



КАК УВЯЗАТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ С ТРЕБОВАНИЯМИ БИЗНЕСА

ПОДХОД CISCO SYSTEMS

Алексей Лукацкий
Бизнес-консультант по безопасности



Содержание

- **Смена приоритетов**
- **Изменение взгляда на информационную безопасность**
- **Связь ИБ и бизнеса**
- **Метрики оценки**
- **Заключение**

СМЕНА ПРИОРИТЕТОВ



На что все ссылаются...

Gartner: 10 тенденций для СІО в 2004

- Взломы/нарушение бизнеса**
- Операционные издержки/бюджет**
- Защита данных и конфиденциальность**
 - * Рост доходов
 - * Эффективное использование информации
 - * Восстановление экономики
- Единый взгляд на заказчика (CRM)
- Ускорение инноваций
- Прозрачность отчетности
- Управление рисками предприятия

Рейтинг		
2002	2003	2004
-	12	↑ 1
1	1	↓ 2
4	2	↓ 3
-	-	↑ 4
-	-	↑ 5
-	-	6
3	5	7
5	3	8
-	7	9
-	4	10

↑ ↓ Смена приоритетов с 2003 года

* Новые вопросы для 2004

Как обстоит на самом деле

Gartner: 10 тенденций для CIO в 2006

- Улучшение бизнес-процессов
- Операционные издержки/бюджет
- Привлечение, удержание и рост клиента
 - ** Поддержка конкурентных преимуществ
 - ** Улучшение конкурентоспособности
- Расширение использования информации
- Взломы сетей и нарушение бизнеса
- Рост доходов
- Ускорение инноваций
- Защита данных и конфиденциальность

Рейтинг		
2004	2005	2006
**	1	↔ 1
2	3	↑ 2
*	*	3
**	4	↔ 4
*	*	5
5	7	↑ 6
1	2	↓ 7
4	6	↓ 8
7	10	↑ 9
3	5	↓ 10

↑ ↓ Смена приоритетов с 2005 года

* Новые вопросы для 2006

Чего не хватает? На что делать ставку?

Gartner: 10 приоритетов CIO в 2006

- Реализация проектов для роста бизнеса
- Связь ИТ и бизнес-стратегий и планов
- Бизнес-знания среди ИТ-специалистов
 - Демонстрация бизнес-значения ИТ
- Привлечение, обучение и удержание ИТ-персонала
- Применение метрик оценки деятельности ИТ
 - Рост качества ИТ-сервиса
- Гибкость технической инфраструктуры
 - Улучшение управления ИТ
 - Консолидация ИТ

Рейтинг		
2004	2005	2006
18	1	↔ 1
4	2	↔ 2
1	9	↑ 3
2	3	↓ 4
*	*	5
14	4	↑ 6
3	7	↔ 7
*	*	8
11	10	↑ 9
**	8	↓ 10

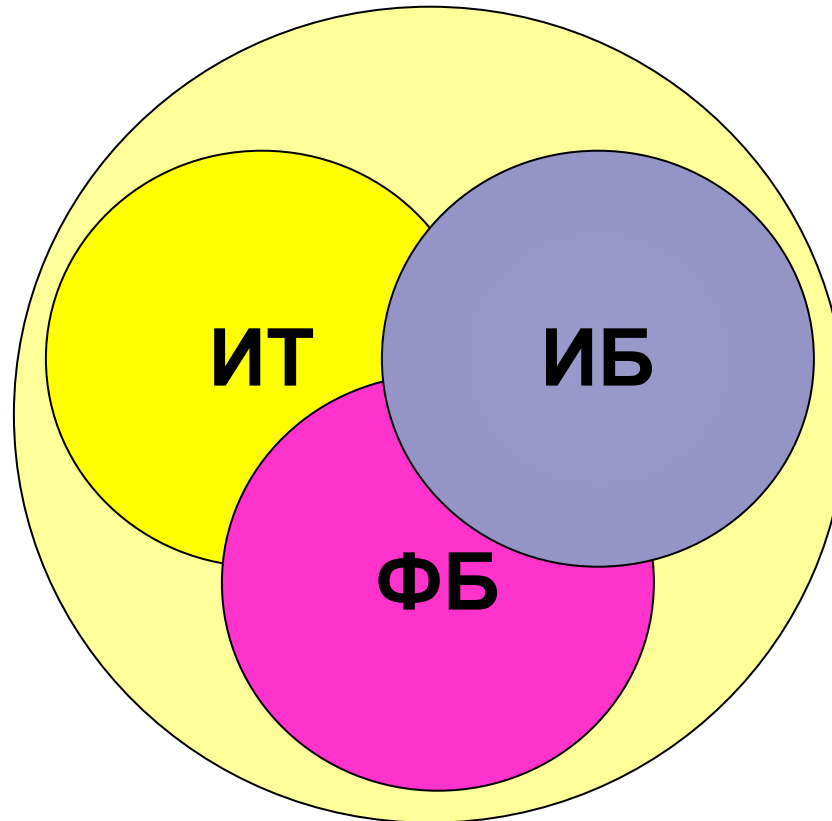
↑ ↓ Смена приоритетов с 2005 года

* Новые вопросы для 2006

ИЗМЕНЕНИЕ ВЗГЛЯДА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ



ИБ – это не только ИТ



- **Информационная безопасность очень тесно связана с остальными процессами в компании**

Информационная безопасность сегодня

- **Информационная безопасность часто воспринимается, как тактическая и чисто техническая задача**
- **Информационная безопасность не нужна сама по себе**
 - Только в приложении к бизнесу-процессам и бизнес-требованиям
- **Для эффективного управления ИБ мы должны сконцентрироваться на 5 основных вопросах**

5 ключей к эффективному управлению

ПРИНЦИПЫ ИСПОЛЬЗОВАНИЯ ИБ

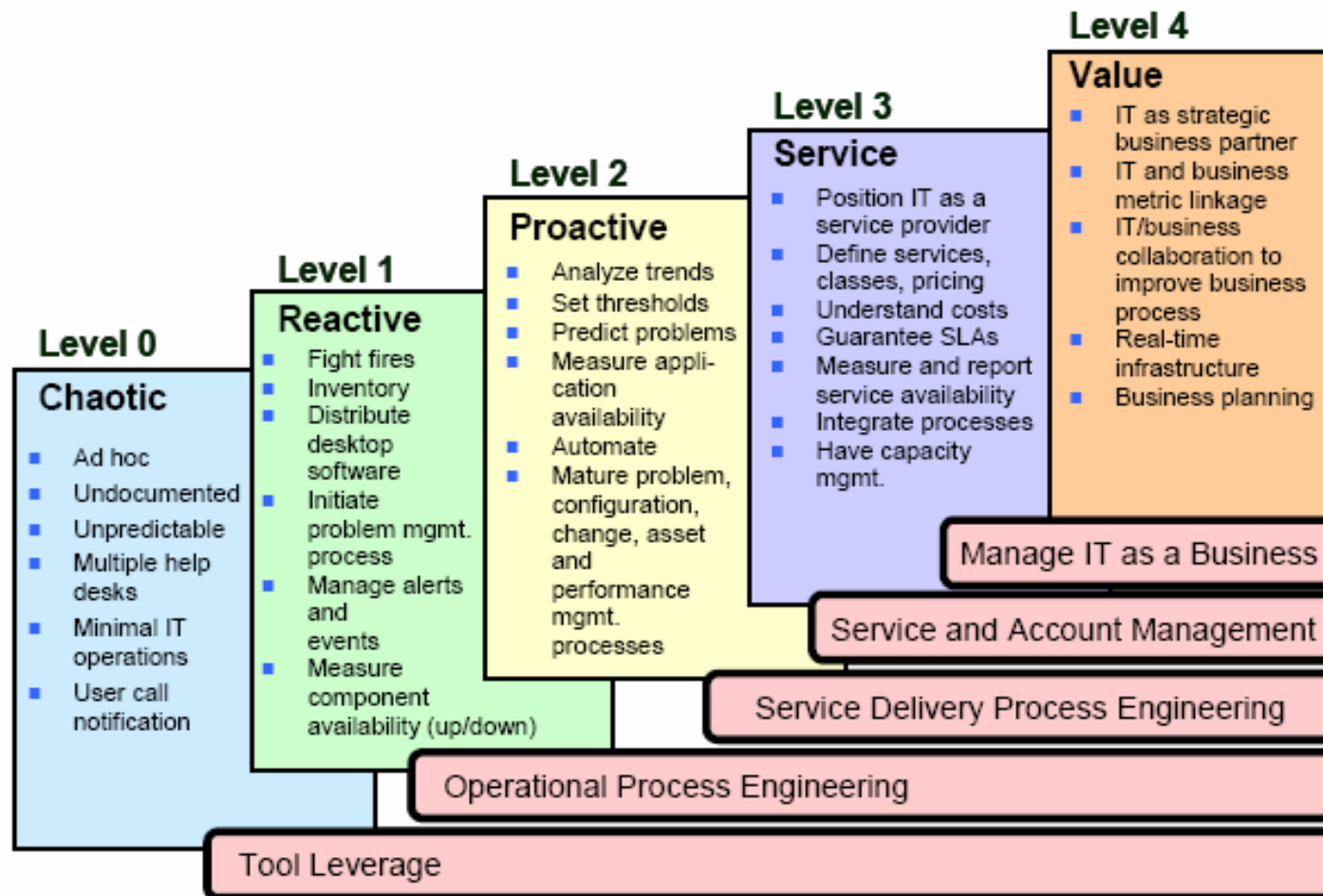
АРХИТЕКТУРА
Требования
План

ИНФРАСТРУКТУРА
ПРИЛОЖЕНИЯ

ИНВЕСТИЦИИ
Ресурсы
Приоритеты

СВЯЗЬ С БИЗНЕСОМ

5 уровней развития ИБ в компании



- От хаоса к бизнес-потребностям

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БИЗНЕС

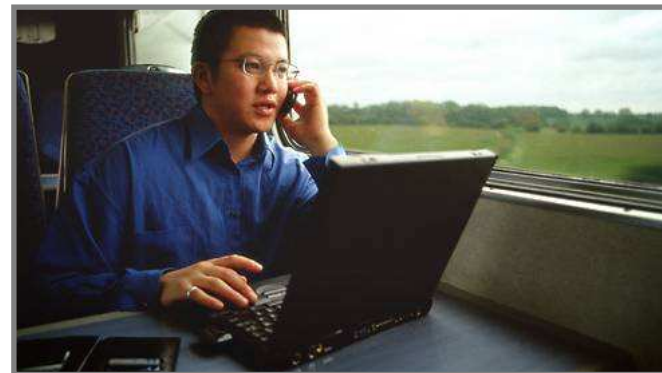


Как увязать ИБ и бизнес?

- **Традиционная модель – подсчет предотвращенных потерь и убытков**
 - Вероятностная оценка
 - Человеческий менталитет («Пока гром не грянет...»)
 - Технический подход
- **Правильная модель – показ значимости для бизнеса**
 - Количественная оценка – Как ИБ может помочь заработать или сэкономить денег?
 - Качественная оценка – Что поможет сделать ИБ в контексте стратегии бизнеса?

Виды убытков

- **Финансовые претензии за упущенную выгоду, срыв договорных обязательств и т.п.**
- **Уголовная ответственность**
- **Снижение стоимости акций**
- **Экологические катастрофы**
- **Другие типы исков**
- **Наказывают не виноватого, а имеющего ресурсы для возмещения ущерба**



Пример ChoicePoint

ChoicePoint – Февраль 2005

- Кража отчета с 150,000 именами клиентов, номеров кредитных карт и т.д.

Воздействие на бизнес

Администрация штата Нью-Йорка отказалась от контракта с ChoicePoint на сумму 800 миллионов долларов



О чем думает CEO?

- **Беспокойство о будущем росте бизнеса**

- **Рекомендация Cisco Systems:**

Не отвлекайтесь на мелочи

Выделите стратегические и долгосрочные показатели роста вашего бизнеса и свяжите свои инициативы по безопасности с ними

Покажите, что внедряемые проекты помогают, а не тормозят развитию бизнеса

Сбалансируйте свои проекты по безопасности и будьте гибкими

- **Примеры: VPN**

О чем думает CEO?

- **Рост конкуренции**
- **Рекомендация Cisco Systems:**
 - Покажите, что внедряемые проекты по ИБ помогут быть лучше, чем конкуренты (снижение CAPEX/OPEX, рост лояльности клиентов, более быстрое обслуживание, новые формы обслуживания и т.п.)
 - В ряде случаев проекты по безопасности позволяют даже открыть новые статьи доходов
 - Предотвращение промышленного шпионажа
- **Примеры: MSS и технологии контроля утечки информации**

О чем думает CEO?

- **Информационная перегрузка менеджеров**
- **Рекомендация Cisco Systems:**
 - **Доносите до руководства не все, что происходит в ИБ, а только то, что имеет первостепенное значение для бизнеса – не держите руководство в неведении**
 - **Внедрите Security Dashboard с ключевыми показателями деятельности по ИБ**
- **Примеры: SIMS, SEMS, STMS**

О чем думает CEO?

- **Слияния и приобретения**
- **Рекомендация Cisco Systems:**
 - ИБ влияет на прозрачность и управляемость бизнеса → прозрачность и управляемость бизнеса влияет на кредитный рейтинг компании → кредитный рейтинг влияет на привлекаемые инвестиции**
 - ИБ позволяет контролировать вновь приобретенные активы**
- **Примеры: все защитные технологии**

О чем думает CEO?

- **Законодательное регулирование**
- **Рекомендация Cisco Systems:**

В России намечается усиление роли государства в контроле над информационными технологиями, в борьбе с терроризмом, нарушением таможенного и иного законодательства

Желательно использовать сертифицированное и официально ввезенное на территорию России оборудование и программное обеспечение по безопасности

Западно-ориентированные компании должны соблюдать множество стандартов и законов – SoX, HIPAA, Bill 1386, GLBA и т.п.

Пример ChoicePoint

ChoicePoint – Февраль 2005

- Кража отчета с 150,000 именами клиентов, номеров кредитных карт и т.д.

Воздействие на бизнес

Компания вынуждена была заплатить большие штрафы и понесла судебные издержки за нарушение американского законодательства



Splits:26-Nov-99 [2:1], 08-Mar-01 [3:2], 07-Jun-02 [4:3]

О чем думает CEO?

- Репутация
- Рекомендация Cisco Systems:

**ИБ влияет на прозрачность и управляемость бизнеса
→ прозрачность и управляемость бизнеса влияет на репутацию и стоимость торговой марки → репутация и стоимость торговой марки влияет на капитализацию компании**

ИБ позволяет предотвратить кражу информации → доверие со стороны клиентов и акционеров не снижается → нет урона репутации

ИБ позволяет предотвратить взломы сайтов → доверие со стороны клиентов и прессы

Пример ChoicePoint

ChoicePoint – Февраль 2005

- Кража отчета с 150,000 именами клиентов, номеров кредитных карт и т.д.

Воздействие на бизнес

После взлома был зафиксирован отток ключевых клиентов, CEO был вызван в Конгресс, пресса ополчилась на компанию



Splits:26-Nov-99 [2:1], 08-Mar-01 [3:2], 07-Jun-02 [4:3]

О чем думает CEO?

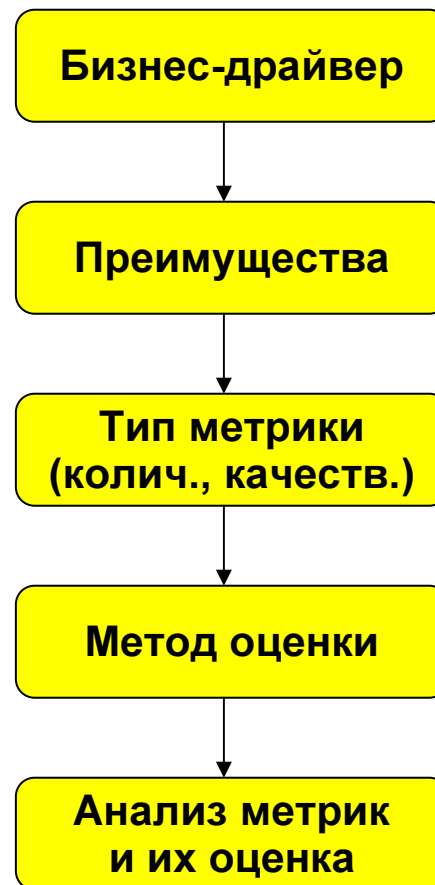
- **ИТ (ИБ) может способствовать росту бизнеса**
- **Рекомендация Cisco Systems:**
 - Покажите, что ИБ – это не технологическая задача, а один из бизнес-процессов
 - Выберите метрики эффективности ИБ и регулярно демонстрируйте их руководству
- **Примеры: все защитные технологии**

О чем думает CEO?

- **ИТ (ИБ) может затормозить изменения**
- **Рекомендация Cisco Systems:**
 - Покажите, что ИБ – это не статья расходов, а инвестиции, которые способствуют целям бизнеса
 - Выберите метрики эффективности ИБ и регулярно демонстрируйте их руководству
- **Примеры: все защитные технологии**

О метриках

- Существует свыше 40 бизнес-драйверов...
- которые несут с собой определенные преимущества для бизнеса...
- которые можно измерить...
- с помощью правильно выбранных методов и метрик



Пример – система регистрации

Старый подход

Решили заменить
пароли на токены

Причина – низкая
защищенность паролей

Выбрали поставщика
токенов

Оценили стоимость
решения

CFO отказал в закупке
из-за высокой
стоимости

Новый подход

Выбрали драйвер –
снижение издержек

Выбрали преимущества –
прозрачность,
поддерживаемость,
экономия, продуктивность

Метрики - количественные

Оценили метрики

Приобрели решение

Исходные данные

- **Число пользователей – 120000**
- **Ежегодная ротация кадров – 15%**
- **Среднее число ID/паролей – 5**
- **Число рабочих часов в день – 8**
- **Число рабочих дней в год - 220**

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**

Вторая фаза расчета – ежедневная работа

- 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 – регистрация в системе**

ЗАКЛЮЧЕНИЕ



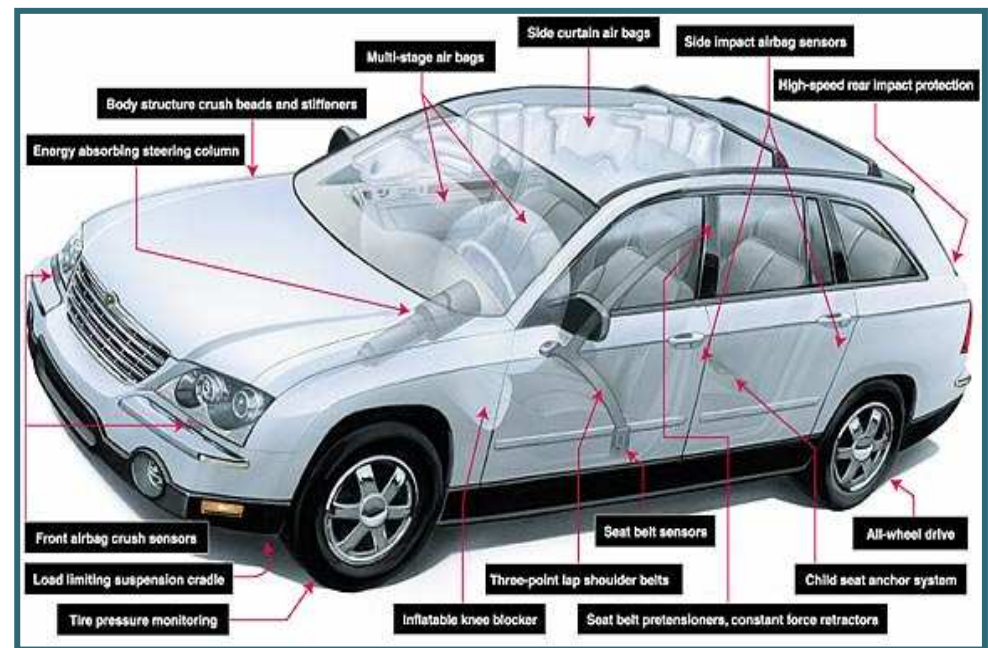
Значение интегрированной безопасности

Безопасность – это не опция!



Безопасность, как опция

- Рост сложности
- Высокая стоимость интеграции
- Медленное внедрение
- Сложность администрирования
- Нет сквозной функциональности
- Отражение не всех угроз
- Низкая надежность



Безопасность, как часть системы

- Снижение сложности
- Тесная интеграция сетевых сервисов и приложений
- Простота внедрения и управления
- Снижение стоимости владения

О чем должны подумать Вы

- **СЕО не обязательно думает обо всех вышеприведенных факторах**
- **Думайте о ИБ, как о бизнес-процессе, а не как о технологической задаче**
- **Не ждите, что СЕО сам спросит вас про безопасность – будьте проактивны – сами предложите ИБ-проекты, увязанные с бизнес-целями**
- **Активно работайте с CFO**

3 заключительных совета

- **Безопасность должна быть одной из движущих сил бизнеса, а не его тормозом**
- **Безопасность должна осуществляться в контексте стратегии развития бизнеса, а не отдельно от нее**
- **Не пытайтесь стать интегратором – пусть производитель/поставщик делает это для вас и за вас**



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

CISCO SYSTEMS

