



**Кейс-стади:
управление рисками в
мире цифровых
зависимостей**

Александра Савельева, ГУ-ВШЭ



Краткое содержание кейса

- ❖ Сотрудник американского банка по запросу клиента отправляет его представителю отчёты по займу посредством электронной почты, но ошибается в адресе получателя.
- ❖ Кроме того, к письму он прикладывает файл с данными других клиентов, который ни под каким предлогом не должен был покидать пределы организации.
- ❖ Когда сотрудник обнаруживает свою ошибку, исправить ее уже поздно: имейл отправлен.
- ❖ На требование удалить письмо без прочтения и связаться с банком владелец злополучного имейла не отвечает.
- ❖ Представители почтовой службы встают на его защиту и отказываются выдать его личность без решения суда.
- ❖ Подача судебного иска приводит к тому, чего опасался банк - происходит огласка факта утечки данных о клиентах.



Цель занятия

- Разобрать поведение компании и оценить правильность каждого из шагов
- Идентифицировать риски с использованием модели «условие-последствие»
- Предложить варианты того, как должна была действовать компания
- Разработать стратегию поведения, которые позволили бы вернуть компании репутацию и удержать существующих/не отпугнуть новых клиентов
- Обосновать меры с точки зрения формальных подходов к оптимизации планирования работы с рисками
- Проанализировать возможные пути развития ситуации, если бы она произошла в России (в т.ч. в свете требований ФЗ "О персональных данных")



- ❖ Что такое управление рисками?
 - “Систематизированный процесс идентификации и анализа рисков, а также определения стратегий реагирования”

- ❖ Что такое **риск**?
 - “Риск – это некоторое событие или условие, которое в случае возникновения имеет позитивное или негативное воздействие по меньшей мере на одну из целей организации.”



Качественный анализ рисков

- ❖ Фокусирует внимание на областях, подверженных значительному риску
- ❖ Оценивает вероятность и воздействие для каждого риска
- ❖ **Точность данных:**
 - выражение уровня понимания риска



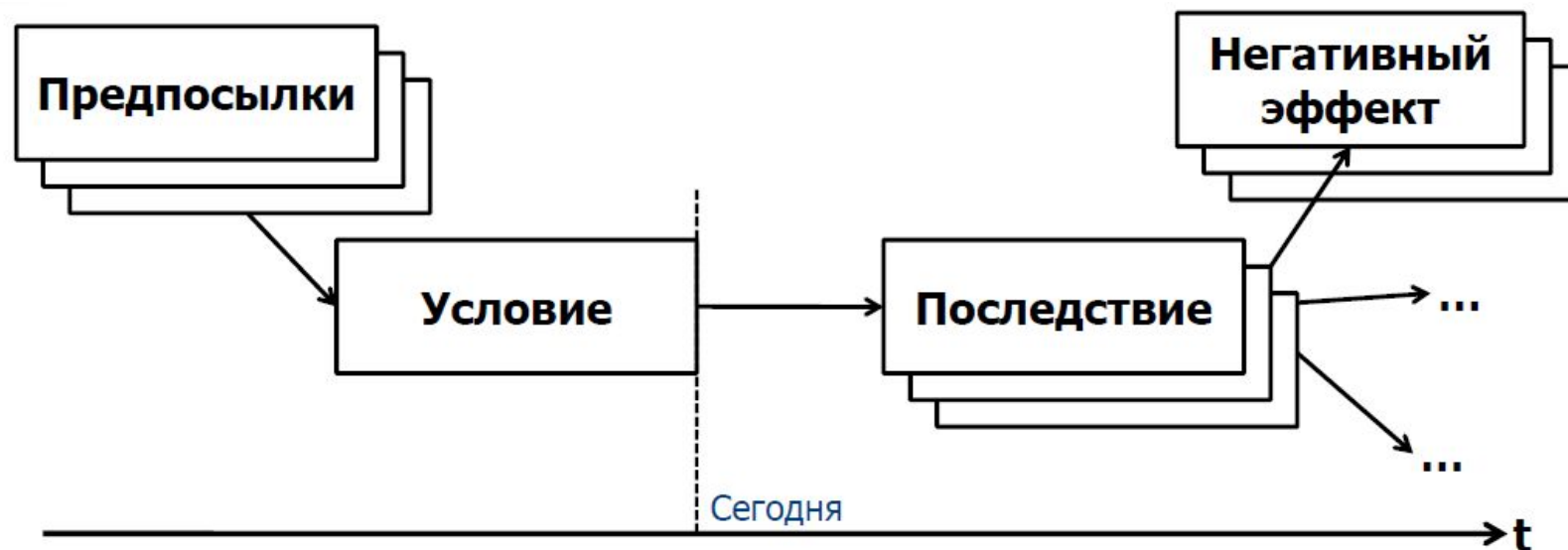
Управление
рисками

Основные риски

Идеи? 😊



Модель «условие-последствие»



Источник: Дмитрий Башакин, курс РМ-021 «Управление рисками», © УЦ Luxoft, 2009

3 кита информационной безопасности

1

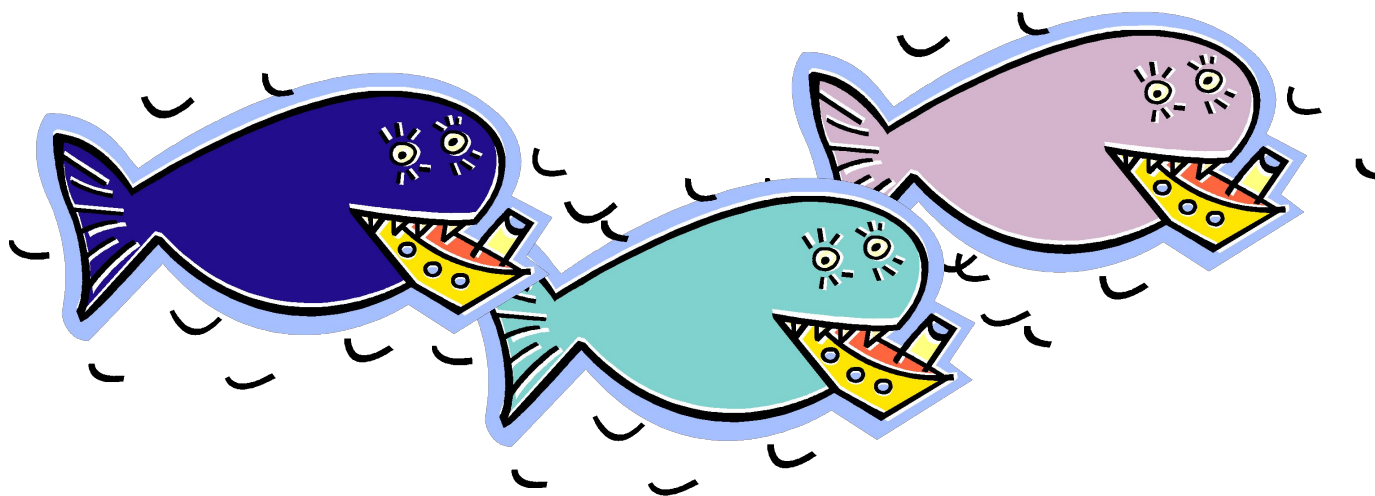
Конфиденциальность

2

Целостность

3

Доступность



Гексада Паркера

- 1 Конфиденциальность
- 2 Целостность
- 3 Доступность
- 4 Управляемость
- 5 Подлинность
- 6 Полезность



- ❖ Человеческий фактор
 - Злые инсайдеры
 - Уволенные по сокращению сотрудники
- ❖ Потеря оборудования
 - Кража ноутбуков
 - Кража систем хранения
- ❖ **Обеспечение ИБ!**



Задача СІО : как выбрать подходящую стратегию обеспечения информационной безопасности в условиях ограниченного бюджета и растущих рисков НСД к информационным активам?

Interim Plan

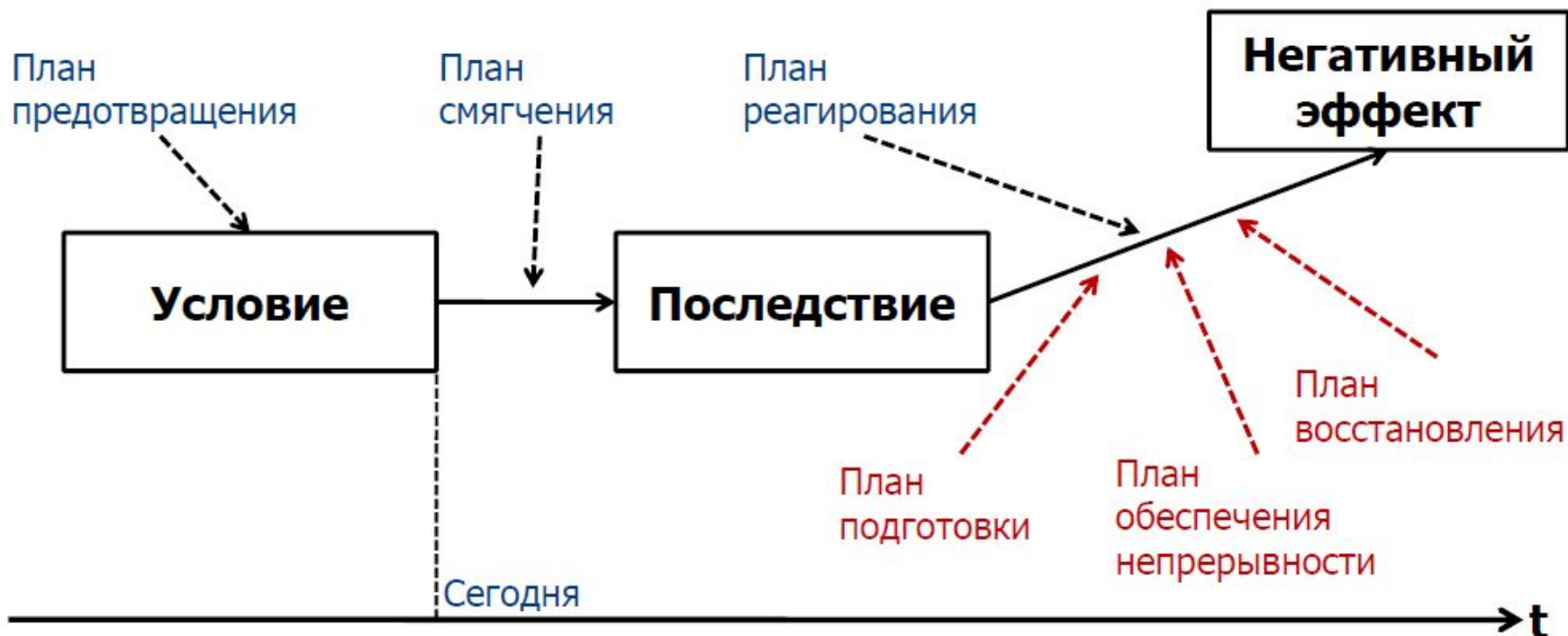
Our Disaster Recovery Plan
Goes Something Like This...



Final Plan Under Construction

© Scott Adams

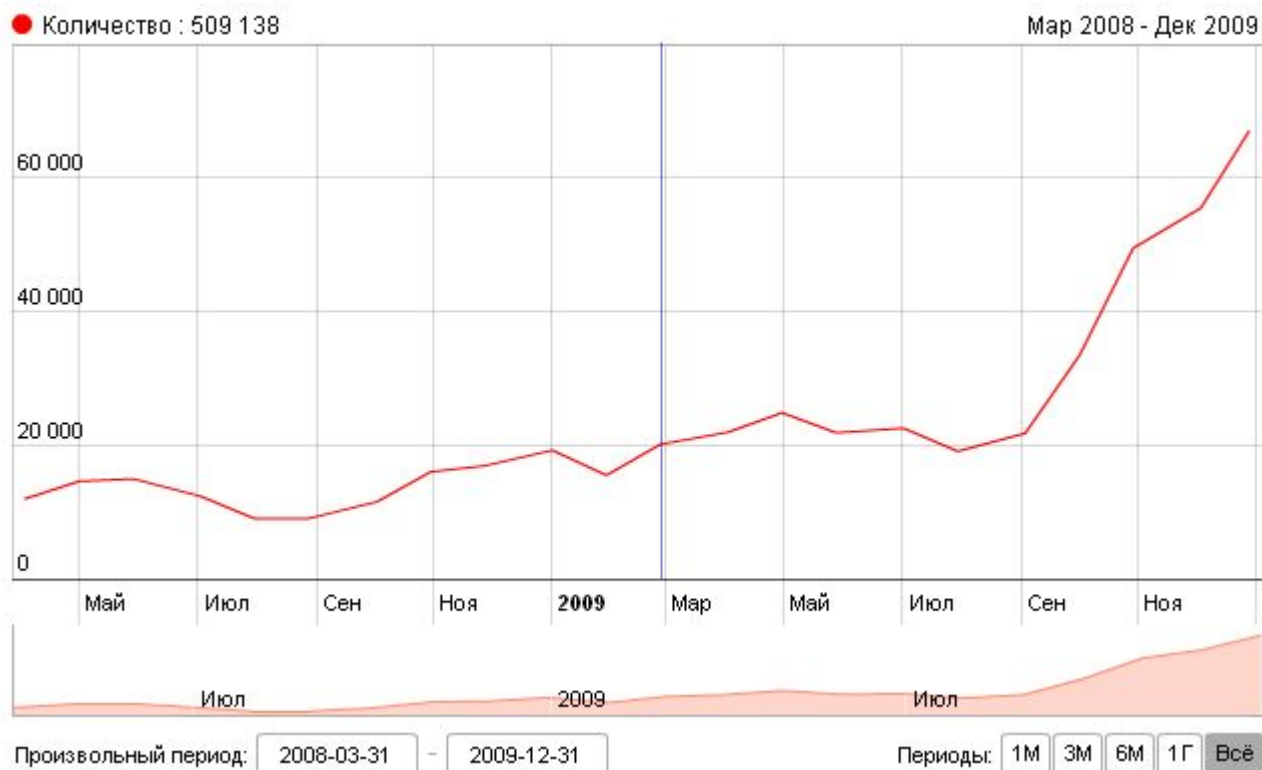
Планирование работы с рисками



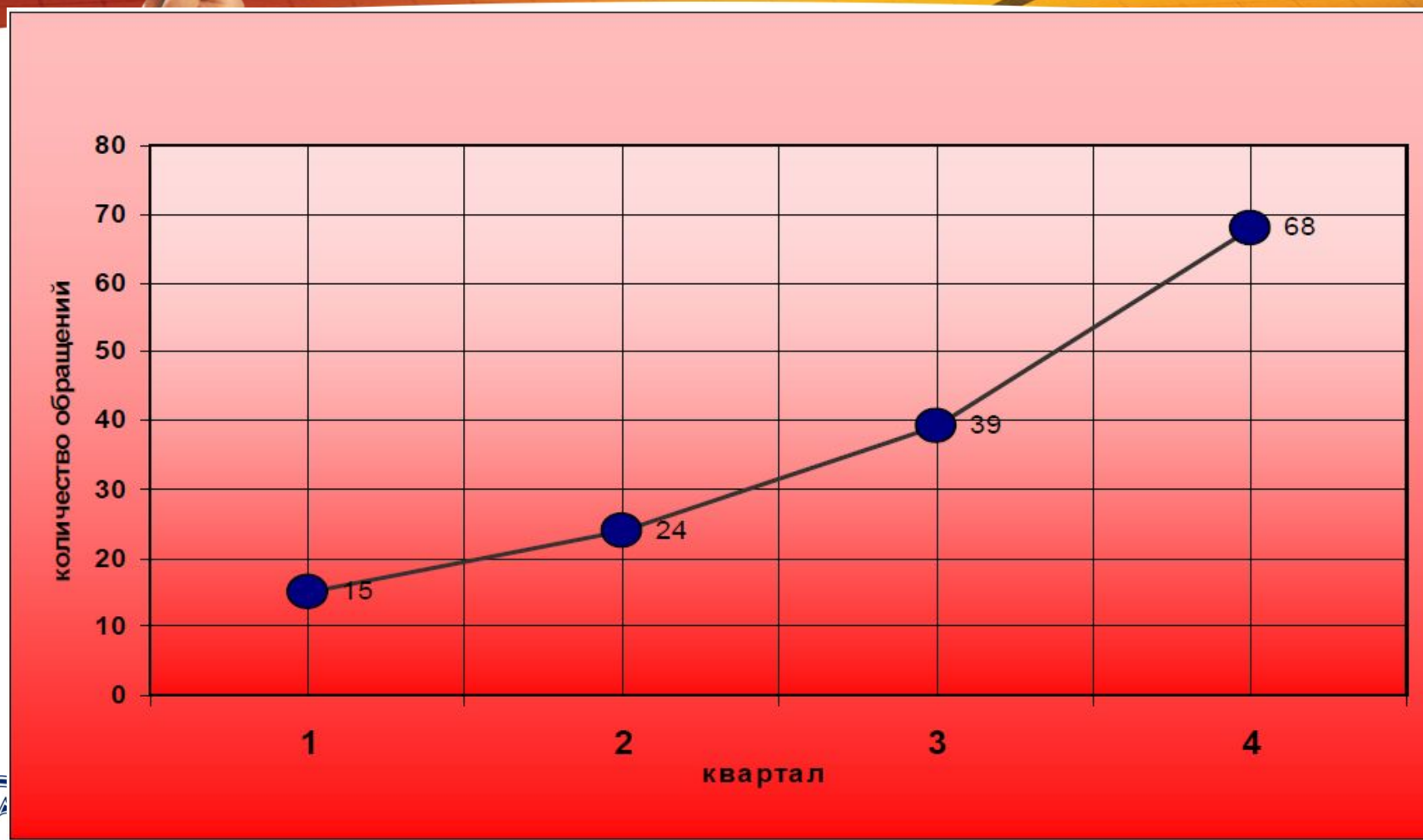
Источник: Дмитрий Башакин, курс РМ-021 «Управление рисками», © УЦ Luxoft, 2009

Интерес к проблеме защиты персональных данных

- ❖ <http://www.google.com/insights/search>
- ❖ <http://wordstat.yandex.ru/?cmd=words>



Количество поступивших обращений в Роскомнадзор (2008)



- На конкретном примере оценили риски и угрозы, связанные с человеческим фактором в информационной безопасности
- Развили навыки применения моделей и методов управления рисками для решения проблем информационной безопасности, сопряженных с человеческим фактором
- Приобрели опыт профилактической и предупреждающей деятельности в области управления рисками



Использованные источники

- ❖ Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных: <http://pd.rsoc.ru/>
- ❖ Башакин Д. РМ-021 Управление рисками, Luxoft, 2009
- ❖ Holtzman D. PRIVACY LOST: How Technology Affects Privacy // Interop'2008 Moscow
- ❖ Руководство к своду знаний по управлению проектами, 4-е издание (PMBOK Guide 4th Ed.), 2008
- ❖ Тимошенко А. Обзор законодательства РФ: типовые юридические и бизнес риски // Softline, 2009.
- ❖ Лирник Д. Организация и проведение работ по защите персональных данных // Softline, 2009.
- ❖ Савельева А. Курс «Организация и технологии защиты информации». ГУ-ВШЭ, 2009.
- ❖ Савельева А. Курс «Управление рисками». ГУ-ВШЭ, 2008.



Вопросы?

Управление рисками

alexandra.savelieva@gmail.com

