cso-summit.ru

Russian CSO Summit

CSO Summit 2009

Второй Съезд директоров по информационной безопасности

23-24 марта 2009, Москва

Александр Астахов
GlobalTrust Solutions

О преимуществах системного подхода к управлению рисками

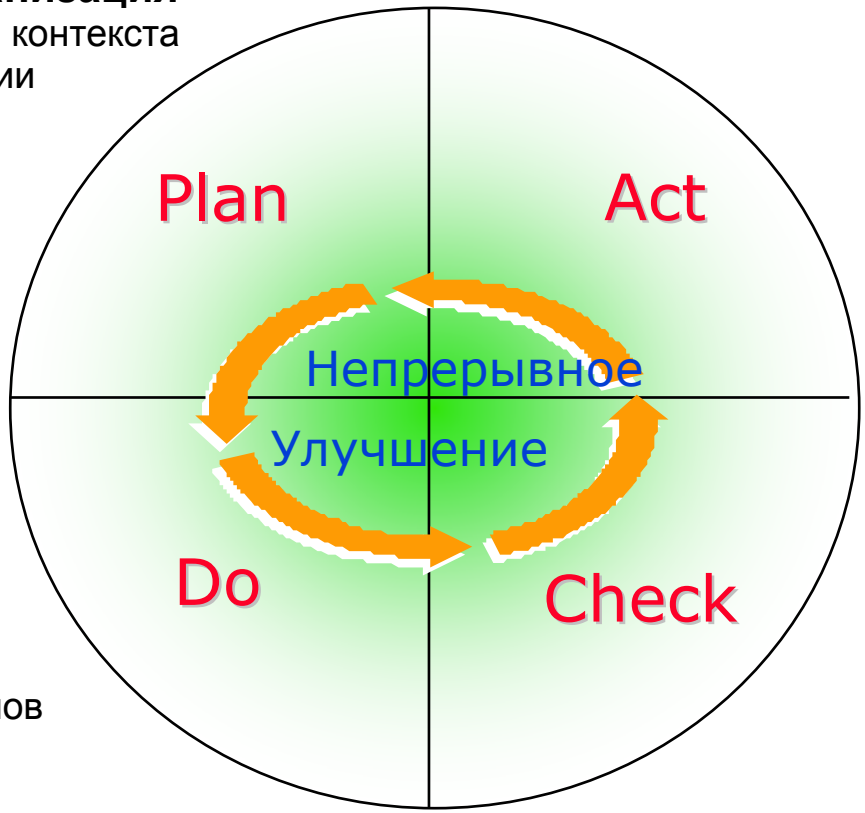
Известные аргументы в пользу усиления функции ИБ, обычно предъявляемые Руководству

- Усиление внутренней угрозы во время кризиса
- Технология «быстрых побед»
- Методы запугивания
- Ужесточение требований законодательства
- Государственная «дубинка»
- Красноречие директора по ИБ
- Магия, гипноз и другие способы воздействия на принятие решений

Все это не всегда срабатывало до кризиса, еще хуже срабатывает во время кризиса

Самоорганизующаяся СУИР не требует уловок для принятия решений по рискам

Планирование и организация
- Определение политики и контекста
- Определение методологии
- Оценка рисков



Поддержка и совершенствование
- Переоценка рисков
- Совершенствование
- методологии
- Пересмотр политик
- Повышение
- осведомленности

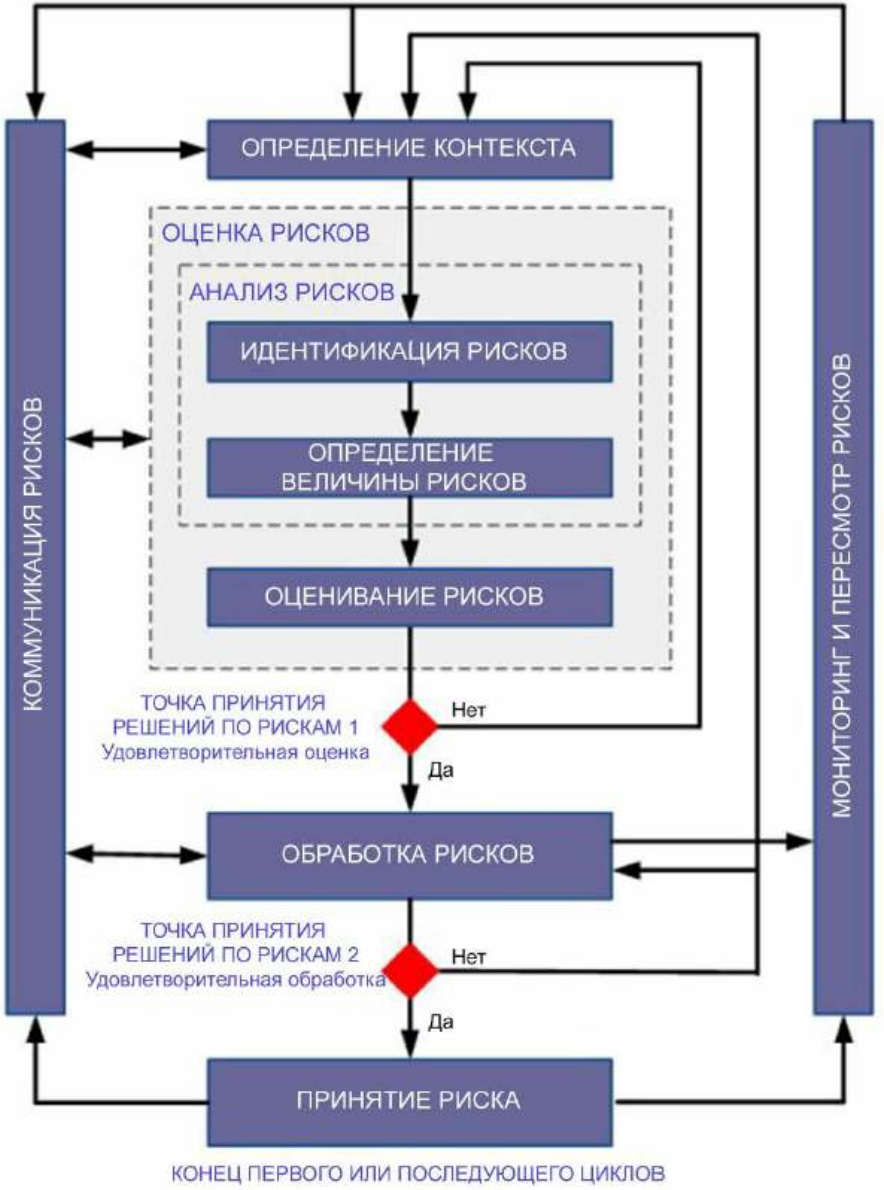
Внедрение и эксплуатация
- Обработка рисков
- Разработка и
- реализация плана
- обработки рисков
- Внедрение механизмов
- контроля

Мониторинг и аудит
- Процедуры мониторинга
- Контроль факторов риска
- Внутренний и внешний аудит

Три необходимые составляющие СУИР

- Формализованные взаимодействующие процессы
- Стандарты, технологии, документооборот
- Организационная структура и кадры

В большинстве организаций отсутствуют все или часть необходимых процессов СУИР



Документация СУИР

- Внешняя: Законодательство и Стандарты
- Внутренний нормативный уровень: Политика и Методология управления рисками
- Внутренний операционный уровень: Реестр и План обработки рисков

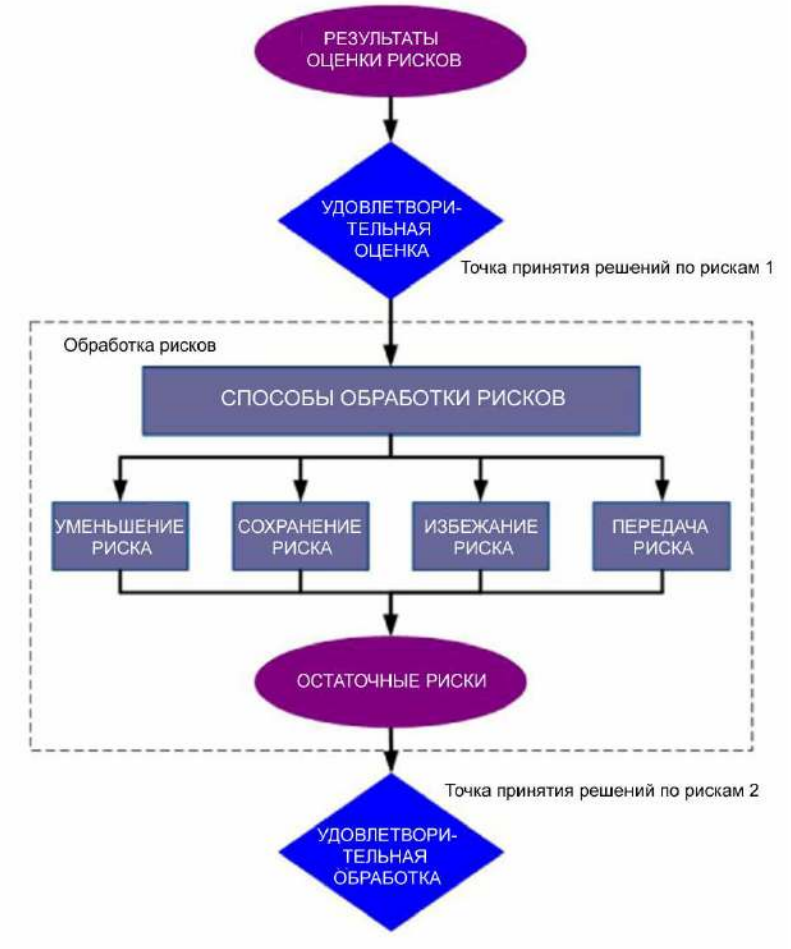
Без грамотно разработанной внутренней документации дальше разговоров дело не пойдет

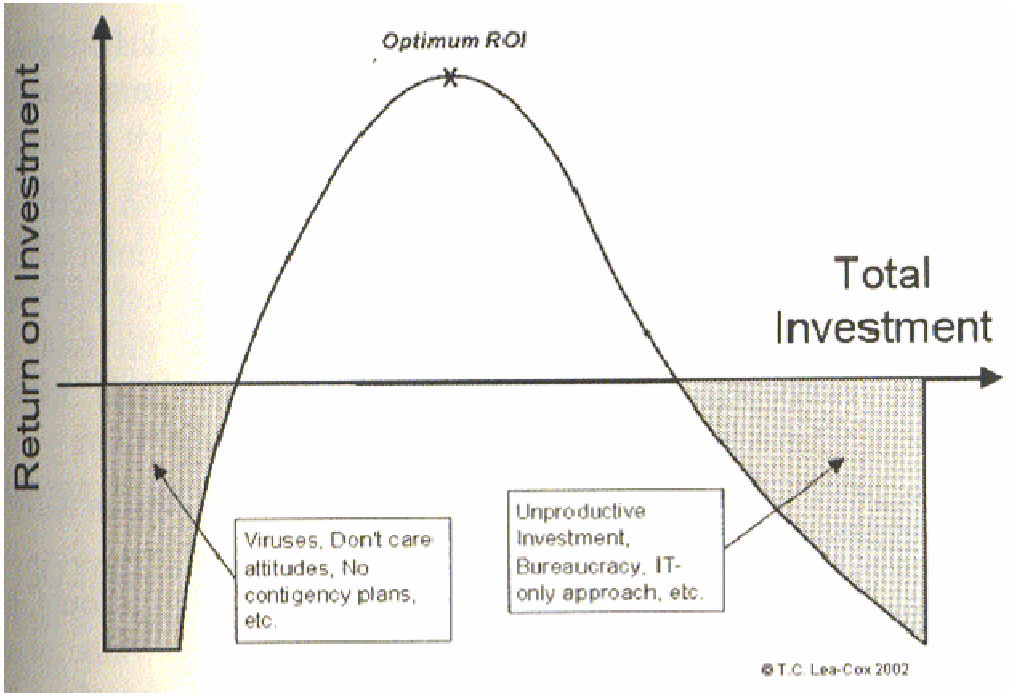
Реестр информационных рисков – основной рабочий документ

Реестр информационных рисков

№	Группы угроз	Уязвимости	Активы	Вероятность угроз	Уровень уязвимости	Ценность актива	Уровень риска	Механизмы контроля
			Риски офисной сети					
			Физические риски					
1	Кража компьютерного оборудования и носителей информации инсайдерами Физический НСД в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов.	Корпоративный веб сайт	М	М	0	2	Средний уровень лояльности сотрудников. Существует политика безопасности в отношении мобильных носителей информации и использования внешних устройств. Существует политика возврата оборудования, носителей информации и документации при увольнении сотрудников. Для доступа на территорию организации используются смарт-карты Территория охраняется службой безопасности Офисное оборудование и документация находятся строго в зонах безопасности.
			Отчеты по мероприятиям			1	3	
			Электронные сообщения			2	4	
			Проектная документация			2	4	
			Договора соглашения			1	3	
			Бухгалтерская база данных			3	5	
			Первичная бухгалтерская документация			3	5	
			Финансовые			3	5	

Максимизация возврата инвестиций в ИБ – основной принцип обработки рисков





План обработки рисков – основа для планирования любых мероприятий и бюджетов

№	Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Комментарии, ресурсы, ответственные
Обработка рисков офисной сети							
Физические риски							
1	Кража компьютерного оборудования и носителей информации инсайдерами Физический НСД в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов.	5	Разработать систему мер, ограничивающих неконтролируемое использование внешних носителей и мобильных устройств вне офиса. Реализовать меры по проверке кредитной истории кандидатов для критичных должностей. Разработать правила работы в зонах безопасности.	4		
2	Кража компьютерного оборудования и носителей	Контроль посетителей на ресепшине не производится.	5	Разработать политику обеспечения физической безопасности, предусматривающую, в том числе,	4		

Russian CSO Summit

CSO Summit 2009

Второй Съезд директоров по информационной безопасности

23-24 марта 2009, Москва

cso-summit.ru

Присоединяйтесь к сообществу менеджеров информационной безопасности!

Консалтинговые услуги в области информационной безопасности

Global Trust Solutions

О преимуществах системного подхода к управлению рисками

Александр Астахов

Генеральный директор

ООО «ГлобалТраст Солюшинс»

Тел.: +7 (495) 651-6617

Факс: +7 (495) 967-7600

ICQ: 195-623-651

Email: AlexAstahov@GlobalTrust.ru