ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ

ООО «Интеллектуальная безопасность»

Экономическая оценка ИБ

3 года спустя

Сентябрь, 2016

Плоскости безопасности

Дихотомии информационной безопасности:

- Реальна/абстрактна
- Эмоциональна/рассчитываема
- Калькулируема/оцениваема

Парадигма восприятия

Качественная оценка ИБ – эмоциональная и субъективная оценка, подверженная множеству спекуляций.

Люди преувеличивают риски, которые:	**Люди преуменьшают значение рисков, которые:**
Производят глубокое впечатление	Не привлекают внимание
Случаются редко	Являются обычными
Персонифицированы	Анонимны
Неподконтрольны или навязаны извне	Контролируются в большей степени или принимаются добровольно
Обсуждаются	Не обсуждаются

Было проведено более 270 исследований на тему восприятия риска

Банальность

Информационная безопасность – это процесс.

Информационная безопасность – это управленческий процесс, вернее его часть.

Главное в оценке влияния одного процесса на другой или целое – дискретность.

Предпосылки расчета

1. Знание себя
2. Процессный подход в ИБ и ИТ
3. Риск ориентированный подход
4. Фокусирование на узких местах (теория ограничений, TOC)
5. База инцидентов

Аксиомы парадигмы расчета

1. Не понесенные убытки = доходы
2. Наибольшие убытки наносят события, к которым мы наименее готовы
3. Качественнее – значит дороже
4. Разумная цена
5. Консалтинг – всегда эффективен (временной фактор не критичен)
6. Новые технологии – всегда эффективны (временной фактор критичен)

Хватает ли ROI?

$$ROI = \frac{\text{Прибыль}}{\text{Размер инвестиций}} \times 100\%$$

$$= \frac{\text{Доходы} - \text{Расходы}}{\text{Размер инвестиций}} \times 100\%$$

Проблемы расчета эффективности ИБ

- Обобщённость размера Доходов и Расходов
- Расходы ≥ Размер инвестиций
- Не учитывается стоимость денег
- Проблема расчета ТСО
- Фрагментарность рассматриваемых проектов

Для фанатов формул

$$C = \sum_{i,m=0}^{n} (M_i \times P_i \times K_m \times S_m \times T)$$

M – величина показателя

P – вероятность возникновения

K – нормирующий коэффициент

S – поправка на значимость

T – время

C – коэффициент эффективности

Группы показателей

Группы показателей:

- Производственные
- Инфраструктурные
- Управленческие
- Организационные
- Антропогенные
- Законодательные
- Санкции
- Нарушения
- Репутационные

Значимость

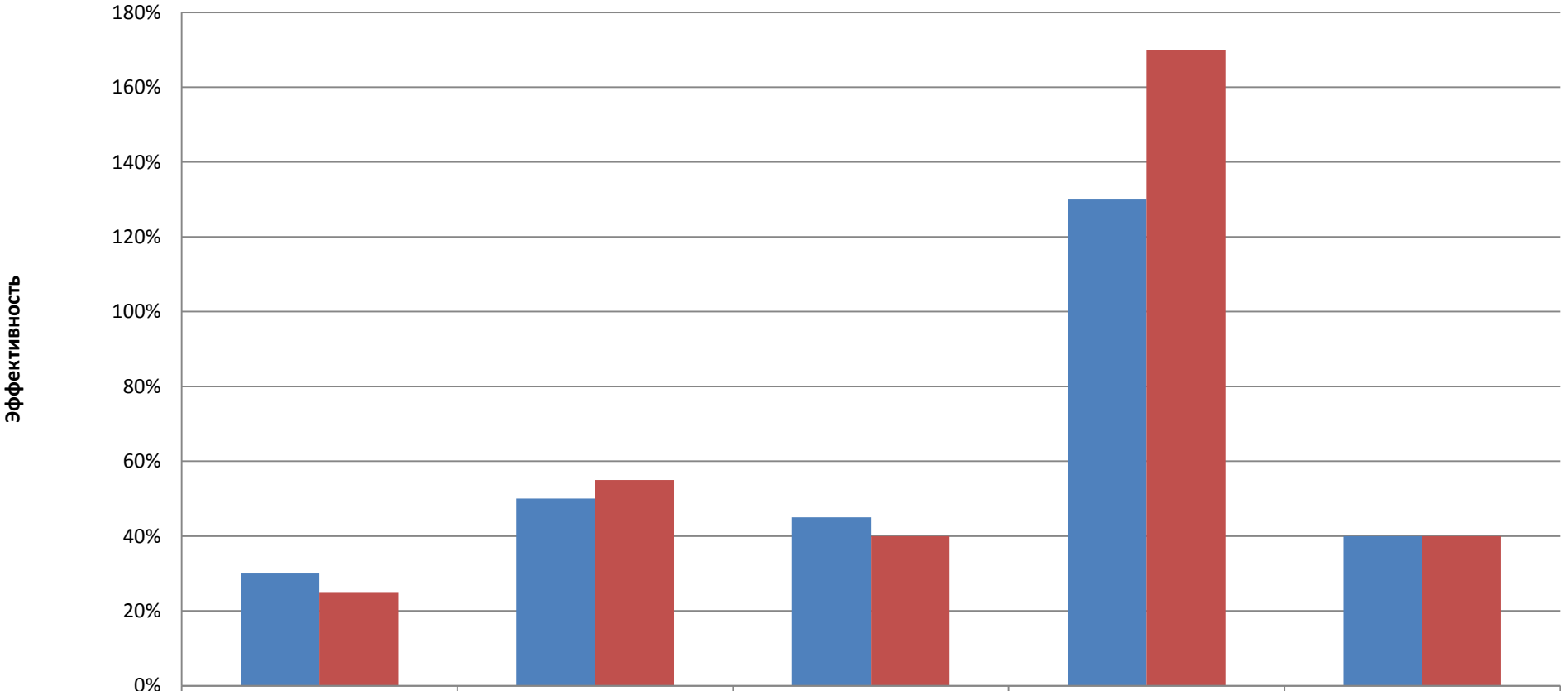
Уровень 1: Операции
Уровень 2: Консолидации
Уровень 3: Интеграции
Уровень 4: Оптимизации
Уровень 5: Инновации

+ Размер

Измерения уровней:

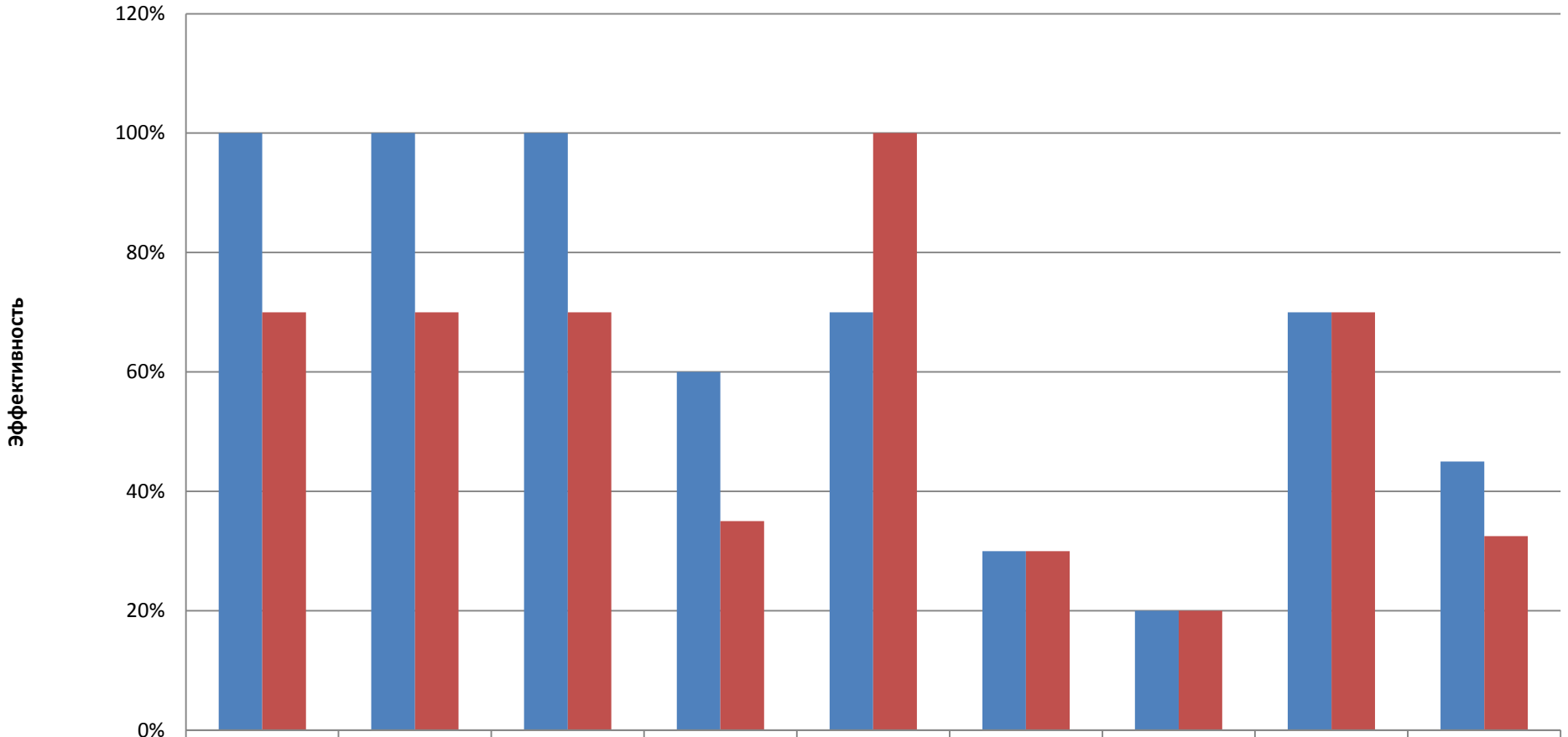
- Инфраструктура
- Процесс получения знаний
- Человеческий капитал
- Культура

Средняя температура по больнице



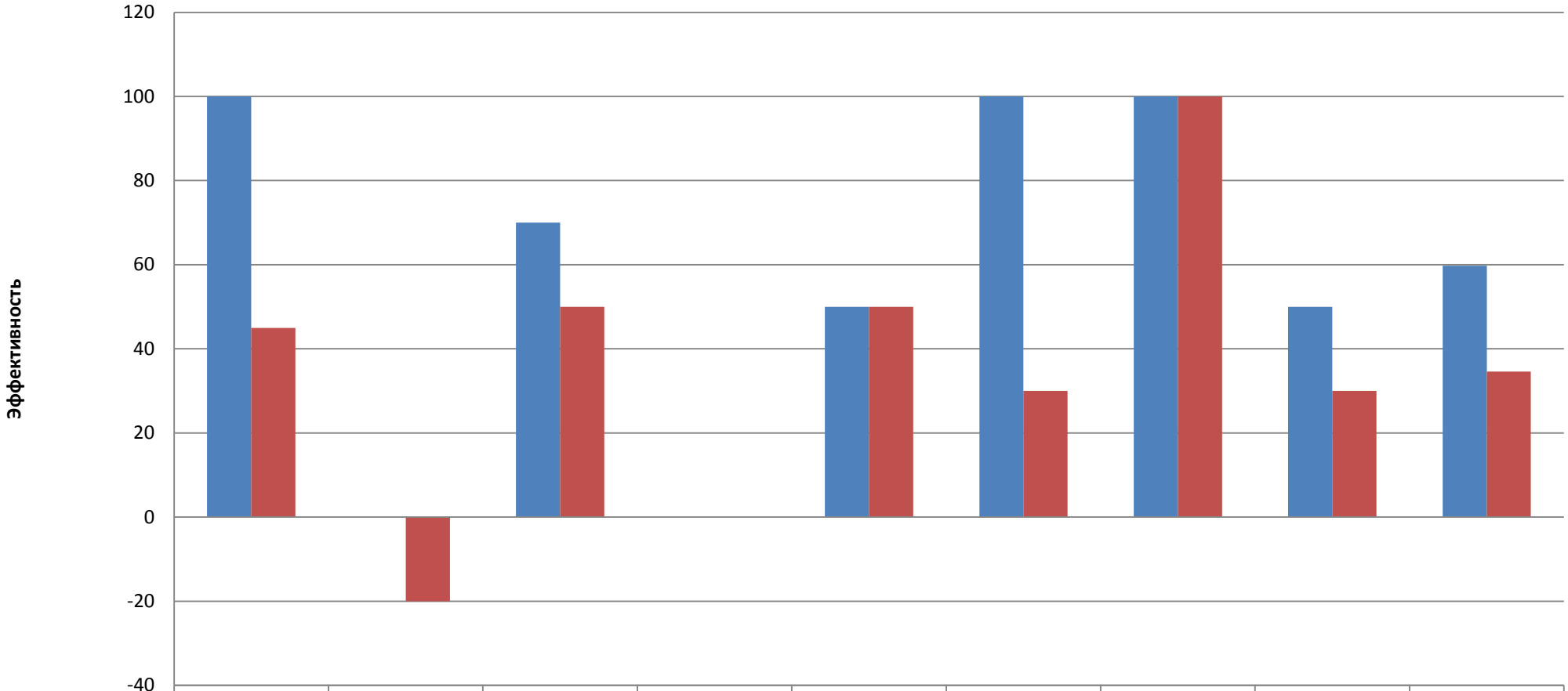
	СКС	Сетевое оборудование	Серверное оборудование	Автоматизация БП	Информационная безопасность
Аналитическое	30%	50%	45%	130%	40%
Постфактум	25%	55%	40%	170%	40%

Пример. Эффективность работ



	1.Аудит ИСПДн (2010 год)	2.Проектирование СЗПДн (2010 год)	3.Разработка ОРД (2011 год)	4.Внедрение СЗПДн (2012 год)	5.Актуализация проекта и ОРД (2012 год)	6.Аттестация (2012 год)	7.Техническая поддержка (2013 год)	Медиана (всех работ)	Медиана (работ 2012-13 гг)
Аналитическая	100%	100%	100%	60%	70%	30%	20%	70%	45%
Постфактум	70%	70%	70%	35%	100%	30%	20%	70%	33%

Эффективность внедрения СЗПДн



	Производственные	Инфраструктурные	Управленческие	Организационные	Антропогенные	Законодательные	Санкции	Нарушения	Среднее
Аналитическое	100	0	70	0	50	100	100	50	60
Постфактум	45	-20	50	0	50	30	100	30	35

Что еще?

Ответ на конкретные управленческие вопросы.
Формулировка правильных вопросов.

Например:

CISO Top-5 банка: стоит ли мне платить по 30 млн. долларов в год за систему защиты от DDOS?

Стало:

- Нужна ли система DDOS?
- Эффективна ли система?
- Есть ли аналоги?

Контакты

Дудко Дмитрий

E: dd@securityvision.ru

SECURITY VISION

УВИДЕТЬ БЕЗОПАСНОСТЬ

Дополнительная информация о Security Vision в сети:

www.securityvision.ru | https://ru.wikipedia.org/wiki/Security_Vision