Как посчитать эффективность информационной безопасности?

Алексей Лукацкий

Бизнес-консультант по безопасности

О чем пойдет речь

- Зачем измерять безопасность?
- Чем измерять безопасность?
- Как нужно измерять безопасность?
- Подводные камни
- Что дальше?

Что говорит и думает руководство?

- Он спрашивает: «Каков уровень риска?»

  Он думает: «Чем нам это грозит?»

- Он спрашивает: «Соответствуем ли мы требованиям?»

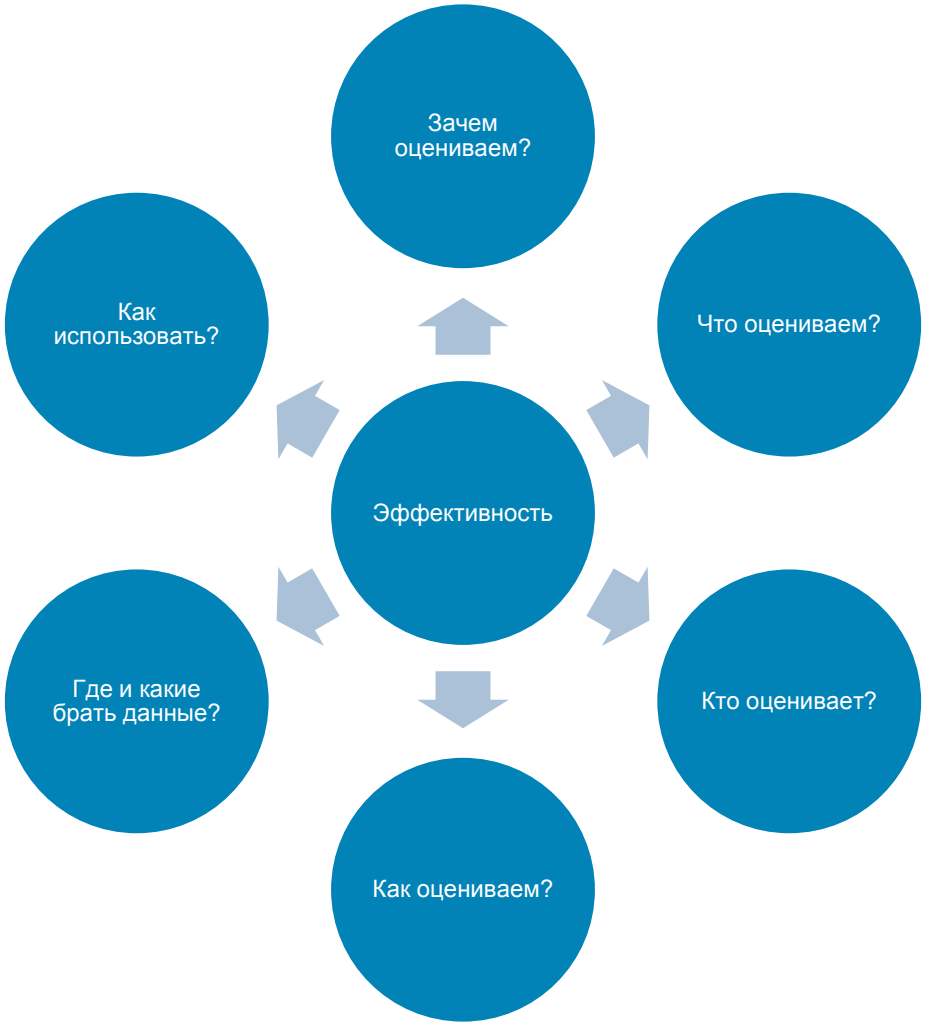
  Он думает: «Не накажут ли нас?»

- Он спрашивает: «Почему так дорого?»

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

- Знания CISO/CIO не совпадают с восприятием CxO

Оценка эффективности ИБ



А можно ли вообще измерять?

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

Зачем нужно оценивать эффективность ИБ?

Зачем нужно измерять безопасность

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

Бизнес

- Безопасность с точки зрения бизнеса – процесс, демонстрирующий, как связанные с безопасностью изменения и инвестиции, с течением времени обеспечивают достижение бизнес-целей
- Любая активность в компании должна подчиняться бизнес-целям

  Не обязательно финансовым – compliance, лояльность заказчиков, географическая экспансия, рост доли рынка
- Достижение цели может быть продемонстрировано только в том случае, если мы можем оценить и измерить, насколько достигнуты результаты

Стандарты

- Об измерении и оценке эффективности информационной безопасности говорят многие стандарты
  - ISO 17799 (ISO 27002)
  - COBIT
  - ITIL
  - ISO 13335
  - ISO 21827
  - GAISP

Инвестиции

- Выигрывает не тот, кто сильнее, а тот кто лучше приспособлен
- Множество проектов и инициатив при нехватке финансовых средств
  - Особенно в условиях кризиса
- Деньги получает тот, кто может сможет лучше обосновать запрашиваемые ресурсы
  - Сколько надо? Почему столько? Какова отдача?

Цели

Бизнес-цель

- «Бизнес-цели» - отталкиваемся не от того, ЧТО защищаем, а КУДА стремимся
- Бизнес-цели не всегда связаны с финансами
  - Нельзя искать только финансовую выгоду от решения вопросов безопасности
  - Необходимо учитывать нефинансовые цели (например, лояльность клиентов) и синергетический эффект
- Бизнес-цель может быть
  - У всего предприятием
  - У отдельного подразделения
  - У отдельного проекта/инициативы
  - У отдельного «важного» человека («спонсора»)

Как определить бизнес-цели?

- Каким бизнесом занимается организация?
- Какие стратегические продукты, сервисы и инициативы в организации?
- Каковы активности и потребности?
- В каких странах и индустриях делается бизнес?
- Какие тенденции, законы и требования отличаются в разных странах?
- Каковы внутренние процессы и политики?
- С кем регулярно ведет бизнес организация?

Как определить бизнес-цели?

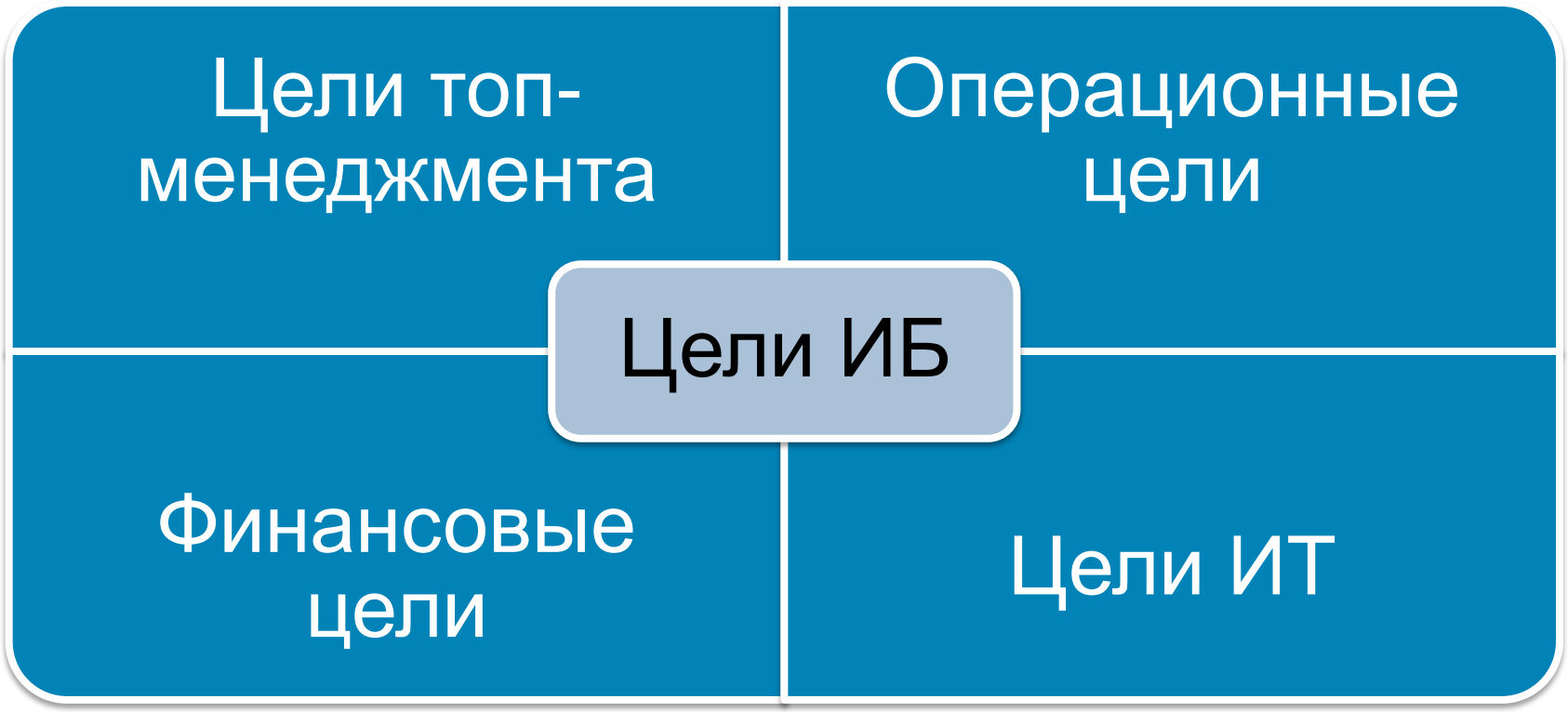
- Какова политическая ситуация?
- Кто владельцы бизнеса?
- Каков уровень зрелости организации?
- Какие бизнес-задачи сложно или невозможно реализовать?
- Каковы риски?
- Каковы стратегические ИТ-инициативы?

- Не выдумывайте – поинтересуйтесь у топ-менеджмента!

Примеры бизнес-целей

- Рост продуктивности сотрудников
  - Network Virtual Organization (NVO)
- Ускорение вывода продукта на рынок
  - Доступ поставщиков и партнеров к корпоративной сети
- Аутсорсинг бизнес- или ИТ-процессов
  - Данное бизнес-требование демонстрирует, что безопасность может быть не столько технической задачей, сколько юридической
- Географическая экспансия
  - Конфликт законодательств разных стран для международных компаний или сдвиг PoS / PoD
- Поглощения и слияния

Достижение каких целей измеряем?



- Цели ИБ в данной ситуации вторичны, т.к. их никто не понимает кроме службы ИБ

  Грустно это признавать, но это так

Метрики информационной безопасности

Что такое «метрика безопасности»?

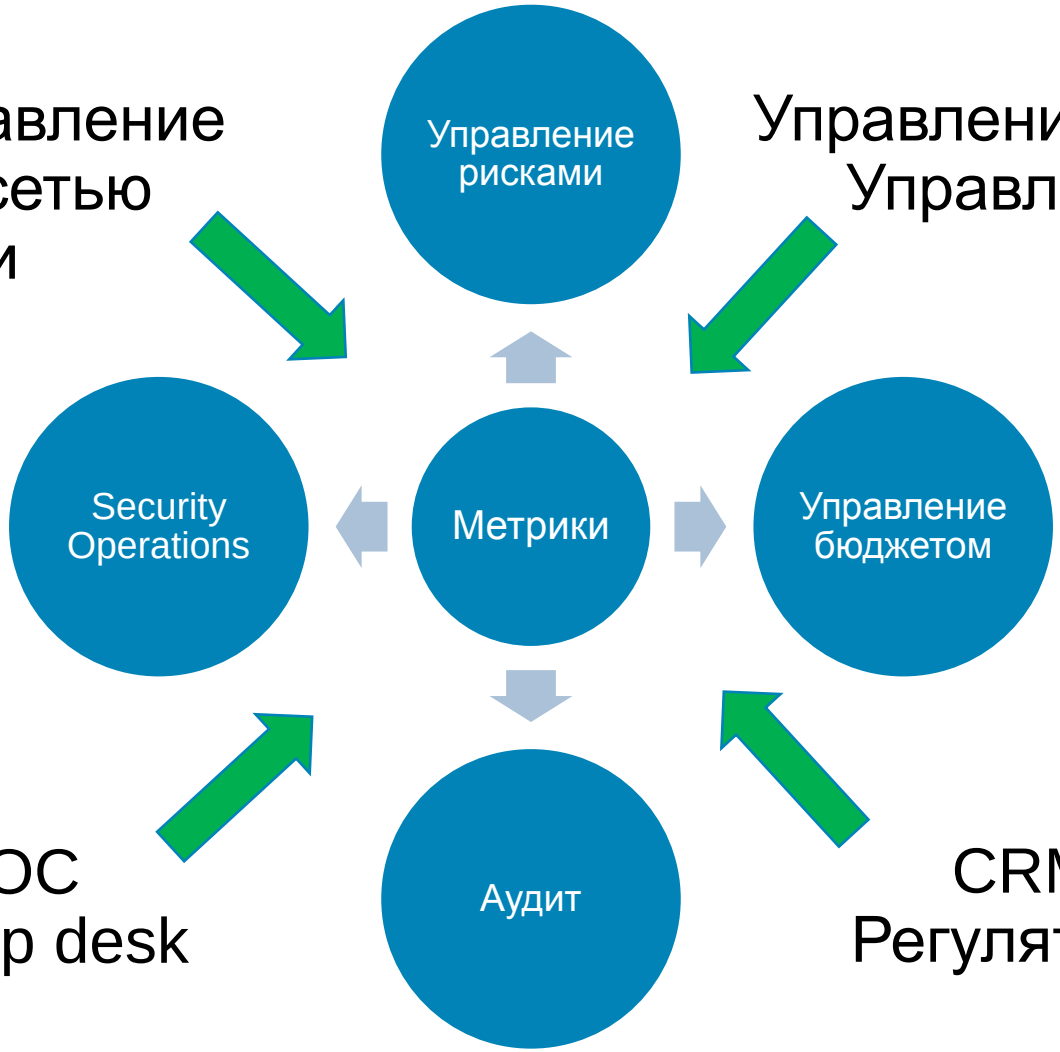
- Метрика – стандарт измерения, использующий количественный, статистический и/или математический анализ
- Метрика безопасности – способ применения количественного, статистического и/или математического анализа для измерения «безопасных» стоимости, преимуществ, удач, неудач, тенденций и нагрузок

  Отслеживание статуса каждой функции безопасности

- KPI, KRI, PI = метрика

Зачем нужны метрики ИБ?

Системное управление
Управление сетью
Политики

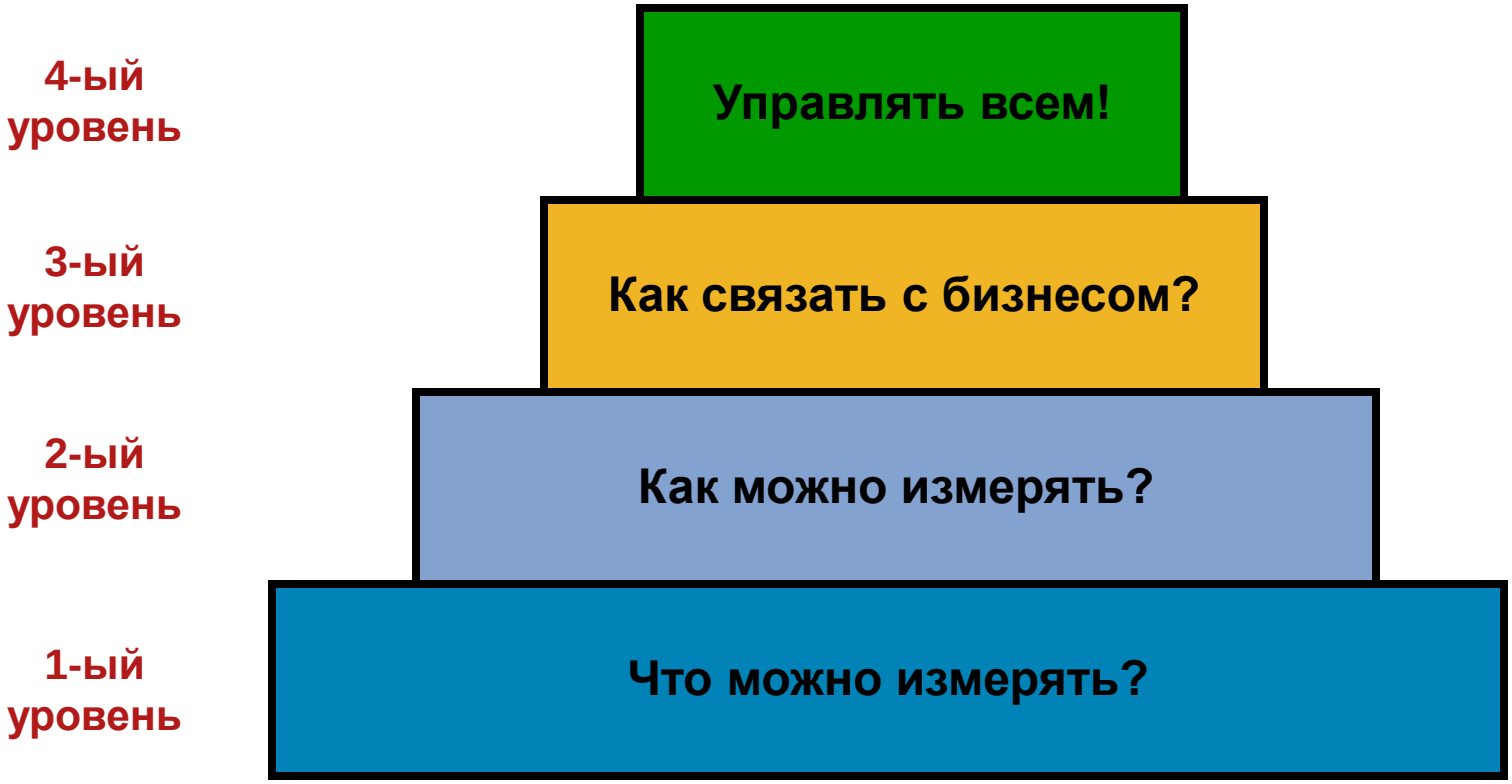


Управление активами
Управление HR

SOC/NOC
Service\Help desk

CRM
Регуляторы

Модель зрелости программы метрик



Качество или количество?

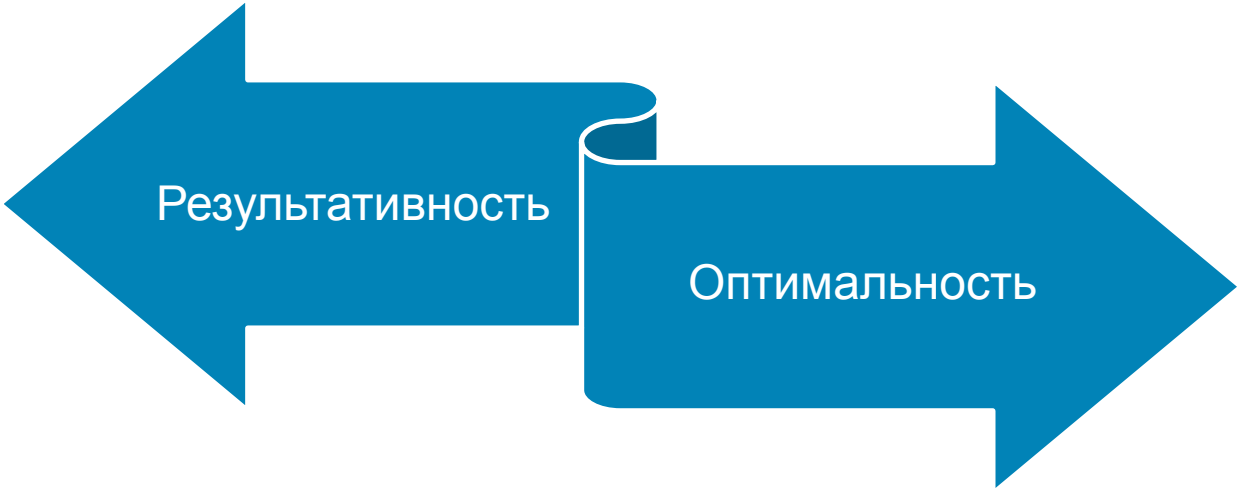
- 1954 г. - Paul Meehl – «Clinical Versus Statistical Prediction: A Theoretical Analysis and Review of the Evidence», 1954

  Работа обновлена в 1996

- Количественная оценка работает лучше экспертной (качественной)

  В 136-ти случаев из 144-х

Efficiency vs. Effectivness



- Сначала мы обычно оцениваем достижение цели как таковой (результат)

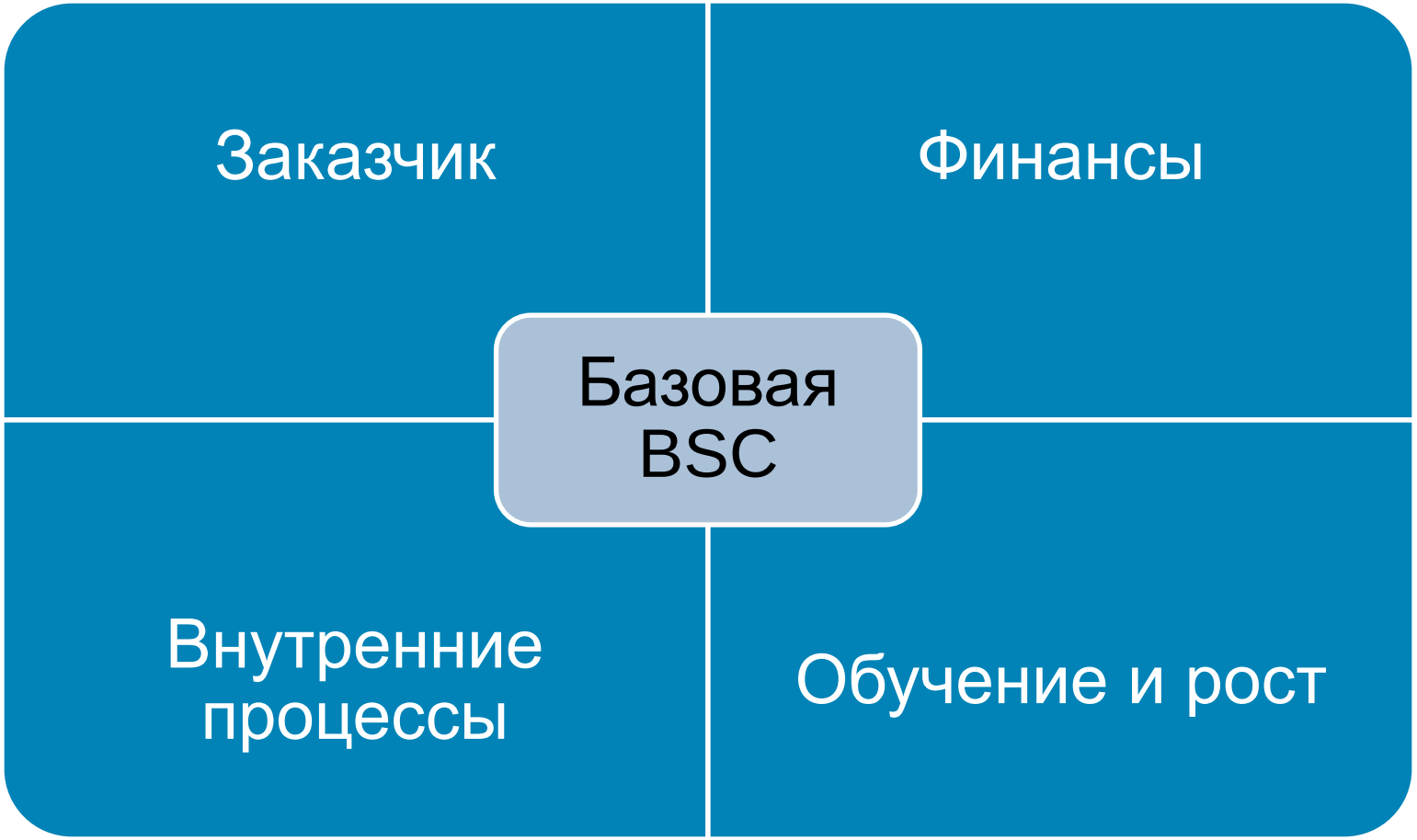
  Но интересно ли нам достижение цели любыми средствами?

Антиспам

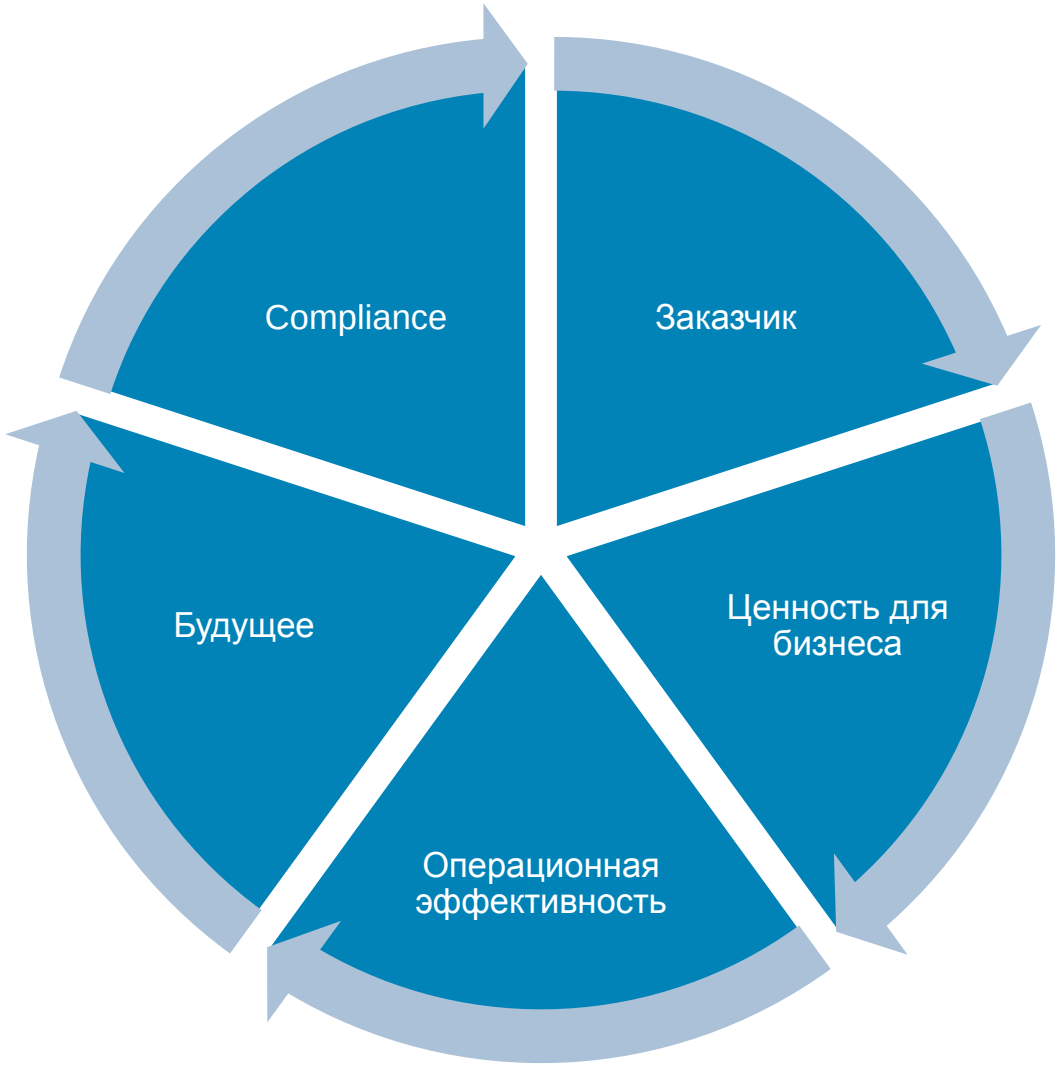
- Процент заблокированного спама
- Процент прошедшего спама через антиспам и о котором сообщили сотрудники, прошедшие тренинг повышения осведомленности

Иерархия метрик

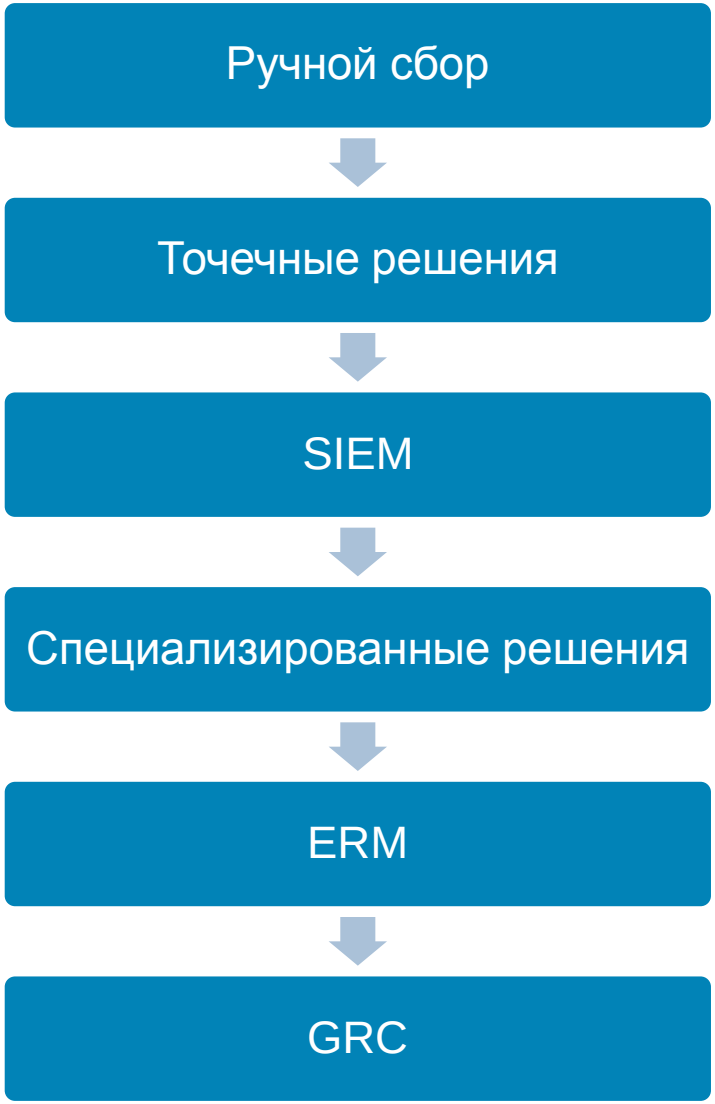
Нефинансовые метрики



Нефинансовые метрики



Автоматизация оценки



- На этапе выбора метрик автоматизация не является критичной
- На этапе сбора данных и вычисления метрик автоматизация становится критичным фактором

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

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

- 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 бизнесе
- Метрика должна быть релевантной, измеримой в адекватных терминах и, желательно, ассоциированной со стоимостью
  - Время/стоимость простоя пользователя в месяц
  - Не идеальна, но соответствует требованиям

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

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

Пример: система 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

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
KPI	Оценки операционных рисков	Проекты по KPI для ИТ/ИБ не получили пока широкого распространения

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

Миф о снижении издержек

- Часто упоминается, что системы защиты повышают эффективность персонала и снижают издержки
  - Это не совсем так!
- Новые системы защиты $\Rightarrow$ новые, ранее невыполняемые функции $\Rightarrow$ возрастает нагрузка на персонал защиты
  - Или увеличивается его численность
- В результате растет стоимость системы защиты

Ошибки при оценке эффективности

Типичные ошибки

- Выбор сотен метрик вместо концентрации на стратегических
- Измерение того, что проще измерить, вместо концентрации на целях измерения
- Отсутствие бизнес-фокусировки
- Фокус на операционных результат-ориентированных метриках вместо оценки эффективности процесса
- Отсутствие контекста

  Снижение цены ИБ при росте инцидентов
- Отсутствие сотрудничества с другими и доверия к себе

Заключение

Прямая и косвенная отдача

- Преимущества для бизнеса и использование преимуществ – это разные вещи
- Снижение арендной платы → уменьшение арендуемых площадей → перевод сотрудников на дом → решение Cisco 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?

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

Что осталось за кадром

- База метрик ИБ
- Комитет выбора метрик
- Сколько метрик нужно?
- Тестирование метрик
- Пересмотр метрик
- Методы измерения эффективности
- Презентация и визуализация метрик

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410