



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



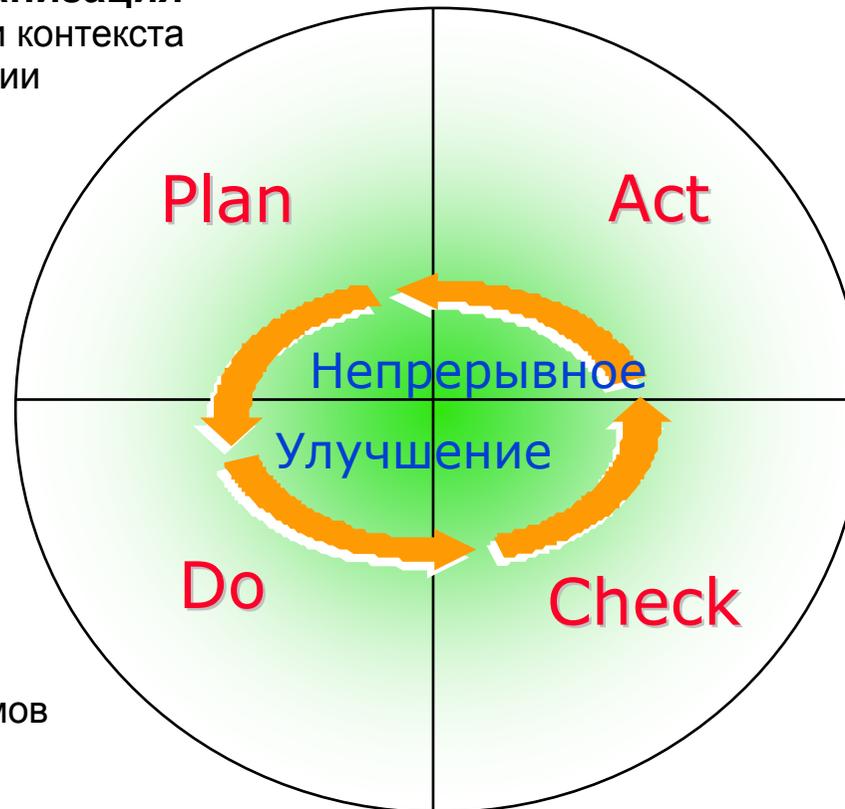
Самоорганизующаяся СУИР не требует уловок для принятия решений по рискам

Планирование и организация

- Определение политики и контекста
- Определение методологии
- Оценка рисков

Внедрение и эксплуатация

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



Поддержка и совершенствование

- Переоценка рисков
- Совершенствование методологии
- Пересмотр политик
- Повышение осведомленности

Мониторинг и аудит

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

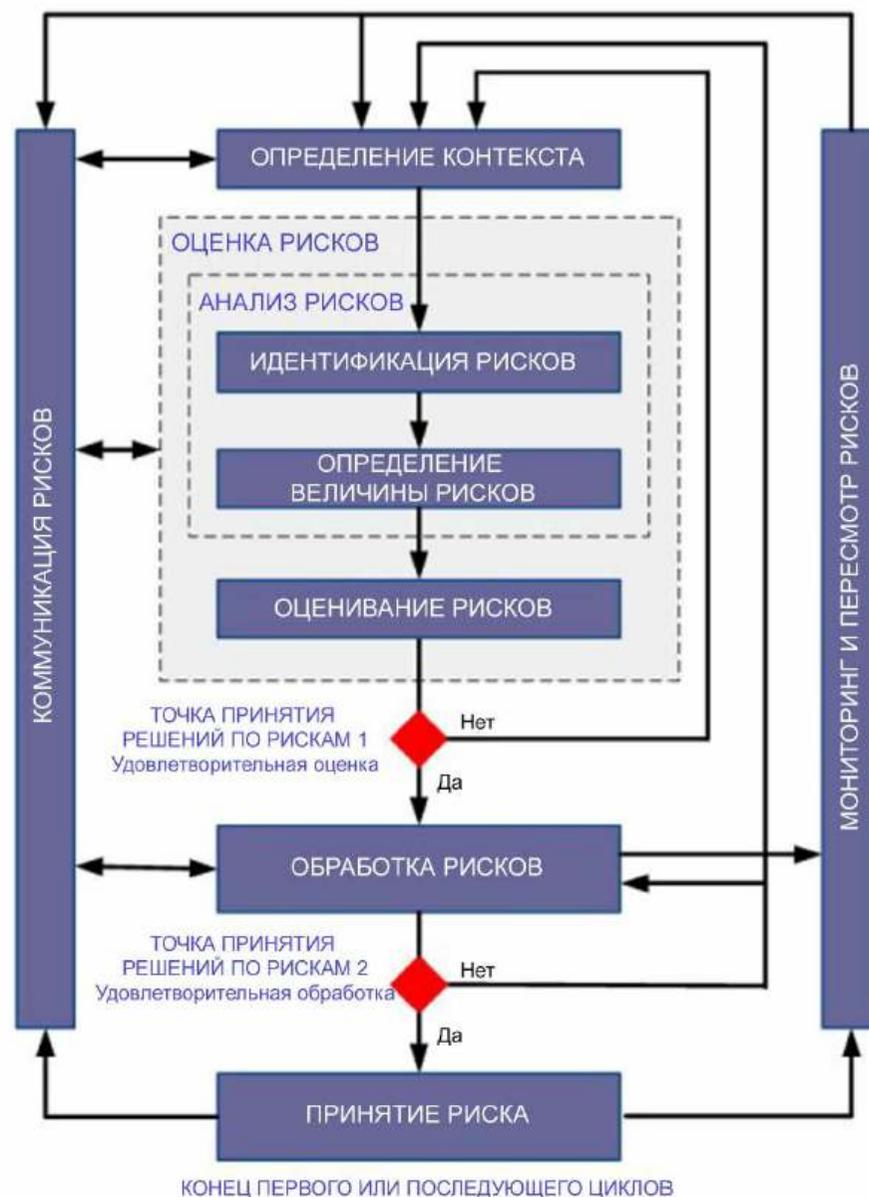


Три необходимые составляющие СУИР

- 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



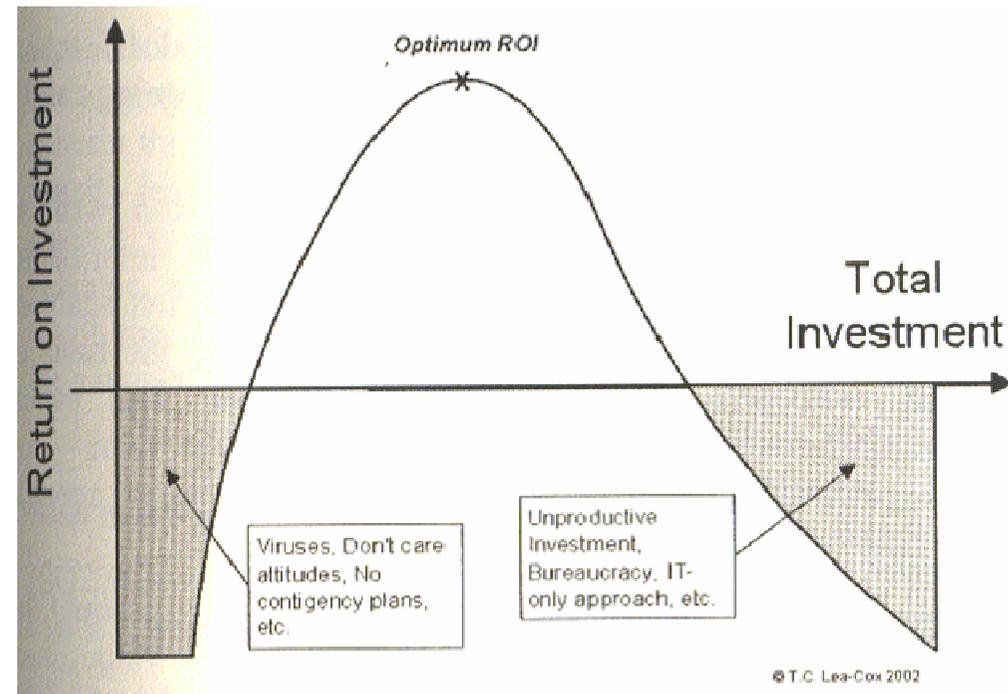
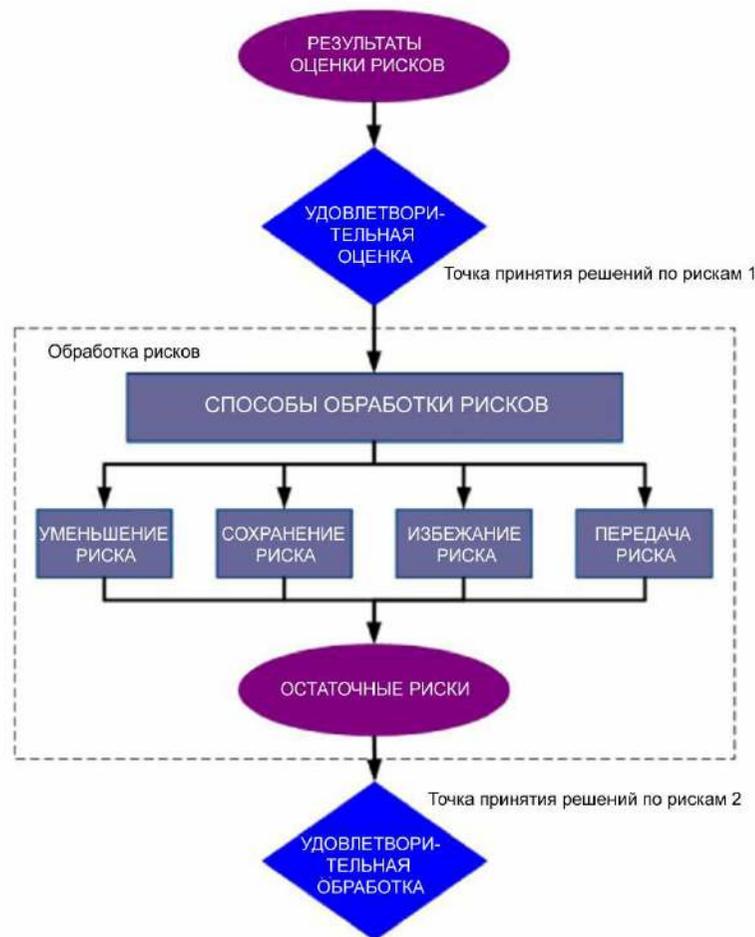
Реестр информационных рисков – основной рабочий документ

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 <u>инсайдерами</u> Физический НСД в помещениях 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 <u>веб сайт</u> Отчеты по мероприятиям Электронные сообщения Проектная документация Договора соглашения Бухгалтерская база данных Первичная бухгалтерская документация Финансовые		M	M	0 1 2 2 1 3 3 3	2 3 4 4 3 5 5 5	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 <u>smart-карты</u> Территория охраняется службой безопасности Офисное оборудование и документация находятся строго в зонах безопасности.



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 <u>инсайдерами</u> Физический НСД в помещении 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

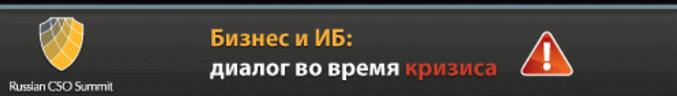
CSO Summit 2009

Второй Съезд директоров по информационной безопасности
23-24 марта 2009, Москва

cs0-summit.ru

Присоединяйтесь к сообществу менеджеров информационной безопасности!





Бизнес и ИБ:
диалог во время кризиса

Главная | Контакты | Карта

Найти

Вы здесь: [Главная](#) Александр Астахов | Моя папка | Мои настройки | Отменить Banner Administration | Выход

- ▣ О ПРОЕКТЕ
- ▣ ЧИТАЛЬНЫЙ ЗАЛ
- ▣ ИНФОРМАЦИОННЫЕ РУБРИКИ
- ▣ ЗАКОНОДАТЕЛЬСТВО
- ▣ СТАНДАРТЫ
- ▣ КАТАЛОГ РЕСУРСОВ
- ▣ КОМПАНИИ
- ▣ СОФТ
- ▣ БЛОГИ
- ▣ ГОЛОСОВАНИЯ
- ▣ ФОРУМ



Портрет нашей аудитории
 Какую позицию вы занимаете?

- 5.30%
Руководитель/владелец компании
- 3.03%

Образованная посредственность все равно остается посредственностью.
Другими словами, если консультанты по ведению бизнеса не имеют своего, зачем они нужны.

«Менеджер мафии»

Сообщество менеджеров информационной безопасности

Приглашаем инвесторов, спонсоров, участников, авторов, рекламодателей, экспертов, разработчиков, поставщиков, потребителей и всех заинтересованных лиц принять участие в формировании самого популярного и авторитетного русскоязычного ресурса в вопросах управления информационной безопасностью.

В фокусе
Предстоящие обновления семейства стандартов ISO/IEC 27000 в 2009 году

Специалист в области ИТ-управления Гэри Хинсон (Gary Hinson) рассказывает про предстоящее обновление влиятельного семейства стандартов ISO/IEC 27000.

Семь основных тенденций информационной безопасности в 2009 году

Рич Могулл (Rich Mogull), бывший аналитик Gartner и основатель компании Securosis, специализирующейся на консалтинге в области безопасности, выделяет семь основных тенденций в наступающем году.

Новости

13-03-2009 - В настоящее время существуют программные продукты поддержки жизненного цикла СУИБ, реализующие не только управление рисками, но и другие жизненно важные процессы. Примером подобного продукта может служить система Proteus, разрабатываемая британской компанией InfoGov.

Предстоящие события

- 
Мастер-класс Александра Астахова "Управлять рисками информационной безопасности теперь не сложно!"
 г. Москва, Краснопресненская набережная, д. 18, блок С, бизнес-центр «Регус», 19-03-2009
- 
Russian CSO Summit II
 Москва, ул. Лесная, д. 15, Holiday Inn Lesnaya, 23-03-2009
- 
Конференция «РусКрипто'2009»
 Подмосковный пансионат «Липки», 02-04-2009
- 
Конференция "Security Director 2.0"
 Москва, Президент-Отель, 16-04-2009

Ближайшие события

Новости

- 
Управление рисками, соответствием, непрерывностью

Март 2009

Вс	Пн	Вт	Ср	Чт	Пт	Сб
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				



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

Email: info@GlobalTrust.ru Web: www.GlobalTrust.ru Магазин: www.GTrust.ru