Управление информационными рисками компании

Сергей Колосков, CISA
Старший консультант отдела по предоставлению услуг в области информационных технологий и ИТ-рисков

6 Ноября 2008

ERNST & YOUNG
Quality In Everything We Do

Результаты ежегодного исследования Ernst&Young в области ИБ 2008

Вопрос: Проводит ли Ваша организация анализ рисков для определения приоритетных мероприятий в области ИБ?

Что такое риск?

- В своей работе компании сталкиваются со множеством различных рисков.
  - **Словарь Webster:** risk \'risk\, сущ. 1) Возможность потери или ущерба; 2) опасность, вызванная определенными причинами или исходящая из конкретного источника
  - **E&Y:** “Риск в сфере бизнеса – это угроза того, что какое-либо событие или действие может негативно повлиять на способность компании к достижению целей ее деятельности.”
  - **Стандарты ISO/IEC**: сочетание вероятности события и его последствий

- Все виды рисков подлежат оценке с целью определения приемлемости данного риска для компании, или необходимости внедрения дополнительных механизмов контроля для его минимизации.

В чем заключается управление рисками?

- Управление рисками представляет собой последовательность согласованных действий по руководству компанией и контролю ее деятельности в ситуации, вызванной наличием **риска**.
- Управление рисками подразумевает систематическое выявление и оценку рисков, принятие необходимых мер и доведение информации о рисках до всех сотрудников компании.
- Управление рисками **НЕ** подразумевает их систематического устранения!
  - Риск нельзя свести к абсолютному минимуму
    - Невозможно выявить все источники рисков
    - Уменьшение некоторых рисков требует чрезмерных затрат
    - Принятие некоторых рисков позволяет увеличить доходность
  - Установление предельного значения риска позволяет определить, до какой степени данный риск следует минимизировать, а до какой – принять

Характер информационных рисков

Возникновение рисков в области ИТ обусловлено следующими существенными причинами:

- Интенсивное использование информационных технологий практически во всех сферах деловой активности современных организаций
- Сложность и разнообразие технических средств и решений, применяемых организациями в своей работе
- Территориальная распределённость сотрудников и информационных систем организаций

Компоненты риска

- **Угроза** – т.е. потенциальная причина нежелательного инцидента, который может привести к нанесению вреда системе или организации (например, мошенничество, кража, вирус, саботаж)
- **Уязвимость** – т.е. слабое звено актива или группы активов, которое может использоваться фактором угрозы (например, компьютерные системы уязвимы для вирусов);
- **Влияние** – прямое (например, финансовый убыток) или косвенное (например, ущерб репутации)

ИТ-процессы и ИТ-риски

ИТ-процесс	ИТ-риск
Обеспечение безопасности систем	Неавторизованный доступ
Управление внесением изменений	Внесение несанкционированных изменений
Обеспечение непрерывности услуг	Недоступность или потеря данных
Согласование с внешними требованиями	Судебный иск в результате нарушения интеллектуальных прав собственности
Приобретение и поддержка прикладного ПО	Несоответствие внедренного функционала потребностям конечных пользователей
Управление производительностью и производственными мощностями	Производительность ИТ систем не соответствует согласованным уровням обслуживания

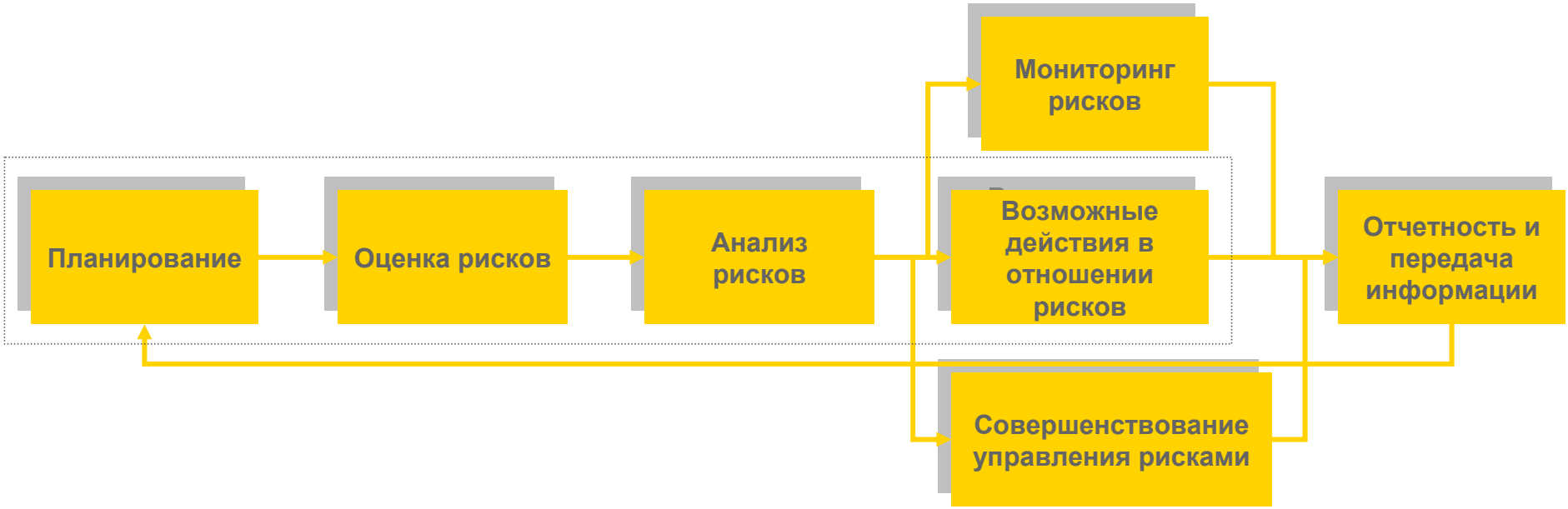
Связь ИТ-рисков с другими рисками

Интеграция управления рисками

Создание устойчивой программы управления рисками в области ИТ/ИБ требует интеграции управления рисками в общую систему управления ИТ/ИБ.

Процесс управления рисками

Управление рисками это процесс, позволяющий сбалансировать операционные и экономические затраты на защитные меры, наращивать возможности по выполнению задач путем защиты информационных систем и данных, поддерживающих деятельность компании.



Действия в отношении рисков: Принятие

- Необходимо помнить о разумном балансе между возможностями и риском
- Организации все время принимают на себя бизнес-риски – успешные организации научились различать разумные риски от неразумных
- Ключевым моментом при принятии риска является вопрос обеспечения этого принятия соответствующими людьми, имеющими надлежащие навыки и полномочия, на основе надлежащей информации
- Работа руководителей ИБ заключается в том, чтобы разъяснить суть риска и рекомендовать последовательность действий

Действия в отношении рисков: Передача

- Обычно передача рисков осуществляется с применением методов страхования или риски передаются сторонним лицам
- Передача рисков требует тщательного взвешивания всех "за" и "против", но в некоторых случаях эта идея может быть привлекательной (в отношении рисков мошенничества, кражи, утраты имущества и т.п.)
- К сожалению, для того, чтобы передать или застраховать риск, необходимо его измерить, а это подчас трудно

Действия в отношении рисков: Минимизация

- В сфере информационной безопасности мы, как правило, предпочитаем рисками управлять ☺
- Управляя риском, мы совершаем действия, направленные на снижение риска до приемлемого уровня за счет:
  - информирования и обучения персонала в отношении рисков и способов обращения с ними;
  - процедур и инструментов, используемых для снижения риска;
  - заключения договоров, распределяющих обязанности и определяющих ответственность сторон.

Остаточный риск

- Не важно, каким способом и с помощью чего мы работаем с каким-то конкретным риском, всегда остается остаточный риск, т.е. риск, оставшийся после того, как были применены все снижающие его средства контроля
- При этом совершенно не обязательно, что это будет наиболее низкий уровень риска, однако он должен представлять идеальное равновесие между возможностью и риском
- Остаточный риск должен быть санкционирован соответствующим руководителем подразделения компании

Управление новыми сценариями развития рисков

- Новые возможности в сфере бизнеса часто означают встречу с новыми рисками, в отношении которых действующие средства контроля не работают.
- Для того, чтобы отреагировать в рамках отведенного времени, диктуемого возникшей возможностью, нам необходимо уметь быстро анализировать **наиболее значительные риски** и определять действия, подходящие с точки зрения их снижения.
- Техника "простой оценки рисков" применяется в целях выработки тактических решений, позволяющих компании воспользоваться представившейся возможностью в пределах отведенного времени.

Пример техники оценки рисков

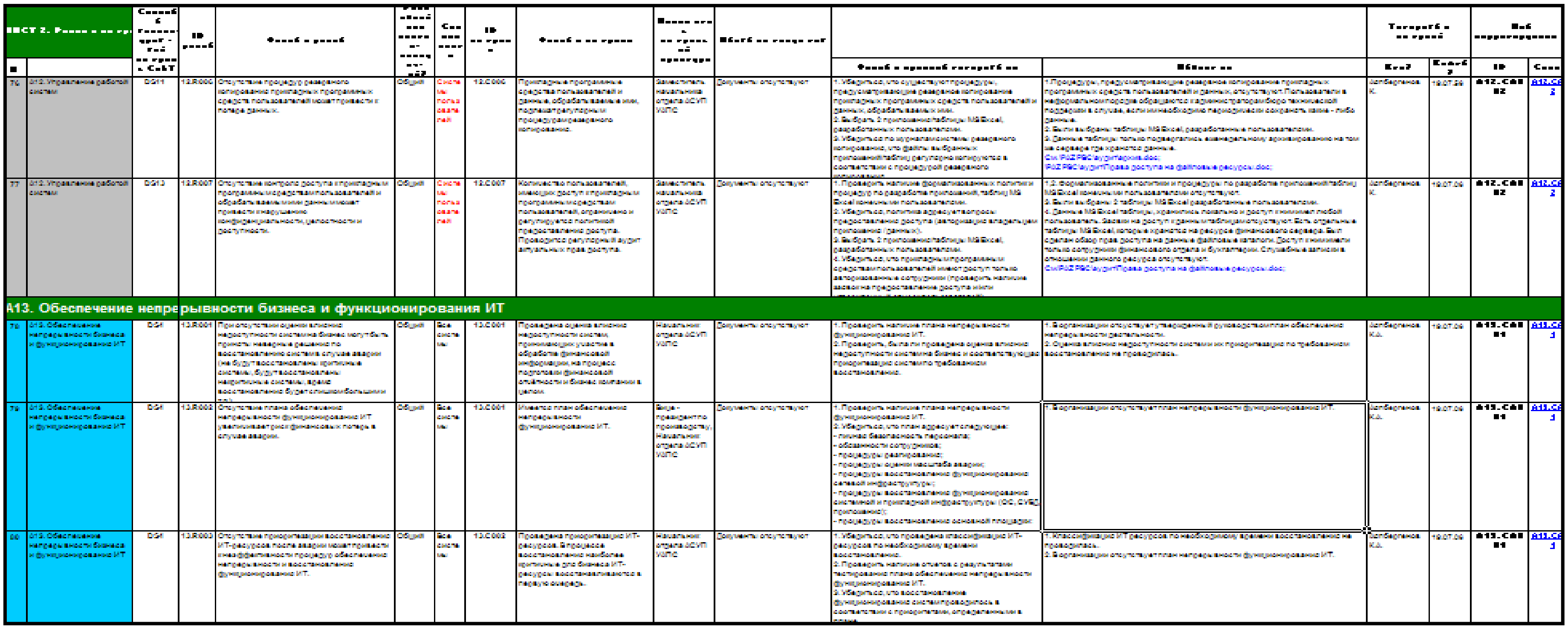
- Определение **ключевых** активов
- Определение сценариев развития угрозы – высокая, средняя или низкая вероятность;
- Определение уязвимостей;
- Описание **наиболее значительных рисков** – общие или конкретные;
- Описание **средств контроля, снижающих риски**, а также **остаточного риска**;
- Описание предлагаемых действий.

Пример: Виды информационных активов

Пример: Категория сотрудники. Виды

Пример: Категория сотрудники. Угрозы

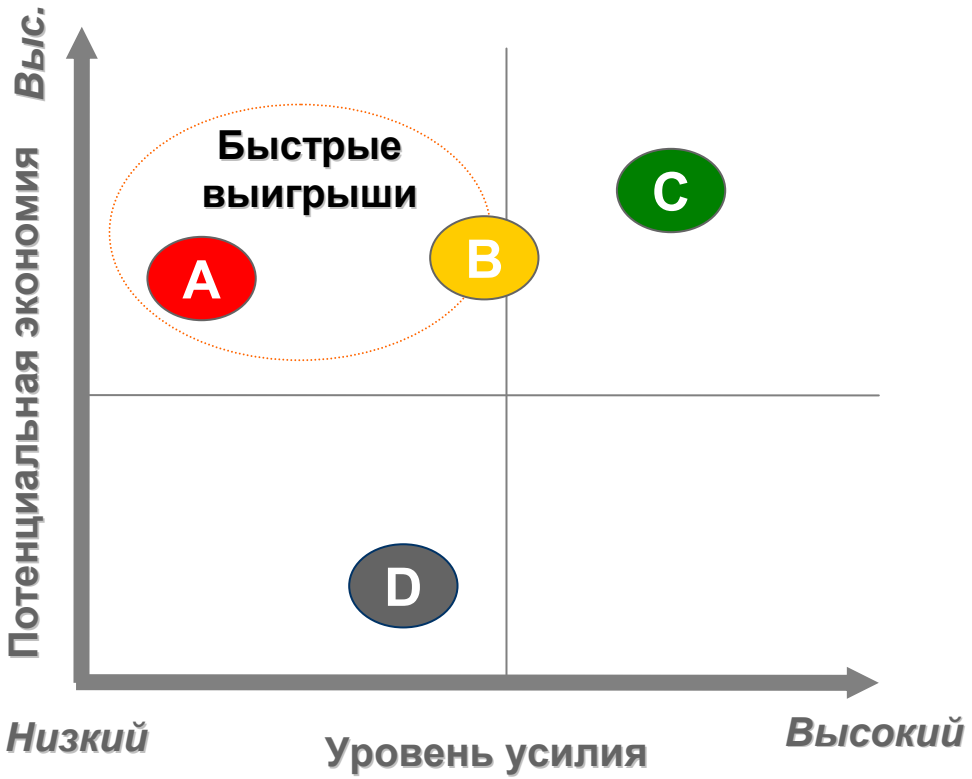
Пример: Матрица рисков и контролей


A13. Обеспечение непрерывности бизнеса и функционирования ИТ

Пример: План корректирующих мер

ЛИСТ 3. План корректирующих мер							
ID	Описание	Ответственный	Требуемые усилия (малые / средние / большие)	Приблизительная стоимость	Приблизительные трудозатраты (часы)	Критичность (низкая/ средняя/ высокая)	Приоритет
A08.CA007	**Разработка руководства по конфигурированию и администрированию межсетевых экранов** Разработать руководство по конфигурированию каждого межсетевого экрана, используемого в Компании. В руководстве должны быть описаны: - правила и настройки межсетевых экранов; - настройки по регистрации системных событий; - определение срока хранения журналов событий (как минимум 1 год); - ссылки на процедуры резервного копирования; - ссылки на соответствующий регламент по внесению изменений и процедуру авторизации изменений.	Руководство ИБ	средние		24	средняя	5
A08.CA008	**Разработка процедуры анализа защищенности сетевых ресурсов** Формализовать и внедрить процедуру анализа защищенности сетевых ресурсов. Необходимо определить: - периодичность проведения тестирования для ресуроов различной степени критичности; - используемое программное обеспечение; - процедуру согласования тестов с владельцами ресурсов; - формат отчета; Также процедура должна определять и проведение независимого анализа защищенности (сторонними организациями).	Руководство ИБ	средние		24	средняя	5
A08.CA009	**Разработка процедуры мониторинга событий информационной безопасности** Формализовать и внедрить процедуру мониторинга событий информационной безопасности в информационных системах Компании. Мониторинг событий информационной безопасности должен осуществляться сотрудниками отдела информационной безопасности. Процедура должна предусматривать коммуникацию событий информационной безопасности руководству Компании.	Руководство ИБ	средние		24	высокая	2
A08.CA010	**Разработка процедуры анализа защищенности сетевых ресурсов** Формализовать и внедрить процедуру анализа защищенности сетевых ресурсов. Необходимо определить: - периодичность проведения тестирования для ресуроов различной степени критичности; - используемое программное обеспечение; - процедуру согласования тестов с владельцами ресурсов; - формат отчета; Также процедура должна определять и проведение независимого анализа защищенности (сторонними организациями).	Руководство ИБ	средние		24	средняя	5
A08.CA011	**Процедура управления доступом в серверные помещения** Формализовать и внедрить процедуру управления доступом в серверные помещения Компании. Процедура должна предусматривать: - наличие заявок на предоставление доступа в серверные помещения, которая согласуется с руководителем УИТ и начальником Отдела информационной безопасности	Руководство ИБ	средние		24	высокая	2

Корректирующие действия: расстановка приоритетов



Техники оценки рисков: за и против

- Глобальные методы оценки рисков:
  - Ставят целью предоставить глобальный взгляд на риски по всей организации;
  - Как правило, требуют много времени;
  - Как правило, производится путем проведения опросов согласно установленным анкетам.
- Простые методы оценки рисков:
  - Применяется в специфических областях или направлениях деятельности;
  - Требует большого опыта и знаний;
  - Использует простые, но эффективные методы.

Ключевые факторы успеха

- Наличие концепции управления ИТ-рисками
- Формирование единого глоссария терминов в области управления ИТ-рисками
- Идентификация и классификация систем и данных
- Оценка вероятности и последствий – измеряем то, что реально и значимо (товар, прибыль, объем продаж)
- Установление единого «языка» общения между ИТ и бизнесом в области управления рисками
- Создание плана мероприятий по минимизации ИТ-рисков

Полезный эффект

- Организация обретает единую методологию управления ИТ рисками, сформулированную в виде полноценной концепции с учетом специфики ИТ-процессов, которая сможет быть интегрирована в общий корпоративный подход в области управления рисками
- Признание ИТ/ИБ в качестве важного компонента управления корпоративными рисками организации в целом
- Классификация систем и данных, проведение оценки, минимизации ИТ-рисков и постановки функции постоянного мониторинга и переоценки ИТ-рисков

Спасибо за внимание

Сергей Колосков, CISA

Старший консультант отдела по предоставлению услуг в области информационных технологий и ИТ-рисков

Sergey.Koloskov@ru.ey.com

+7 (495) 755-9700

Ernst & Young

Quality In Everything We Do