидать честности и независимости и которые сложно проверить
Мониторинг соответствия	Отчеты о соответствии	Ориентировано больше на демонстрацию соответствия, чем на качество программы ИБ
BSC	Общая оценка деятельности службы ИБ	Проекты по BSC слишком часто заканчиваются неудачей
KRI	Оценки операционных рисков	Проекты по KRI для ИТ/ИБ не получили пока широкого распространения

Качественная или количественная оценка?

Качество или количество?

- 1954 г. - Paul Meehl – «Clinical Versus Statistical Prediction: A Theoretical Analysis and Review of the Evidence», 1954
  - Работа обновлена в 1996
- Количественная оценка работает лучше экспертной (качественной)
  - В 136-ти случаев из 144-х
  - Качественная оценка необъективна по своей сути
  - При качественной оценке сложно предъявить доказательства

Качество/количество: кому доверять?

- Отсутствие количественной оценки не позволяет
  - Оценить адекватность затрат на снижение рисков
  - Оценить возможность перекладывания рисков
  - Продемонстрировать снижение рисков
  - Сравнить текущий уровень с предыдущими значениями

Когда нет цифр?

- Количественная оценка не всегда возможна из-за
  - Недостатка информации о системе
  - Недостатка информации о деятельности, подвергающейся оценке
  - Отсутствии или недостатке данных об инцидентах
  - Влияния человеческого фактора
- Качественная оценка требует
  - Четкого разъяснения всех используемых терминов
  - Обоснования всех классификаций частот и последствий
  - Понимания всех плюсов и минусов качественной (экспертной) оценки

Метод: экспертная оценка

Достоинства	Ограничения
Простота реализации	Возможность влияния на экспертное мнение заинтересованными лицами
	При оценке случайных событий принцип «здравого смысла» неприменим
	Волюнтаризм экспертов
	Отсутствие достаточного количества экспертов
	Балльные оценки экспертов не позволяют судить о количественных соотношениях между оцениваемыми объектами
	Зависимость от квалификации эксперта
	Психология восприятия риска

Насколько опасно или как измерить вероятность риска?

7 подходов к оценке

Собственная статистика (первый метод)

- Историческая (статистическая) оценка позволяет на основании данных прошлых периодов прогнозировать будущее
- Один из эффективных методов
  - При условии неизменности среды оценки
- Необходимо наблюдение и сбор данных в течение нескольких лет
  - Без наличия адекватных инструментальных средств это непростая задача – сбор, нормализация, хранение и анализ данных

Чужие отчеты и статистика (второй метод)

- У нас же есть отчеты CSI/FBI, E&Y, PwC, KPMG, МВД, Infowatch, Perimetrix и т.п.!
  - Мы не знаем условий, при которых произошел инцидент
  - Мы не имеем деталей по каждому респонденту
  - Средняя температура по больнице
  - Ориентация на отрасль в целом, чем на конкретную компанию
- Пример: риски для АСУ ТП
  - Небольшое число внедрений
  - Публичной статистики нет (базы BCIT и INL не в счет)
  - Статистики вендоров нет – «закрытые» технологии
  - Собственной статистики нет – у ИБ/ИТ не доступа к АСУ ТП
  - Экспертных оценок в России нет

О доверии к статистике

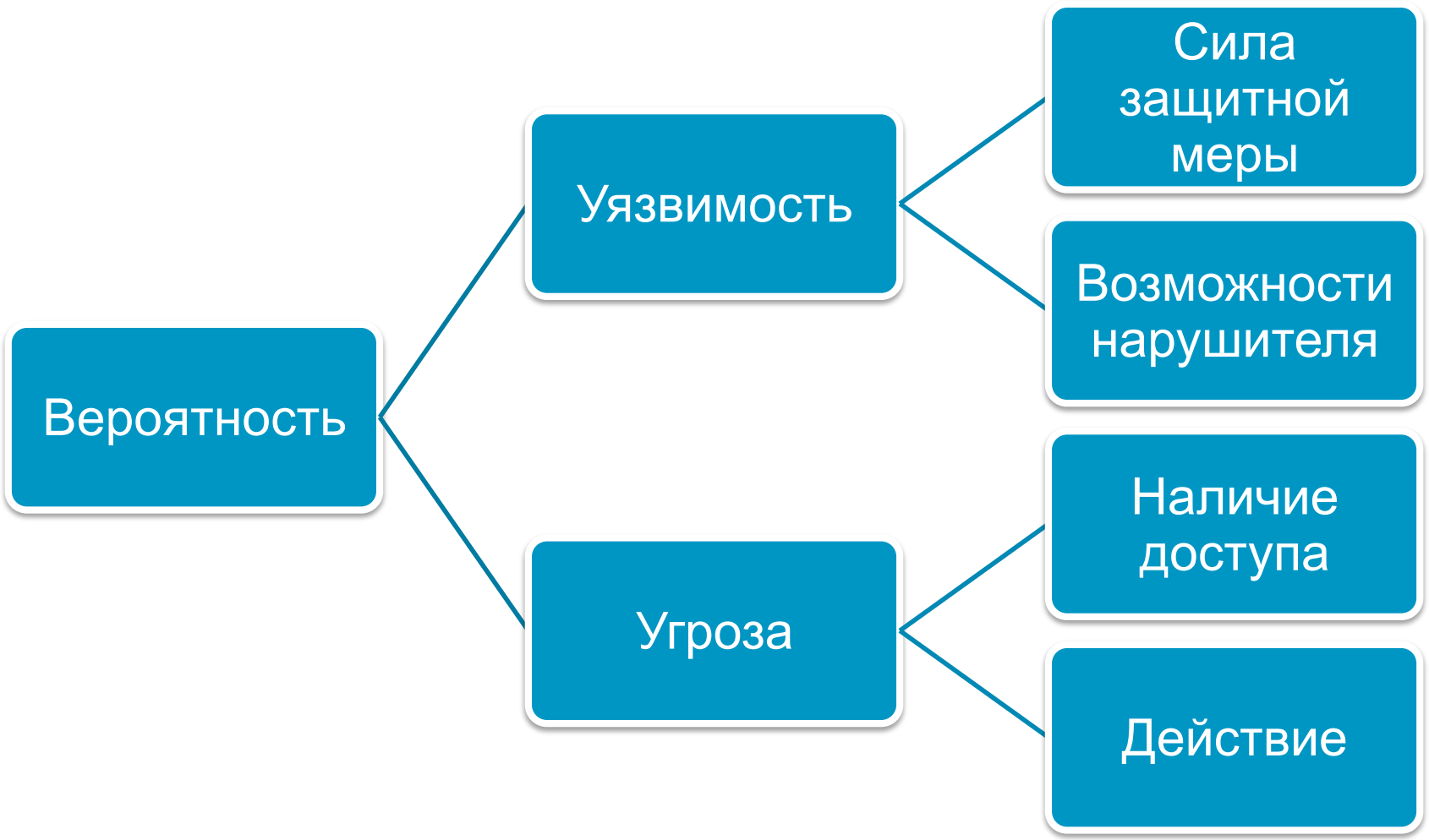
- Собираемая статистика очень сильно зависит от используемых методов опроса, аудитории, желания респондентов делиться информацией, масштаба опроса и даже от того, с какой ноги встал интервьюер
- Не каждая компания приглашает социологов для осуществления опросов

Proofpoint	Infowatch	IDC
• 43% утечек через e-mail	• 5% утечек через e-mail	• 56% утечек через e-mail

Публичные отчеты со статистикой угроз

- WhiteHat Security – Web Vulnerability Statistics
- Positive Technologies – Статистика уязвимостей Web
- CSI – CSI Computer Crime & Security Survey
- Aberdeen Group – The 2008 Email Security Report
- IBM ISS – X-Force 2009 Trend & Risk Report
- Symantec – Global Internet Security Threat Report
- MessageLabs – 2009 Annual Security Report
- Cisco – 2009 Annual Security Report
- Verizon – 2009 Data Breach Investigations Report
- PwC – 2008 Information Security Breaches Survey

Считаем самостоятельно (третий метод)



Сравнение с другими рисками (четвертый метод)

- Сравнение/сопоставление с аналогичным риском
  - ГОСТ Р 51344-99
- Сравнение с риском на аналогичном решении с учетом следующих факторов
  - Аналогичное оборудование безопасности
  - Предполагаемое использование и технологии на обоих решениях сравнимы
  - Опасность и элементы риска сравнимы
  - Технические условия сравнимы
  - Условия использования сравнимы
- Необходимо учитывать дополнительные факторы
  - Например, тип защищаемой информации или потенциал нападения

Аналитика (пятый метод)

- Прогнозирование с использованием аналитических методов
  - «Дерево неисправностей» (Fault Tree Analysis) – диаграмма всех возможных последствий инцидента в системе (МЭК 61025)
  - «Дерево событий» (Event Tree Analysis) - диаграмма всех возможных последствий данного события
  - Имитационное моделирование отказов/инцидентов
- В области ИБ не применяется или применяется крайне редко
  - В критически важных областях

Бинарная вероятность (шестой метод)

- Вероятность принимается равной единице, если угроза может быть осуществлена, и нулю – если нет
  - При отсутствии защитных мер
- Этот подход имеет право на жизнь, но только для небольшого количества систем и сценариев
  - В обычной жизни это слишком дорого
- …или для угроз, которые являются очень распространенными
- Данный метод применяется в небольшом количестве различных методик
  - Ключевые системы информационной инфраструктуры – ФСТЭК
  - Security Architecture for Enterprise (SAFE) – Cisco
  - Методика ФСБ по персданным

Когда нет цифр?

- Количественная оценка не всегда возможна из-за
  - Недостатка информации о системе
  - Недостатка информации о деятельности, подвергающейся оценке
  - Отсутствии или недостатке данных об инцидентах
  - Влияния человеческого фактора
  - Нежелания заниматься измерениями
- Качественная оценка требует
  - Четкого разъяснения всех используемых терминов
  - Обоснования всех классификаций частот и последствий
  - Понимания всех плюсов и минусов качественной (экспертной) оценки, а также психологии восприятия риска

Экспертная оценка (седьмой метод)

- При отсутствии статистической/исторической информации экспертная оценка является единственным методов определения частоты/ вероятности реализации угроз
- Эксперты ранжируют вероятность наступления события исходя из своего опыта и знаний анализируемой системы

Достоинства/недостатки метода

Достоинства	Ограничения
Простота реализации	Возможность влияния на экспертное мнение заинтересованными лицами
	При оценке случайных событий принцип «здравого смысла» неприменим
	Волюнтаризм экспертов
	Отсутствие достаточного количества экспертов
	Балльные оценки экспертов не позволяют судить о количественных соотношениях между оцениваемыми объектами
	Зависимость от квалификации эксперта
	Психология восприятия риска

Психология восприятия риска

- Даже при наличии фактов и достаточного объема информации об анализируемой системе у экспертов существует сложность с восприятием риска
- Безопасность основана не только на вероятности различных рисков и эффективности различных контрмер (реальность), но и на ощущениях
- Ощущения зависят от психологических реакций на риски и контрмеры

  Чего вы больше опасаетесь – попасть в авиакатастрофу или автоаварию?

  Что вероятнее – пасть жертвой террористов или погибнуть на дороге?

  Что опаснее – низкая квалификация персонала или универсальный червь для сетевого оборудования?

Метод Дельфи

- Основной принцип: если опросить людей, обладающих компетенцией в интересующем нас вопросе, их усредненная оценка обычно будет точна более чем на 80%
  - Если провести второй раунд, предварительно ознакомив экспертов с результатам первого, то результативность становится еще выше
- Модификация метода: брать среднюю оценку после отбрасывания крайних значений
  - Данный метод рекомендуется применять, если эксперты не могут подкрепить свое мнение серьезными аргументами
- Экспертов должно быть не менее трех, а лучше пять

Метод Дельфи: пример

Эксперты	Раунд 1	Раунд 2
Эксперт 1	50	55
Эксперт 2	65	60
Эксперт 3	100	80
Эксперт 4	30	50
Эксперт 5	60	60
Итого	**61 / 58**	**61 / 58**

Другие методы повышения качества экспертной оценки

- Нормированные z-показатели Робина Доуза
- Модель линзы Брунсвика
- Когнитивные методы Руссо
- Модель Раша
- Регрессионные модели
- Нелинейные модели

Финансовые модели оценки ИБ

Проблема финансовой оценки ИБ

- Универсального метода финансовой оценки ИБ не существует

  Возможность применения различных финансовых методик зависит от знаний и опыта как стороны демонстрирующей оценку (служба ИБ), так и стороны, которой демонстрируют

- Многие руководители (не только службы ИБ) считают, что оценить ИБ финансово невозможно

  Но можно оценить стоимость защищаемой информации, ущерб от инцидентов, эффективность проекта по IT Security

- Это возможно, но только при условии выхода на бизнес-уровень, где вы можете посчитать отдачу!

Изменение стратегии продаж

- Решение по защищенному удаленному доступу и защите от утечек информации → географическая экспансия → рост числа клиентов → рост выручки
- Решение по защищенному удаленному доступу → оснащение мобильными устройствами и подключением к Интернет → рост числа сделок → рост выручки
- Решение по защищенному удаленному доступу, защите Интернет-ресурсов → Интернет → новый канал продаж → рост числа клиентов/сделок, ускорение сделок, снижение себестоимости сделок → рост выручки

Снижение арендной платы

- Решение по защищенному удаленному доступу → перевод сотрудников на дом → уменьшение арендуемых площадей → снижение арендной платы
- Экономия на:
  - Аренда площадей
  - Питание сотрудников
  - Оплата проездных (если применимо)
  - Оплата канцтоваров
  - Оплата коммунальных расходов, ***а также***
  - Улучшение психологического климата за счет работы дома
  - Рост продуктивности

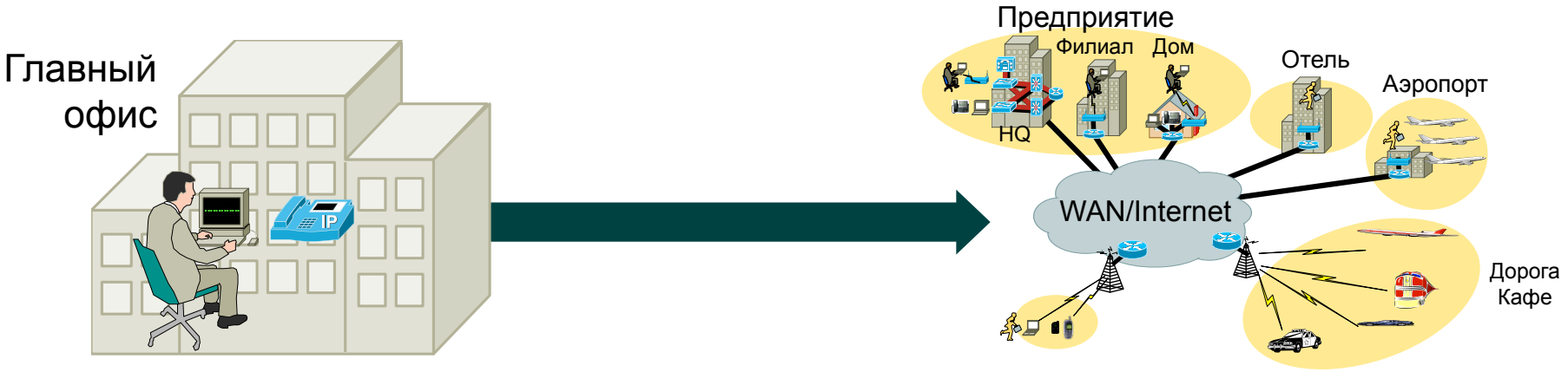
Уменьшение складских запасов

- Решение по защищенному удаленному доступу, защита Интернет-ресурсов, Identity & Entitlement Management → удаленный доступ к складской ИС поставщиков → уменьшение складских запасов
- Экономия на:
  - Уменьшение складских площадей
  - Оптимизация логистики
  - Ускорение цикла поставки

Рост продуктивности сотрудников

- Решение по защищенному удаленному доступу → перевод сотрудников на дом → снижение времени, потраченного на дорогу → рост продуктивности
- Рост продуктивности – от 10% до 40%
- Дополнительно:
  - Увеличение рабочего времени
  - Экономия на аренде площадей
  - Экономия на питании сотрудников
  - Экономия на оплате проездных (если применимо)
  - Экономия на оплате канцтоваров
  - Улучшение психологического климата за счет работы дома

Рост продуктивности



Вчера: Люди “шли” на работу	Сегодня: Работа “идет” к людям	

	100 сотрудников	500 сотрудников	1000 сотрудников
Зарплата ($25K в год)	**$2,5 млн.**	**$12,5 млн.**	**$25 млн.**
1 час потери продуктивности	**$1,200**	**$6,000**	**$12,000**
Потери в год от 1 часа в неделю	**$62,5K**	**$312,5K**	**$625K**

- Многие компании фокусируются на предоставлении сервиса на своей территории (зарплата, билеты, документооборот…)
- Сотрудник в среднем тратит только 30–40% времени в офисе

Уменьшение числа командировок

- Решение по защищенному удаленному доступу и защите унифицированных коммуникаций → внедрение видеоконференцсвязи/унифицированных коммуникаций/TelePresence → уменьшение числа командировок
- Экономия на:

  Командировочных затратах ($300-400 на авиабилет + $100 на гостиницу в сутки)

Рост продуктивности сотрудников

- Антиспам-решение → отвлечение на незапрошенную корреспонденцию → чтение электронной почты
- Экономия на:
  - Интернет-трафике
  - Времени чтения почты
  - Последствия вирусных эпидемий
- Особенности
  - Экономия на времени чтения почты имеет значение для предприятий с большим числом сотрудников

Сокращение затрат на Интернет

- Решение по контролю URL → блокирование загрузок постороннего ПО, музыки, видео и контроль посторонних сайтов → контроль действий сотрудников в Интернет
- Экономия на:

  Интернет-трафике
- Дополнительно

  Рост продуктивности (может быть)

  Защита от вирусов и троянцев в загружаемом трафике

Другие примеры

- Защита коммуникаций (технологии VPN, AAA и т.п.) → внедрение унифицрованных коммуникаций и Telepresence → снижение рисков путешествий (и затрат на них) для сотрудников
- Защита и разграничение удаленного доступа (технологии VPN, AAA, МСЭ и т.п., а также проработка юридических и организационных моментов, связанных с ИБ) → аутсорсинг → снижение издержек на ИТ
- Внедрение системы автоматического управления паролями пользователей (технология AAA) → снижение издержек на внутренний Helpdesk

Как превратить безопасность в деньги?

AAA с точки зрения денег

- Число пользователей – 120000
- Ежегодная ротация кадров – 15%
- Среднее число ID/паролей – 5
- Число рабочих часов в день – 8
- Число рабочих дней в год - 260

Первая фаза расчета – установка ID

- Ежегодное число новых пользователей – 18000 (120000*15%)
- Необходимо поддерживать 90000 новых ID/паролей (5*18000)
- Создание нового ID/пароля – в среднем 120 секунд (анализ заявки, создание и настройка учетной записи)
- Всего на администрирование новых пользователей уходит 3000 часов (~2 человека при полной нагрузке)

Вторая фаза расчета – рутина

- В среднем 20 входов в систему/приложения ежедневно (из-за истекшего таймаута, смены приложения и т.д.)
- Среднее время регистрации – 15 секунд
- Ежедневно тратится 10000 ресурсо-часов на регистрацию
- Ежегодно тратится 2200000 ресурсо-часов на регистрацию в разные системы и приложения

Третья фаза расчета – проблемы

- В среднем 1% всех попыток регистрации заканчивается неудачно
- Повторная регистрация разрешается через 60 секунд
- Общее время на повторную регистрацию в год составляет 88000 часов

Четвертая фаза расчета – поддержка

- В среднем после 3-х неудачных попыток входа в систему учетная запись блокируется
- После 2-х неудачных попыток входа рекомендуется позвонить в службу поддержки
- 2400 звонков ежедневно в службу поддержки по факту 2-х неудачных попыток входа в систему
- SLA = 4 часа на обработку одного инцидента
- 18000 пользователей ждут максимум по 4 часа – 72000 часа потери времени (продуктивности)
- 2400 звонка максимум по 4 часа – 9600 часов в день или 2112000 ресурсо-часов в год

Итого

- Время затраченное на администрирование новых ID/паролей, ежедневную регистрацию и повторные ввод ID/пароля составляет 2291000 часов в год…
  - что составляет 1% всего рабочего времени компании
- Еще 2184000 ресурсо-часов в год на поддержку неудачных попыток входа…
  - что также больше 1% всего рабочего времени компании
- Итого – 4475000 ресурсо-часов или больше 2% всего рабочего времени компании в год - только на одну задачу – управление Identity

General Motors - факты

- Предоставление доступа в среднем через 7 дней после заявки
- Синхронизация паролей и ID в разных системах – 3 дня
- 50% запросов требует контактов с пользователем
- «Разруливание» проблем с доступом – 10 дней
- Конфликт между ID может приводить к задержкам в работе до 90 дней

General Motors - потери

- Обработка 6600 проблем с доступом – потеря продуктивности – 3,000,000 долларов
- Восстановление доступа для 56000 учетных записей – потеря продуктивности – 18,200,000 долларов
- 2500 сотрудников (учетных записей) уволено – затраты на удаление – 162,500 долларов
- Прямой ущерб – 1,200,000 долларов

Финансовые модели оценки ИБ
Продолжение

Что надо сделать!

- Вспомните про цели и определение объекта измерения!
- Что вы хотите измерить деньгами
  - Сколько вы потеряете не внедрив систему защиты?
  - Сколько вы потратите на систему защиты за 3 года?
  - За сколько лет вернутся деньги, потраченные на систему защиты?
  - Выгоден ли этот проект? (определите, что для вас выгода)
  - Какая система защиты из двух дешевле? Или выгоднее?
  - Рискованны ли инвестиции в этот проект?

Классические финансовые модели
Оценка проекта по ИБ

- Total Cost of Ownership (TCO)

  Во сколько обойдется проект с учетом косвенных и всех прямых затрат?

- Net Present Value (NPV)

  Какова ценность вкладываемых финансовых ресурсов для проекта при определенной ставке дисконтирования?

- Internal Rate of Return (IRR)

  Какова ставка дисконтирования, при которой проект еще имеет смысл?

- Return on Investment (ROI)

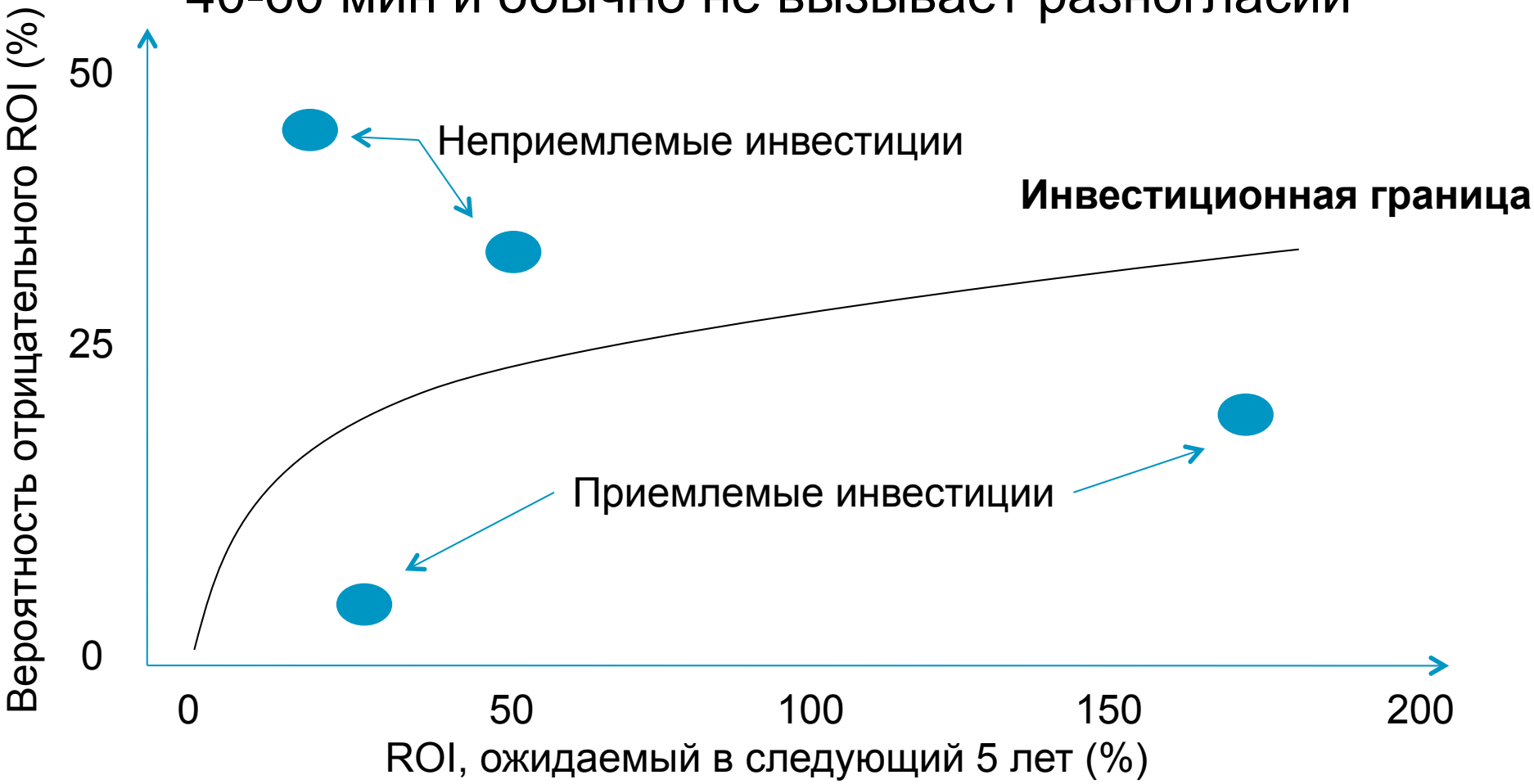
  Что мы потеряем и что получим от внедрения проекта?

- Playback Period (PbP)

  Когда вернутся инвестиции?

Уровень риск-аппетита

- Построение инвестиционной границы занимает 40-60 мин и обычно не вызывает разногласий



«Новые» финансовые методы

- Economic Value Added (EVA)
- Economic Value Sourced (EVS)
- iValue
- Total Economic Impact (TEI)
- Applied Information Economics (AIE)

Как оценить стоимость информации?

Как оценивать информацию?

- Информация стоит денег сама по себе
  - Самый простой метод
- Информация позволяет улучшить что-то
  - Стоимость информации равна разнице между стоимостью «до» и «после»
- Информация позволяет принимать решения
  - Самый сложный сценарий оценки стоимости
  - Методы AIE, iValue и другие

Малоизвестные безопасникам методы

- МСФО 38 «Нематериальные активы»
- GAAP – для США
- EVS 2000 – для Евросоюза
- Стандарты оценки РФ

  Утверждены ПП-519 от 6.07.2001

Нематериальные активы

- Патенты, изобретения, технологии…
- Авторские права
- Деловая репутация
- Фирменные знаки и наименования
- Документированные консультации
- Торговые марки
- ПО, обособленное по «железа»
- Права на эксплуатацию
- Лицензии
- И т.д.

Виды стоимости НМА

Вид стоимости	Определение
Стоимость обмена	Вероятная цена продажи, когда условия обмена известны обеим сторонам и сделка считается взаимовыгодной
Обоснованная рыночная стоимость	Наиболее вероятная цена, по которой объект оценки переходит из рук одного продавца в руки другого на открытом рынке и добровольно
Стоимость использования	Стоимость объекта оценки в представлении конкретного пользователя и с учетом его ограничений
Ликвидационная стоимость	Стоимость объекта оценки при вынужденной продаже, банкротстве
Стоимость замещения	Наименьшая стоимость эквивалентного объекта оценки

Методы оценки НМА

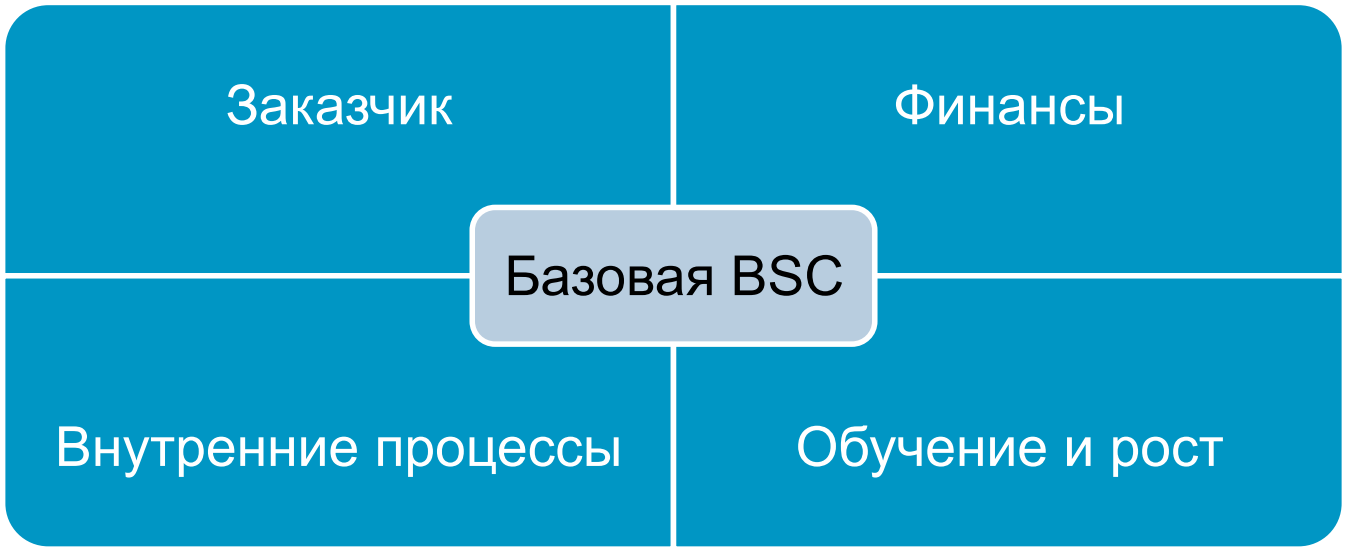
- У каждого метода есть своя область применения, свои достоинства и недостатки

Рыночный	Затратный	Доходный
• Метод сравнения продаж аналогичных объектов оценки	• Метод стоимости замещения • Метод восстановительной стоимости • Метод исходных затрат	• Метод расчета роялти • Метод исключения ставки роялти • Метод DCF • Метод прямой капитализации • Экспресс-оценка • Метод избыточной прибыли • Метод по правилу 25% • Экспертные методы

Система сбалансированных показателей

Классическая BSC

- Система сбалансированных показателей известна как метод, позволяющий оценивать предприятие не только с точки зрения финансовых показателей, а сбалансировать (именно сбалансированность является ключевым преимуществом данного подхода) оценку по 4-м направлениям



BSC для жизни

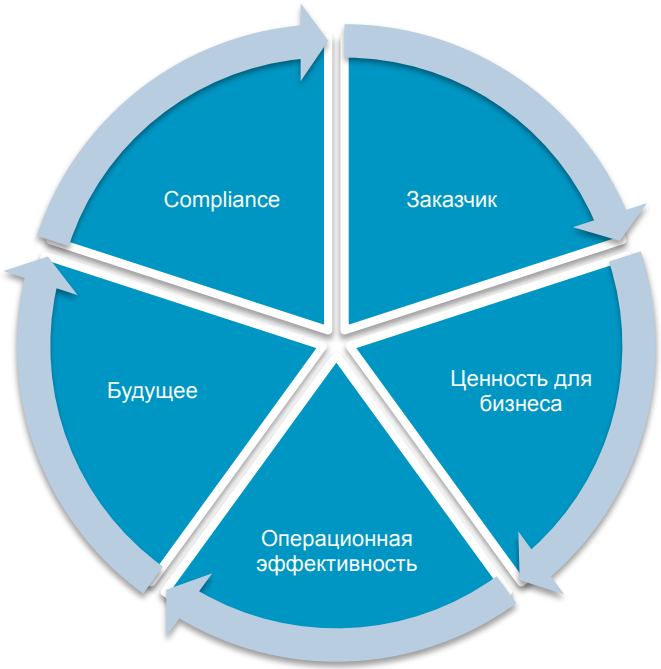
- Основная задача BSC – уйти от непонятной и сложно формализуемой миссии компании в сторону конкретных, измеряемых и достижимых целей

  При этом баланс заключается не только в оценке материальных и нематериальных активов, но и в оценке текущей деятельности и будущих перспектив, которые и позволяют компаниям развиваться в конкурентной среде, а не стоять на месте

- В последние годы ряд экспертов, внедрявших BSC на предприятиях, предложили расширить изначальные направления новыми, лучше отражающими специфику отдельных компаний

  Пользователи, поставщики, регуляторы и т.п.

BSC в ИБ



Достоинства	Ограничения
BSC – известный топ-менеджменту метод оценки бизнеса и его преломление в область ИБ позволит найти общий язык с бизнесом	Если BSC не принят в организации, то ограничение его только областью ИБ может не дать эффекта на уровне предприятия

BSC: ориентация на заказчика

Цель	Что измеряем
Удовлетворенность заказчиков	Индекс удовлетворенности заказчиков (например, по результатам опроса)
	Число сотрудников бизнес-подразделений, которым делегированы некоторые функции по ИБ
	Число сотрудников, успешно прошедших тренинги по ИБ
Партнерство с бизнесом	Частота встреч управляющего комитета
	Вовлечение службы ИБ в новые проекты, задачи и направления бизнеса (например, в виде индекса)
	Наличие в компании топ-менеджера, ответственного за ИБ
Выполнение проектов	Заданное качество проекта (например, в виде индекса)
	Завершение проекта в срок (например, в виде индекса)
	Уложились в бюджет (например, в виде индекса)
Реакция на запросы	Скорость реагирования на звонки в help desk
Выполнение SLA	Процент приложений и сервисов, для которых разработан SLA
	Число подразделений/заказчиков, заключивших SLA

BSC: ценность для бизнеса

Цель	Что измеряем
Рост выручки предприятия	Выручка от запуска нового канала продаж
Рост выручки на одного заказчика	Рост удовлетворенности заказчика
	Снижение текучки заказчиков
Снижение затрат	Разница между ценой коммерческой СЗИ и свободно распространяемой
	Стоимость звонков в help desk до и после внедрения системы автоматизированного управления паролями
	Стоимость работ по восстановлению работоспособности ИТ-инфраструктуры
Контроль и управление ИБ-бюджетом	Соотношение реальных затрат с запрошенными
	Процент ИБ-бюджета от выручки
	Стоимость ИБ на одного сотрудника
Положительный возврат инвестиций	ROI, NPV, PbP проекта по ИБ
Снижение затрат, связанных с рисками	Число инцидентов безопасности в квартал
	Число систем, соответствующих требованиям регуляторов по ИБ

BSC: операционная эффективность

Цель	Что измерять?
Эффективность процессов	Процент сбоев системы защиты
	Соответствие стандарта ISM3 или ISO 27001
	Уровень зрелости процессов управления ИБ
	Скорость процессов управления ИБ
	Качество процессов управления ИБ
Адаптивность	Время инициации проекта после первого запроса
	Время на внедрение/настройку системы защиты для нового приложения
	Скорость реакции на новые регулятивные требования
Управление проектами	Число завершенных проектов
	Процент успешно завершенных проектов
	Процент расхождения с бюджетом
Внутренняя безопасность	Текучка кадров в службе ИБ

BSC: ориентация на будущее

Цель	Что измерять?
Кадры	Процент руководителей, в MBO которых включены пункты по ИБ
	Процент сотрудников службы ИБ, имеющих планы профессионального развития
	Процент трудовых договоров, включающих пункты о соблюдении конфиденциальности и правил ИБ
Информация	Соотношение «будущее развитие/текучка» в ИБ-бюджете
	Число компаний, с которыми заключены контракты
	Число систем защиты на аутсорсинге
	Существование архитектуры ИБ
	Уровень стандартизации процессов, технологий и систем
Культура	Число сотрудников, понимающих миссию службы ИБ
	Индекс зрелости культуры ИБ
	Число задокументированных best practices или success stories в области ИБ

BSC: ориентация на регуляторов

Цель	Что измеряем?
Соответствие	Завершение аудита на соответствие PCI DSS
	Внедрение рекомендаций по управлению ИБ ITU-T X.1051
	Аттестация ФСТЭК на соответствие СТР-К
Регуляторы	Число претензий со стороны регулирующих и надзорных органов

Универсальный метод измерения

Универсальный алгоритм

1. Что вы пытаетесь измерить? Что представляет собой объект измерения?
2. Почему вы хотите его измерить? Какое решение будет принято по результатам измерения? Какое пороговое значение определяемого показателя?
3. Что вам известно сейчас?
4. Какую ценность имеет данная информация? К каким последствиям приведет ошибка? Какова ее вероятность? Какие усилия по измерению будут экономически оправданы?
5. Какие наблюдения позволят подтвердить или исключить различные возможности?

Прямая и косвенная отдача

Прямая и косвенная отдача

- Преимущества для бизнеса и использование преимуществ – это разные вещи
- Снижение арендной платы → уменьшение арендуемых площадей → перевод сотрудников на дом → решение по защищенному удаленному доступу
- Экономия на:
  - Аренда площадей
  - Питание сотрудников
  - Оплата проездных (если применимо)
  - Оплата канцтоваров
- Принятие решения о переводе принимает менеджмент
  - Надо не только предлагать решение, но и продвигать его

Прямая и косвенная отдача

Статья экономии	Человека/часов	Цена*
Идентификация несоответствующих компьютеров	1.0	$12.00
Определение местоположения несоответствующих компьютеров	1.0	$12.00
Приведение в соответствие	2.0	$24.00
Потенциально сэкономленные затраты на 1 компьютер		**$48.00**

- ИБ дала возможность сэкономить, но…
- …воспользовался ли бизнес этой возможностью?

Что дальше?

Что дальше?

- Метрики не нужны сами по себе
- Метрики нужны для принятия решений
- Не готовы к действиям – не внедряйте программу управления метриками

- Пример

  Метрика - число уязвимых ПК в финансовом департаменте за прошедший квартал

  Готовы ли мы внедрить процесс управления патчами для этих ПК?

  Готовы ли мы регулярно оценивать уязвимости и ставить новые патчи?

А что после выбора метрик?

Цель	Метрика	Целевое значение	Инициатива
Улучшить управление рисками	# инцидентов безопасности	< 7 в квартал	Обучение пользователей
	% систем защиты, отданных на аутсорсинг	43%	Заключение SLA на аутсорсинг ИБ
Улучшение управления проектами	% проектов, завершенных в срок	95%	Увеличить число сертифицированных специалистов по управлению проектами
	% проектов, выполненных в рамках бюджета	95%	Внедрение PMO в отделе
Повысить уровень бизнес-знаний в службе ИБ	% сотрудников, прошедших MBA	25%	Обучение MBA
	Количество Business Relations Manager (BRM)	1	Изменение оргштатной структуры отдела
Compliance	Соответствие ISO 27001	Получение сертификата через год	Обучение по ISO 27001 Внедрение compliance-решения
Улучшение операций	% сбоев в системе защиты	< 5 в квартал	Внедрение системы контроля качества

Заключение

Прогресс и изменения

- Все жаждут прогресса, но никто не хочет изменений
- Люди инертны

  Склонны верить тому, что узнали в самом начале (ВУЗе, первой работе и т.д.)

  Ленивы и не будут упорно трудиться ради изменений

  Людей устраивает средний результат. Это зона комфорта. Best Practices никому не нужны (как и мировые рекорды)

  Люди считают свои решения лучшими
- Чтобы пересмотреть точку зрения, человека надо долго переубеждать или показать воочию
- Изменения происходят не вдруг – имейте терпение

Новый взгляд на безопасность

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +38 044 391-3600