Риски информационной безопасности при передаче систем на аутсорсинг

Докладчик:
Мелехин Иван
Начальник отдела консалтинга

Информзащита
Системный интегратор

Аутсорсинг –

Передача организацией на основании договора определенных бизнес-процессов или производных функций на обслуживание другой компании, специализирующейся в соответствующей области.

ИТ аутсорсинг (ITO) –

Передача части (всех) **функций** по поддержке и обслуживанию собственных информационных систем **сторонней компании**, специализирующейся в этой сфере.

Модели аутсорсинга

Аутсорсинг ИТ инфраструктуры
Поддержка пользователей (Help desk)
Управление вспомогательными активами
Поддержка непрерывности бизнеса (Резервирование,
Управление сетями
Управление безопасностью
Аутсорсинг приложений
Поддержка приложений
Хостинг приложений

Выбранная модель и состав передаваемых функций определяют возникающие риски информационно безопасности

Информзащита
Системный интегратор

Определение контекста

Какие системы передать на аутсорсинг?

Какая информация содержится в системе и какова её ценность?

Какие требования по безопасности предъявляются?

Какие ИТ функции передать, а какие оставить?

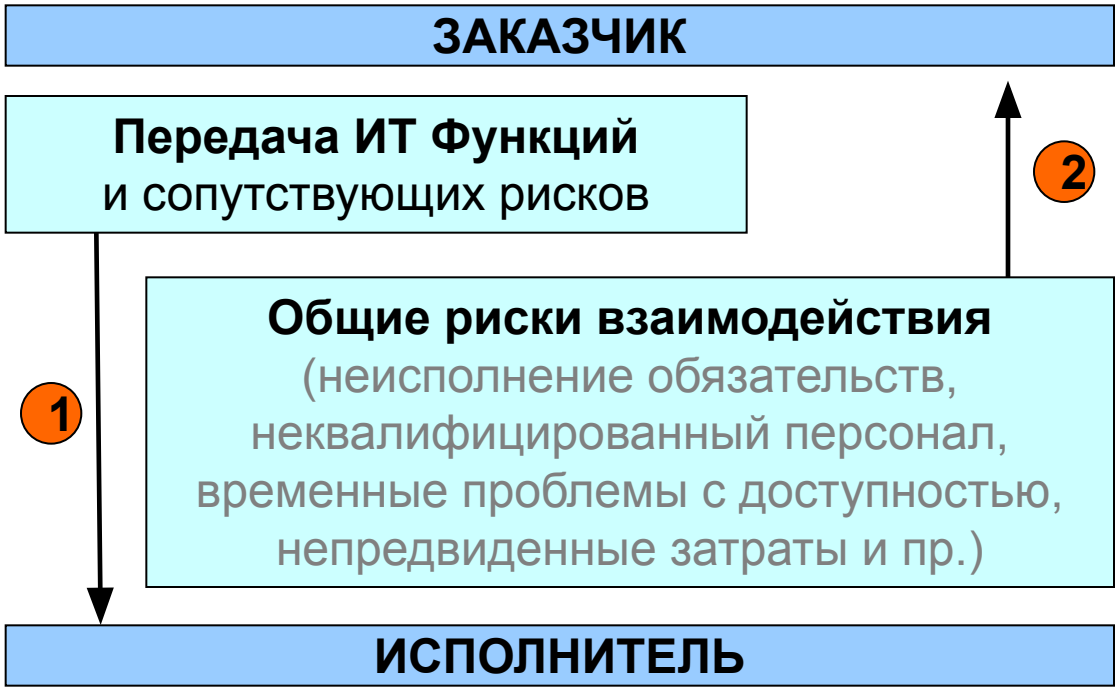
Кому? На каких условиях?

Какие риски принять, а какие обработать?

Новые условия окружения

- Резко сужается круг доверенных лиц
- Более активное использование внешних каналов связи
- Неизвестная исходная защищенность инфраструктуры провайдера
- Неизвестный круг третьих лиц, получающих доступ к инфраструктуре и системе, включая физический уровень
- Отсутствие контроля над регламентами и их исполнением на стороне провайдера
- Отсутствие оперативной обратной связи и информирования по инцидентам ИБ на стороне провайдера

Источники (факторы) риска



1. **Готова ли Компания-Аутсорсер** обеспечить обработку взятых на себя рисков? Имеет ли она необходимые меры контроля, снижающие риски до приемлемого уровня?
2. **Готов ли менеджмент Компании-Заказчика** к обработке рисков взаимодействия?

Информзащита
Системный интегратор

Новые риски

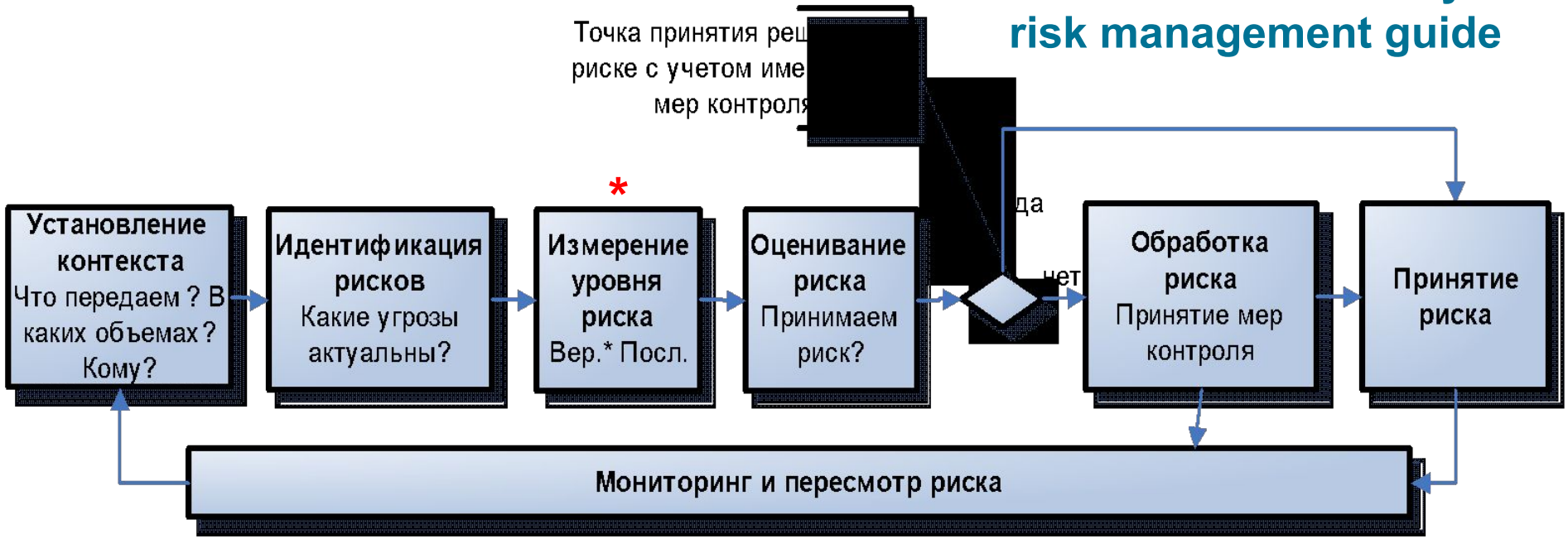
Аутсорсинг ИТ инфраструктуры	
Поддержка пользователей (Help desk)	- доступ к конфиденциальной информации на рабочих станциях пользователей
Управление вспомогательными активами	- воздействие на вспомогательные активы - нарушение качества сервиса;
Поддержка непрерывности бизнеса	- риски природного и техногенного характера
Управление сетями	- несанкционированное сетевое взаимодействие
Управление безопасностью	- данные об инцидентах ИБ под контролем Исполнителя
Аутсорсинг приложений	
Поддержка приложений	- доступ к конфиденциальной информации, содержащейся в бизнес-приложениях
Хостинг приложений	- нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры

От выбранной модели и полноты передаваемых функций зависит итоговый перечень актуальных угроз и рисков ИБ, которые следует проанализировать!

Общий подход к менеджменту рисков

- ISO 27005

- Microsoft © Security risk management guide



* Качественный, количественный или комбинированный подход

Информзащита
Системный интегратор

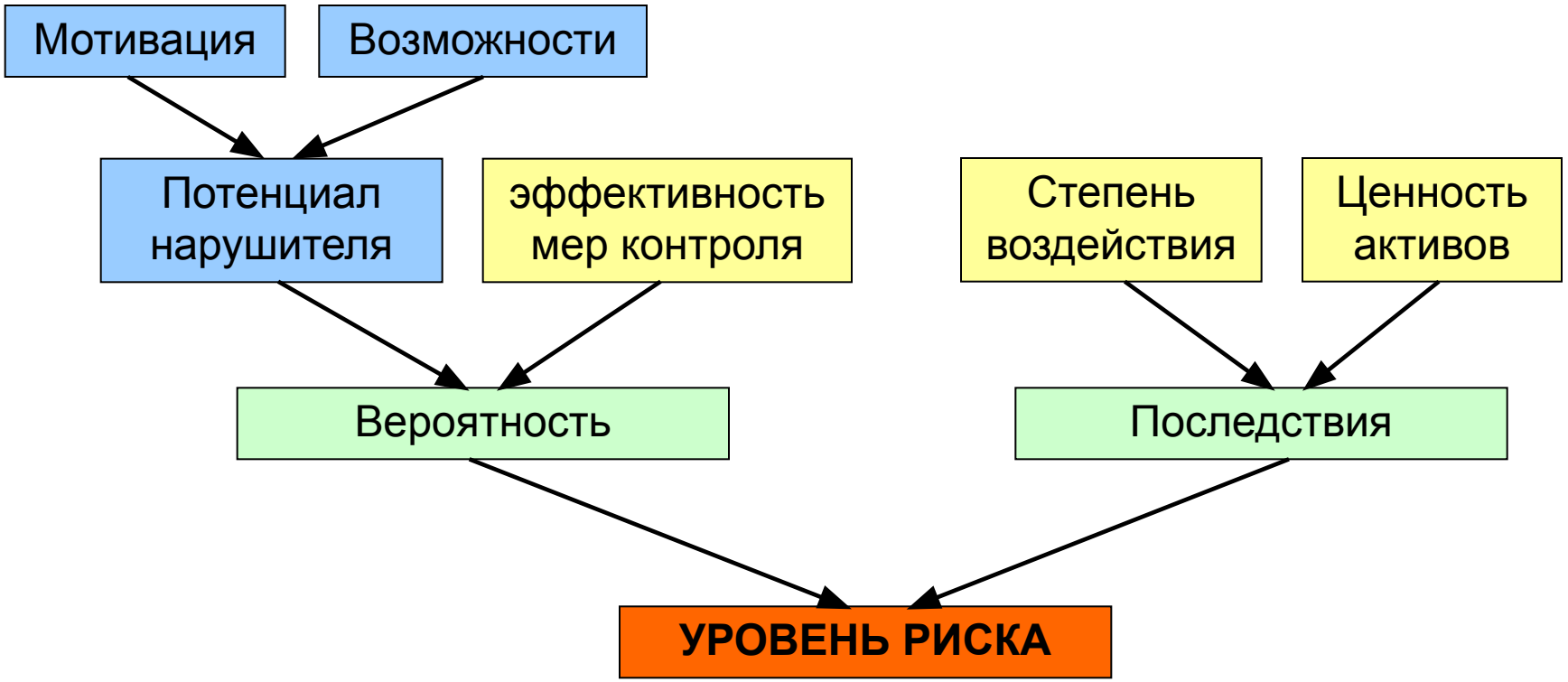
Применение менеджмента рисков к передаче систем на аутсорс

- Выделить области изменений в системе в связи с передачей на аутсорс
- Оценить в выделенных областях текущие риски в с учетом существующих контролей
- Оценить в выделенных областях будущие риски с учетом известных контролей аутсорсера
- Принять решение об управлении рисками
- Оценить стоимость контракта с учетом требований к аутсорсеру по реализации контролей
- Принять решение о передаче на аутсорс
- Принять решение о модификации аутсорсингового контракта

Основные этапы управления рисками

- Идентификация активов
- Оценка активов
- Идентификация угроз и уязвимостей
- Идентификация имеющихся контролей
- Оценка рисков

Факторы влияющие на уровень риска



Результаты работ

- Перечень новых рисков, возникающих в связи с передаче систем на аутсорсинг
- Для рисков выше приемлемого уровня – рекомендуемые контроли по снижению рисков
- Рекомендации по составу требований к аутсорсеру по реализации контролей

Ключевые моменты работ

- Согласование шкал и критериев оценки активов и последствий
- Увязка с существующими в организациями подходами к оценке и управлению рисками
- Определение уровня приемлемого риска
- Получение объективной информации о наличии контролей у аутсорсера

Пример оценки

Информзащита
Системный интегратор

Пример контролей по снижению риска

Риски	Угрозы	Категория нарушителя	Объект воздействия	Уязвимости	Контроли
Нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры (доступ через сеть Интернет).	2.2.1. Превышение допустимых показателей качества сервиса;	$Куп_1$	Сервис	1) Отсутствие резервных каналов доступа в сеть Интернет; 2) Не достаточно проработаны требования по уровню сервиса (SLA).	**Исполнитель:** 1) Поддерживать свою сетевую инфораструктуру для обеспечения соответствия необходимому уровню качества сервиса в показателях времени отклика и пропускной способности; **Компания:** 1) Предусмотреть резервные каналы доступа в сеть Интернет; 2) Оценить необходимые уровни качества сервиса и заложить их в SLA (с учетом прогнозируемого роста нагрузки и т.д.)

Пример шкалы оценки активов по свойству конфиденциальности

Значение шкалы	Классификация информации
1	Общедоступная информация в т.ч. общедоступные персональные данные
2	Служебная информация, не относящаяся к конфиденциальной
3	Конфиденциальная информация, не относящаяся к персональным данным и коммерческой тайне
4	Персональные данные*
5	Коммерческая тайна

Возможные трудности

- Нечеткая классификация информации на стороне клиента
- Плохо формализованные требования на стороне клиента
- Невозможность сформулировать стоимость информации на стороне клиента
- Отсутствие сведений о контролях на стороне аутсорсера

«Хороший» провайдер

- Готов фиксировать в договорных обязательствах свою ответственность за нарушение режима КТ и инциденты ИБ
- Готов идти на регулярный внешний аудит ИБ по требованиям Заказчика
- Имеет сертифицированную систему управления ИБ с «правильной» областью деятельности
- Готов предоставлять журналы регистраций событий ИБ по первому требованию
- Готов строить интегрированную систему управления инцидентами ИБ и мониторинга состояния защищенности информации Заказчика

Спасибо за внимание!

Информзащита
Системный интегратор

Информзащита
Системный интегратор