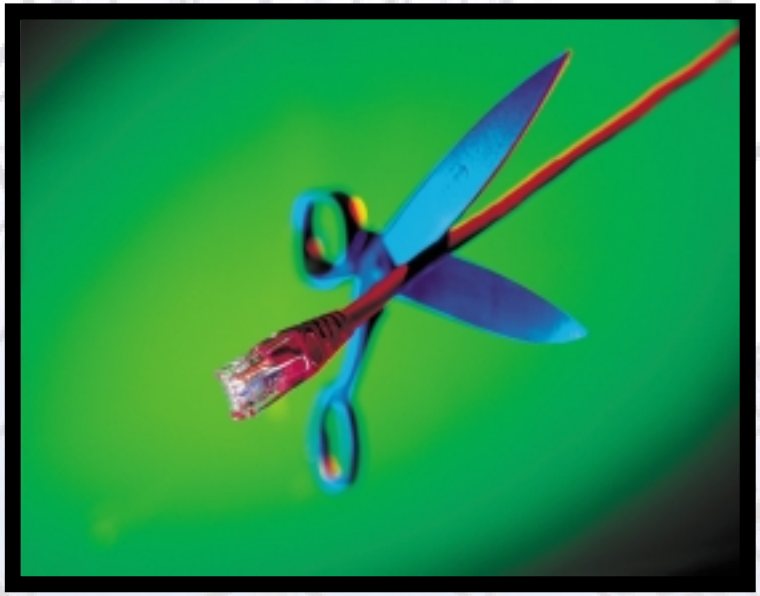
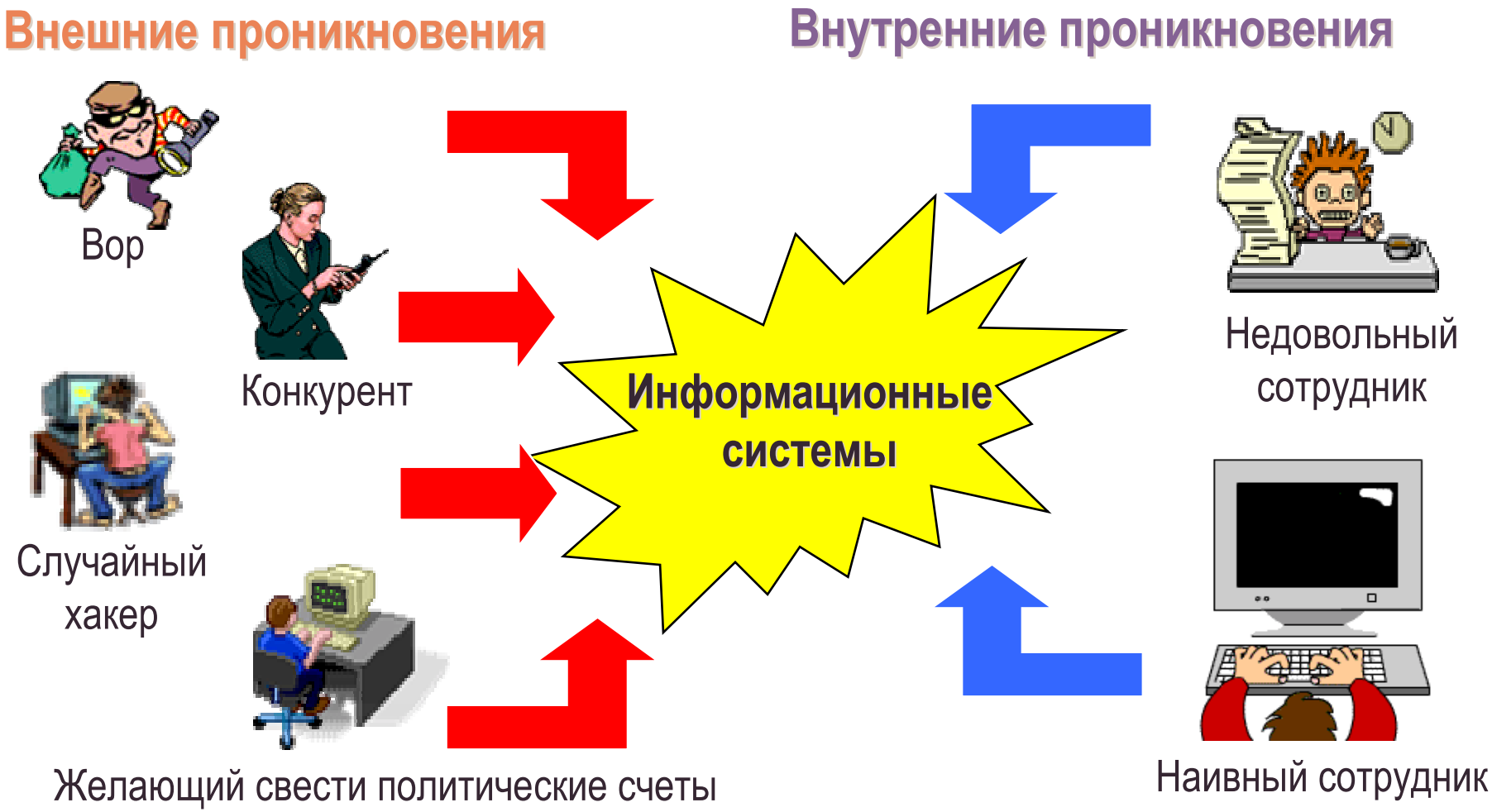
«Эрнст энд Янг»



Насколько Ваш бизнес уязвим перед кибер-терроризмом?

Почему Ваша компания должна уделять приоритетное внимание **информационной безопасности**?

Риски в области информационной безопасности



Риски в области информационной безопасности

Почему мы сталкиваемся с этими рисками?

Внешние проникновения

- Прибыль
- Подрыв конкуренции
- Интеллектуальные упражнения/развлечения
- Сведение политических счетов

Внутренние проникновения

- Прибыль
- Сведение личных счетов
- “Это чистая случайность!”

Риски в области информационной безопасности

Риски в области информационной безопасности → **Бизнес-риски**

- Прямые финансовые убытки от противозаконных операций
- Кража конфиденциальной информации/коммерческих тайн
- Потеря возможностей для бизнеса в результате сбоев в работе
- Несанкционированное использование ресурсов
- Утрата уважения или доверия к компьютерным технологиям
- Ущерб для репутации

Риски в области информационной безопасности

С нами этого не случится ! → **Но риск существует…**

- ❑ Отказ от электронного бизнеса → Конфиденциальная информация в ИС
- ❑ Незаметность → Объектом атаки хакеров может стать кто угодно
- ❑ Установка систем информационной безопасности → Эффективны ли они?

Риски в области информационной безопасности

Сохраняющиеся риски/проблемы

- Выявление новых уязвимых мест в
  - операционных системах
  - системах защиты данных
  - сетевых услугах
- Создание новых вирусов

Риски в области информационной безопасности

Сохраняющиеся риски/проблемы (продолжение)

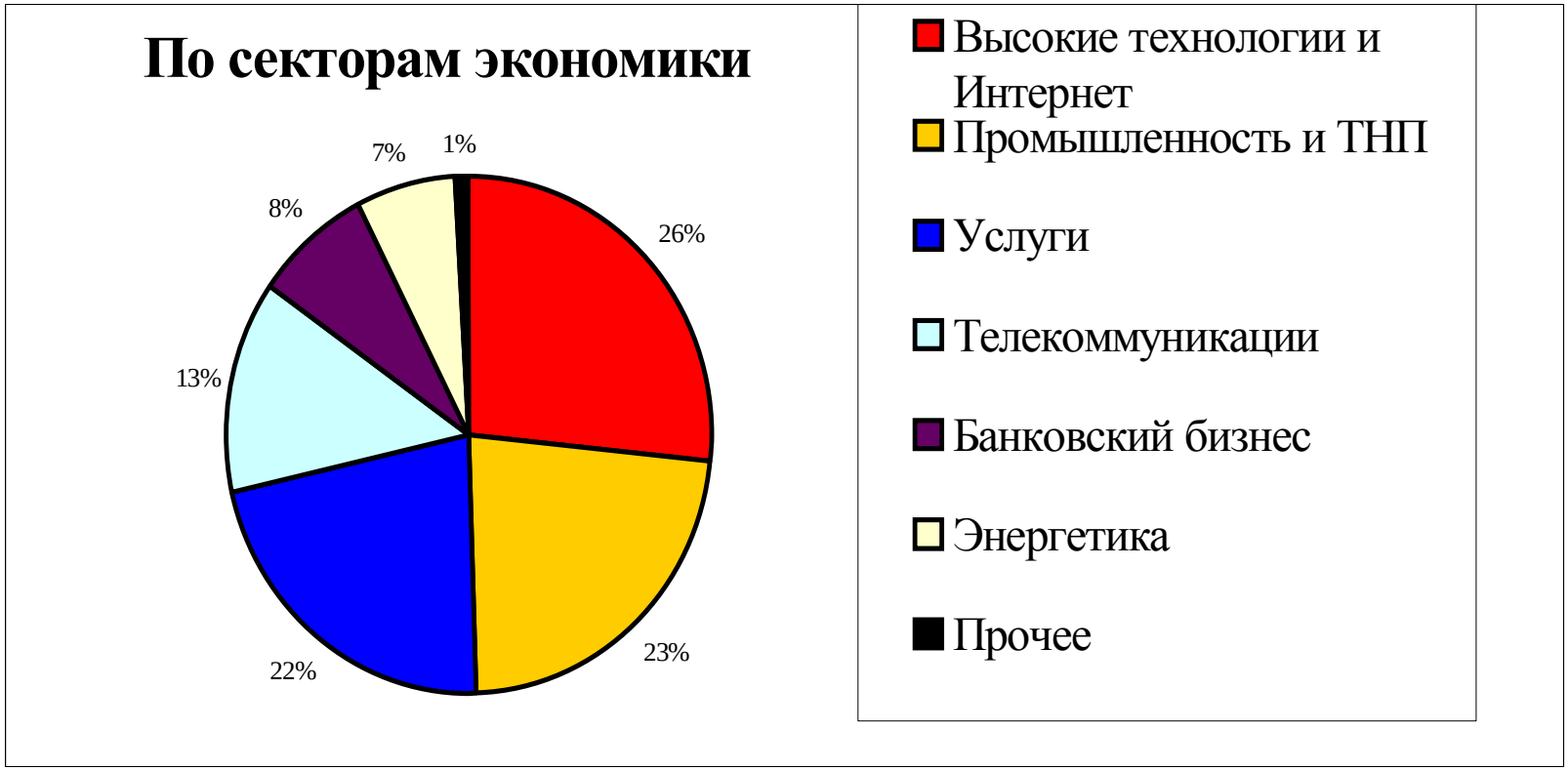
- Человеческий фактор
  - ошибки в конфигурации
  - недостаточный контроль
  - недостаточное внимание к защите данных
  - недостаточная оперативность/отсутствие мер по обновлению устаревших версий программного обеспечения с выявленными уязвимыми местами

В июне-июле 2001 года

фирма «Эрнст энд Янг» провела **исследование по проблемам информационной безопасности** для анализа мнений предприятий, работающих в России и других странах СНГ, о **рисках в области информационной безопасности**.

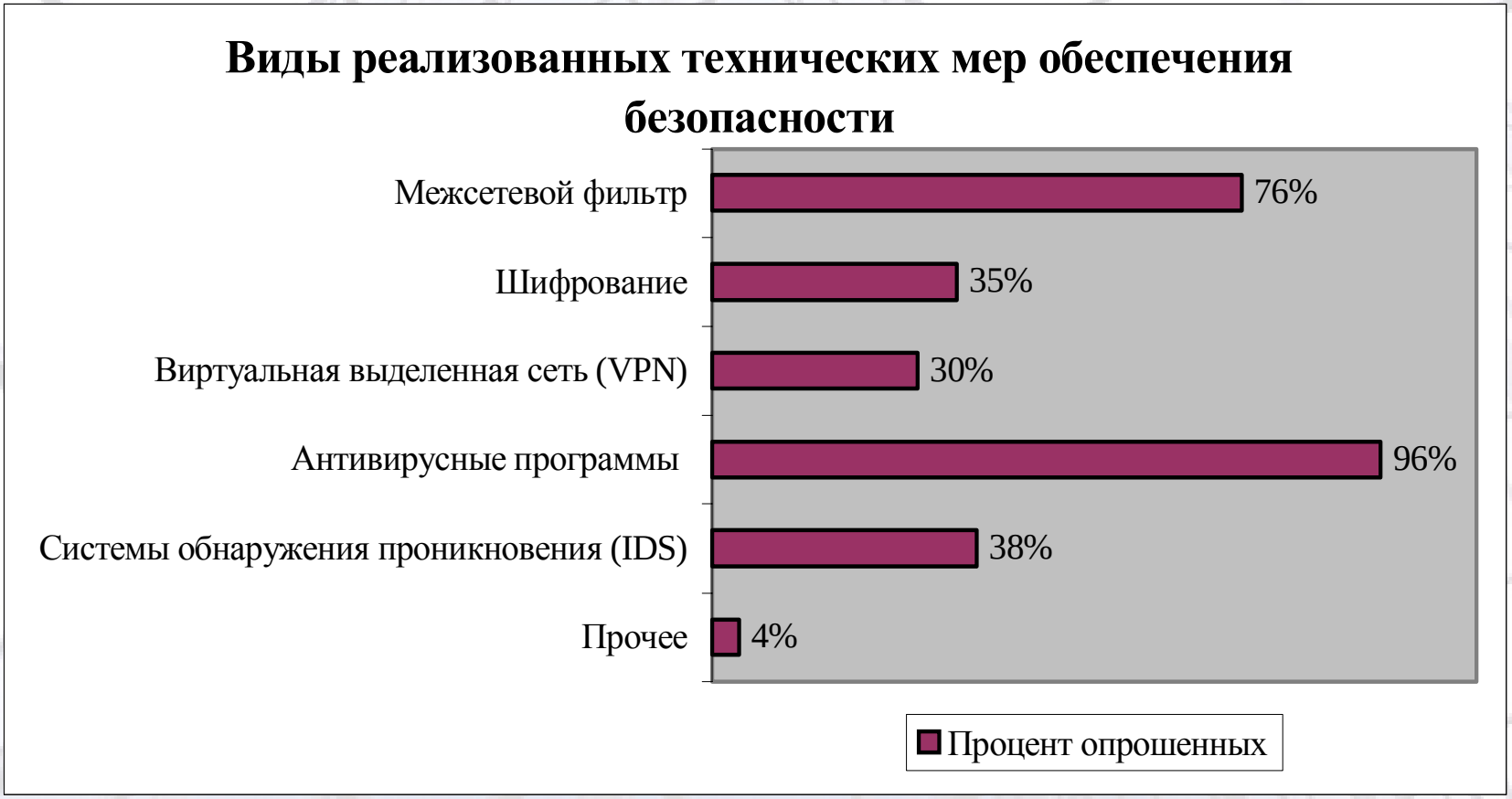
Результаты по России/СНГ

Участники исследования



Результаты по России/СНГ

Технические меры обеспечения безопасности



Результаты по России/СНГ

Организационные меры обеспечения безопасности

Результаты по России/СНГ

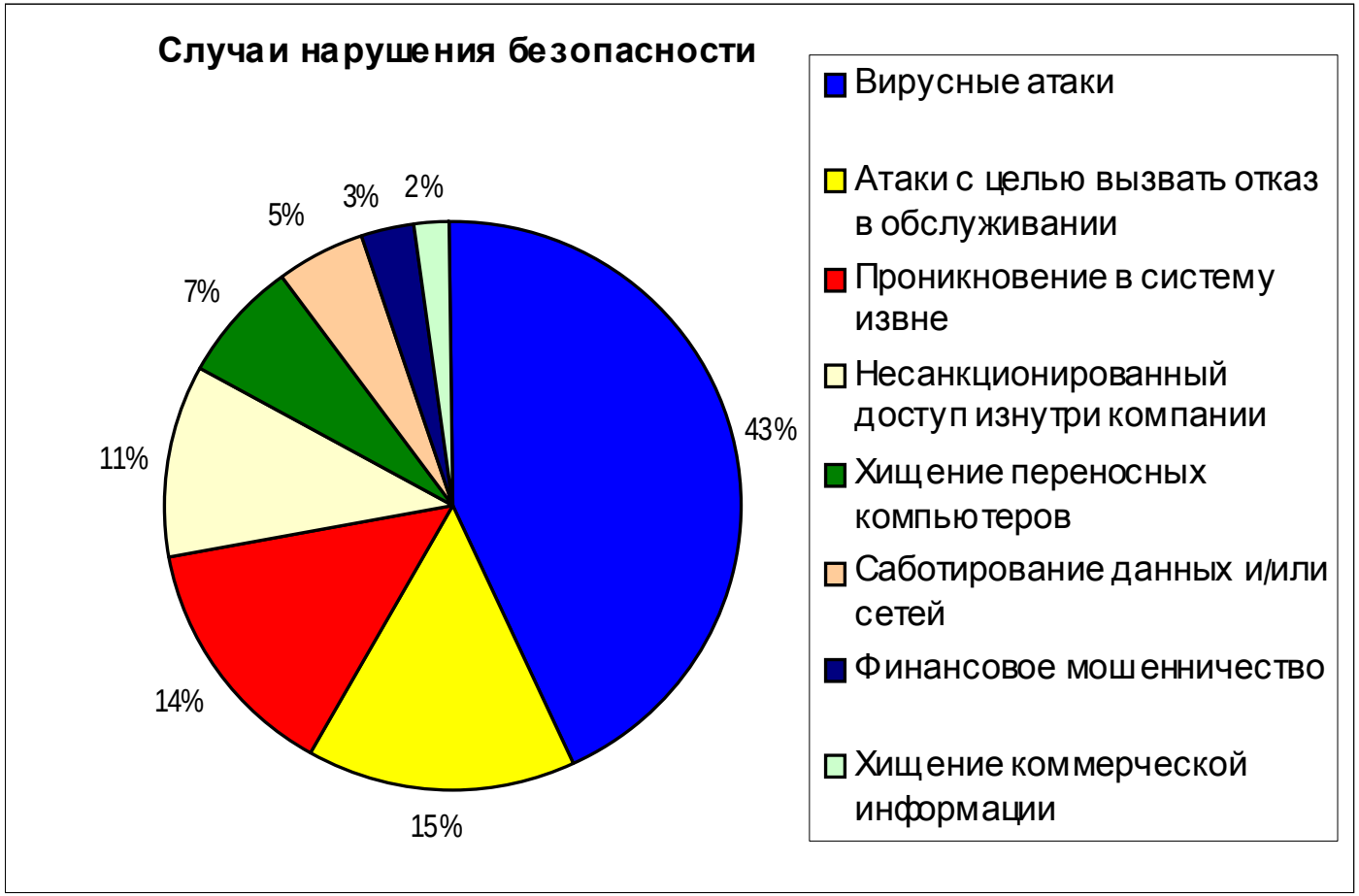
Достаточны ли эти меры безопасности?

- **65%** респондентов сталкивались с **нарушениями безопасности** за последний год

- **50%** нарушений были связаны с **хакерскими атаками**, например:
  - проникновение в систему извне
  - несанкционированный доступ изнутри компании
  - атаки с целью вызвать отказ в обслуживании
  - нарушение целостности данных и сетей

Результаты по России/СНГ

Случаи нарушения безопасности



Решения в области информационной безопасности

Чтобы до минимума сократить риски нарушения безопасности,

…….необходима **эффективная стратегия обеспечения безопасности,**

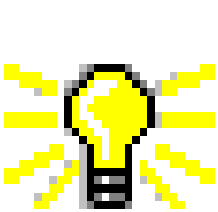
которая предусматривает:

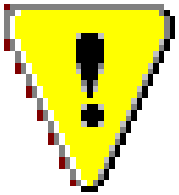
- **определение угроз и уязвимых мест**
- **разработку соответствующих мер обеспечения безопасности**
- **регулярное тестирование этих мер**
- **обнаружение атаки (если она произойдет)**

Решения в области информационной безопасности

Определение угроз и уязвимых мест

- **регулярный анализ** обнаруживаемых уязвимых мест программно-аппаратного комплекса





ВНИМАНИЕ!!

ARCserve (Computer Associates):
Версии этого продукта настроенного по умолчанию, позволяют любому пользователю домена получить доступ к сетевым ресурсам "ARCSERVE$"

Потенциальный хакер

Доступ к этим ресурсам может позволить недобросовестному пользователю ознакомиться с конфиденциальными системными данными или разрушить файлы, используемые для резервирования.

Ваш менеджер по информационной безопасности

Решения в области информационной безопасности

Разработка соответствующих мер безопасности

- **тщательный подбор** мер безопасности
- **надлежащая реализация** мер безопасности
- разработка и реализация **правил и процедур работы с компьютерной техникой**

Незащищенная компьютерная среда

Беспечный сотрудник

Защищенная компьютерная среда

Решения в области информационной безопасности

Регулярное тестирование мер безопасности

- необходимо обеспечить **эффективность работы** этих мер для всех известных уязвимых мест.
- должно проводиться **независимым подрядчиком** (т.е. оценка безопасности путем имитации взлома системы).

Решения в области информационной безопасности

Обнаружение атаки

- **Системы обнаружения попытки проникновения** упрощают распознавание атаки на ранней стадии. Это позволяет:
  - представить себе последствия хакерской атаки для деятельности компании
  - понять, какие меры необходимо принять для недопущения подобных инцидентов в будущем

Решения в области информационной безопасности

План по поддержанию деятельности в экстремальных ситуациях

- позволяет избежать **отказа важнейших систем обеспечения деятельности** (из-за стихийных бедствий, сбоев оборудования и т.п.)

По данным нашего Исследования:

- 26% респондентов испытали такие отказы в течение последнего года
- 78% из них либо
  - не имели плана,
  - либо не тестировали его

Заключение

Интернет-экономика

Новые возможности и новые риски

Успешный бизнес

Довольные сотрудники, руководители, акционеры

"Эрнст энд Янг"
Услуги в области информационных технологий и обеспечения информационной безопасности

- Оценка возможности безопасной реализации **стратегии электронного бизнеса**
- **Оценки рисков обеспечения безопасности** ("имитация взлома") информационных сетей и систем
- Консультирование по разработке **правил и процедур работы с компьютерной техникой**

Контактное лицо:

Мишель Мур (Michelle N. Moore)

"Эрнст энд Янг"

Услуги в области информационных технологий и обеспечения информационной безопасности

Подсосенский переулок, 20/12,

Москва 103062

Тел.: 705 9749

E-mail: michelle_moore@notes.eycis.com