# Практика проведения инструментального анализа ИБ ИС

*Качалин Алексей*

*Перспективный мониторинг*

# Вместо вступления: *Целевая атака не пройдет*

**From:** Ассоциация «РусКрипто» [mailto:info.ruscrypto@mail.ru]
**Sent:** Tuesday, November 13, 2012 6:59 AM
**To:** [redacted]
**Subject:** Приглашение на работе XIV международной конференции «РусКрипто'2013»

Ведущему специалисту
ОАО «[redacted]»

Уважаемый господин

Ассоциация «РусКрипто» и Академия Информационных Систем приглашают вас принять участие в работе XIV международной конференции «РусКрипто'2013», посвященной основным вопросам информационной безопасности.

Даты проведения: 28 — 31 марта 2013 года
Место проведения: Московская область, Солнечногорский р-н, ГК «Солнечный Park Hotel & SPA»

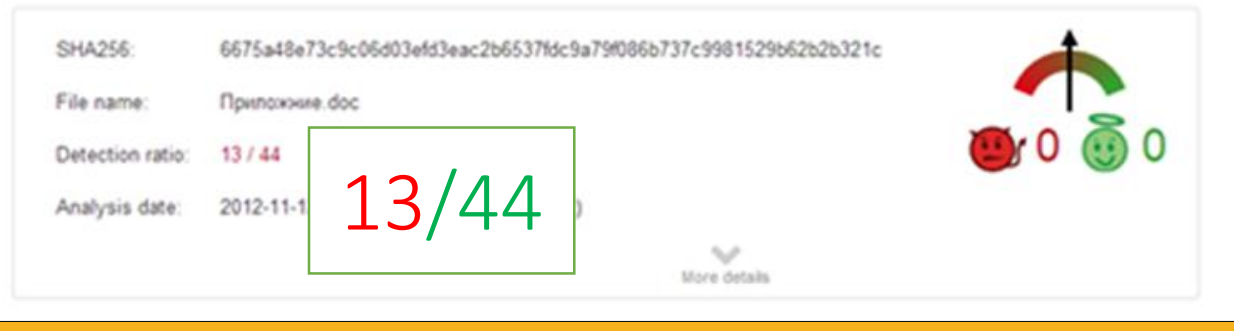
- Пришло несколько десятков писем
- Внутренняя пересылка
- Открытие вложения? Конечно
- Оповещение ИБ/ИТ? Нет

**Subject:** НА: Приглашение на РусКрипто - потенциально вирус

Эх, где ты был раньше… ;(
Я вот тоже с утра в подозрениях мучуюсь, т.к. кликнул в Outlook на предварительный просмотр вложения этого письма и эта зараза что-то успела заинсталлировать…
После этого скачал свежий релиз проверялки от Касперского – она ничего

**Subject:** FW: Приглашение на работе XIV международной конференции «РусКрипто'2013»

Говорят – вирус. Да /нет?
http://blogs.mcafee.com/mcafee-labs/cve-2012-0158-exploit-in-the-wild



# Обязательная часть доклада за ½ слайда


- Определяем определения
- Сканируем сканерами
- Анализируем анализаторами
- Бумажность мер и специалистов
- Комплайнс/ПДн – не решение реальных проблем
- apt, scada, cybercrime, cloud, cyberwar, cybercyber

** И даже обязательная картинка про пентест*

В оставшееся время

- Проблемы возникающие на практике
- Ценность услуг по анализу ИБ
- Что нужно добавить к годным инструментам

# «Требования бизнеса»

- Оставим без внимания,
  дабы не нарушать общности
  - Blackhat, торговля уязвимостями
  - Поиск уязвимых сервисов в Интернет
  - Хактивизм, pr
  - Академические исследования
  - Бесплатный пентест как средство продвижения услуг

Т.е. говорим о легитимных работах, тогда:

- Есть Заказчик – Удовлетворенность?
- Есть договорные отношения – Развитие?
- Контроль/снижение себестоимости
- Контроль/сокращение сроков выполнения работ

# Очень клиенто-ориентрованный слайд

# Но есть пара вопросов

Мотивация Заказчика

- Ограничения в возможностях и сроках
- Противоречия в желаниях
- Импульсивные желания - отработка по инциденту

Специфика (проектность, вариативность) услуги

- Анализ продукта/отдельного сервиса
  - Код, дистрибутив
  - Стенд, продуктив
- Анализ ИС
  - Инфраструктура/Сервисы
  - Пользователи, активность
- Актуальная модель угроз
  - Публично-доступный ресурс

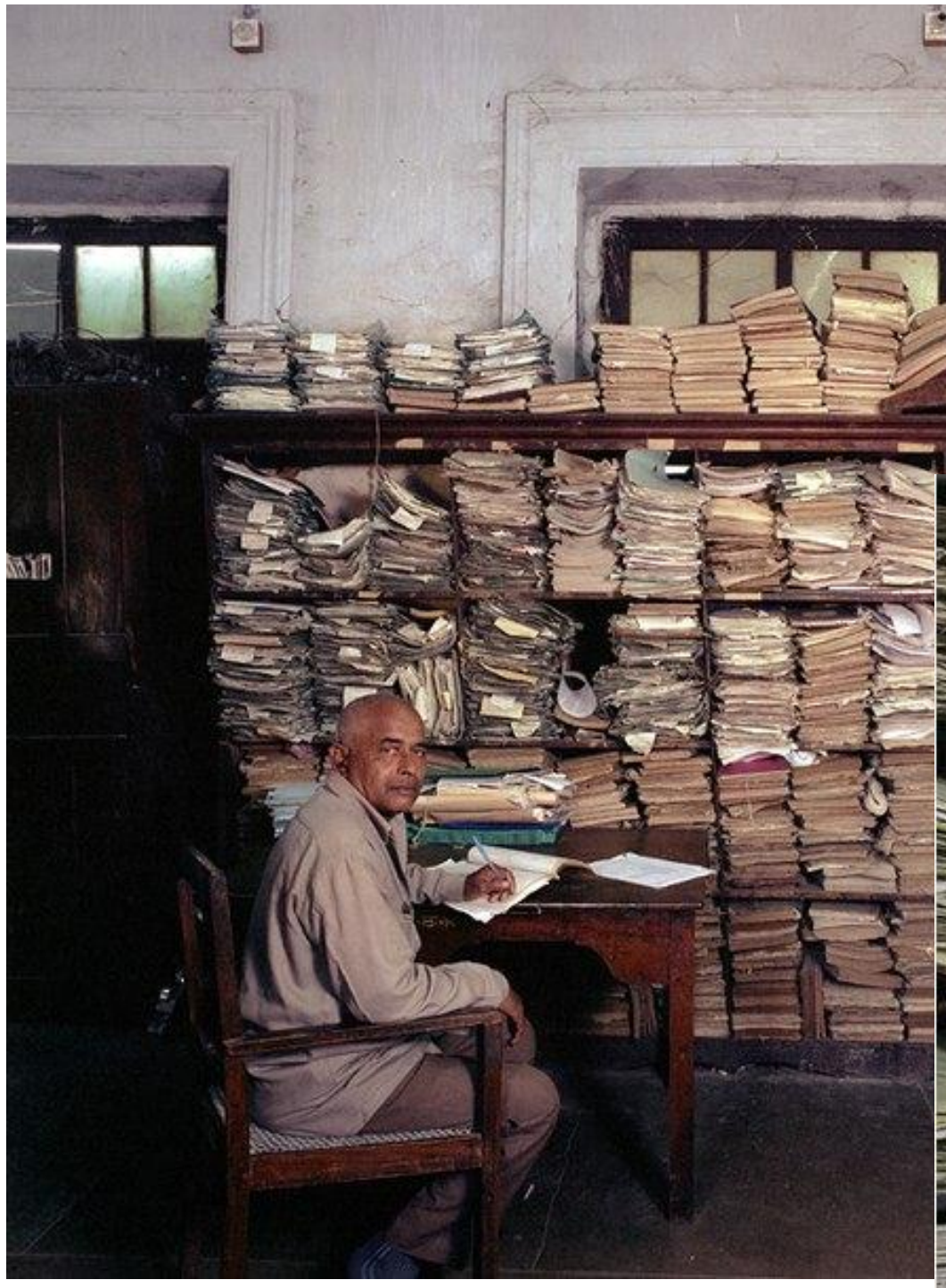
ВОПРОС

? !

ВОПРОС РЕБРОМ

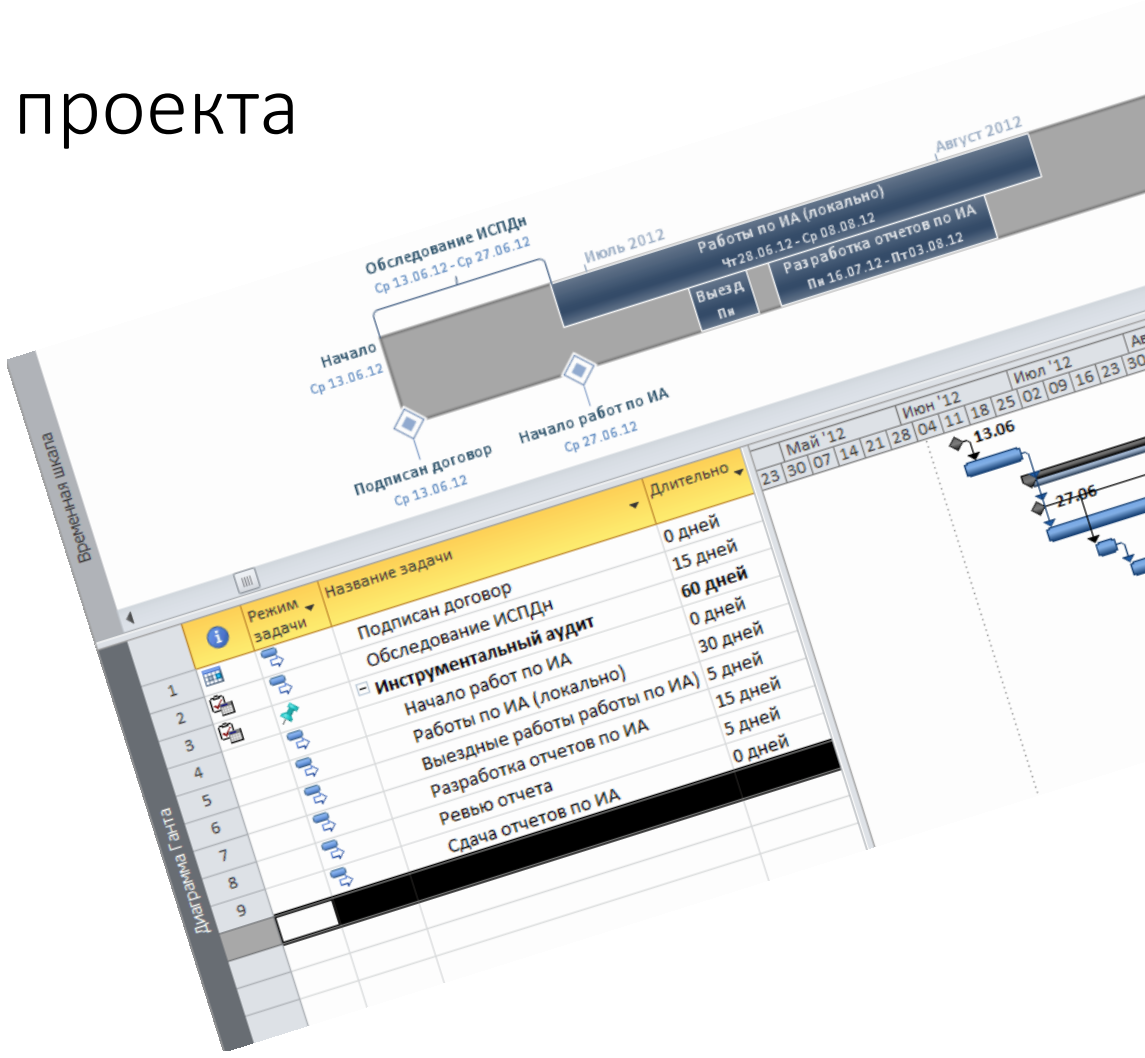
# Выявляем ЗП и потребности

# Ага! Вот эти ребята!



# Выполнение работы

- Менеджмент
  - Уточнение/фиксация границ проекта
  - Планирование работ
  - Учет рисков проекта
  - Соблюдение сроков работ
- Коммуникации
  - Начало работ
  - Устранение проблем
- Повышение эффективности
  - накопление компетенций
  - наработка знаний по клиенту/продукту
  - оптимизация расписаний
- **Выполнение работ с необходимым качеством!**



# Исследуй @ Ломай?!

# Торопиться не надо!

- Документация не успела, люди поменялись
  - Недокументированное
  - Существующее только на бумаге
- Географическое расположение объектов ИС
- Специфичные системы - заказная разработка
- Ограничения по объектам исследований
  - Работайте, только ничего не трогайте
- Привлечение специалистов Заказчика
  - Интервьюирование, сопровождение работ
- Специфичные угрозы
  - Зависимость от вендора
  - Влияние на непрерывность бизнеса 5-10-… лет
- Организационно-правовые нюансы
  - Аутсорсеры
  - Партнеры

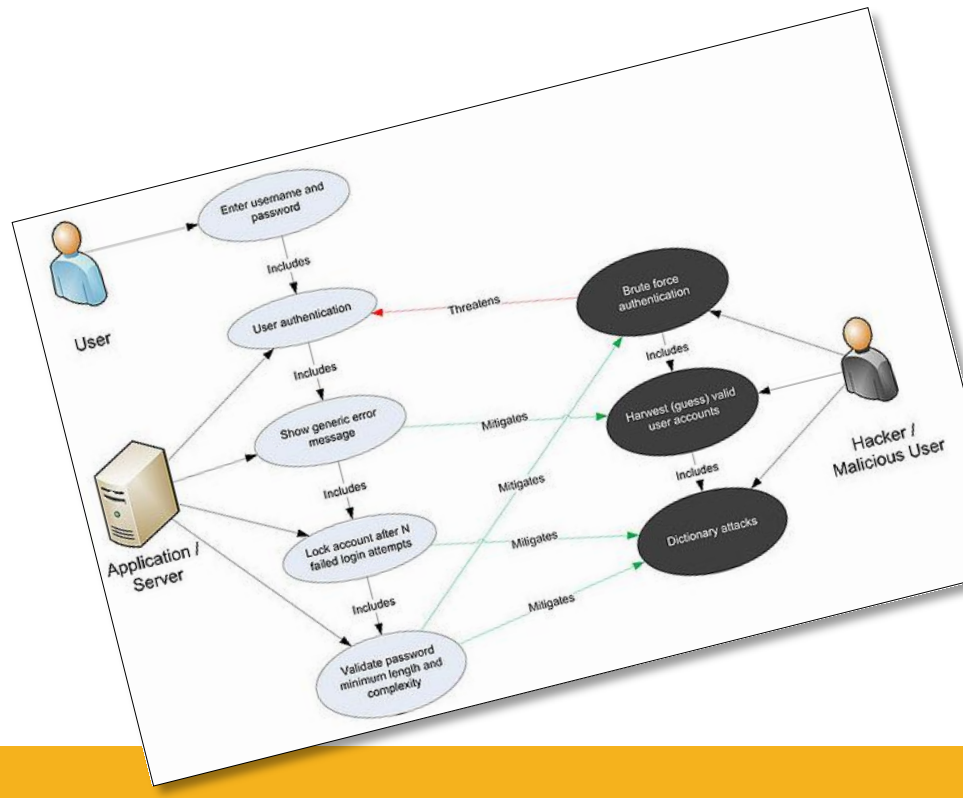
# Давайте уже бахнем?!

- Собрали документацию
- Провели интервью
- Провели инструментальный анализ мощным инструментом

# Есть над чем подумать

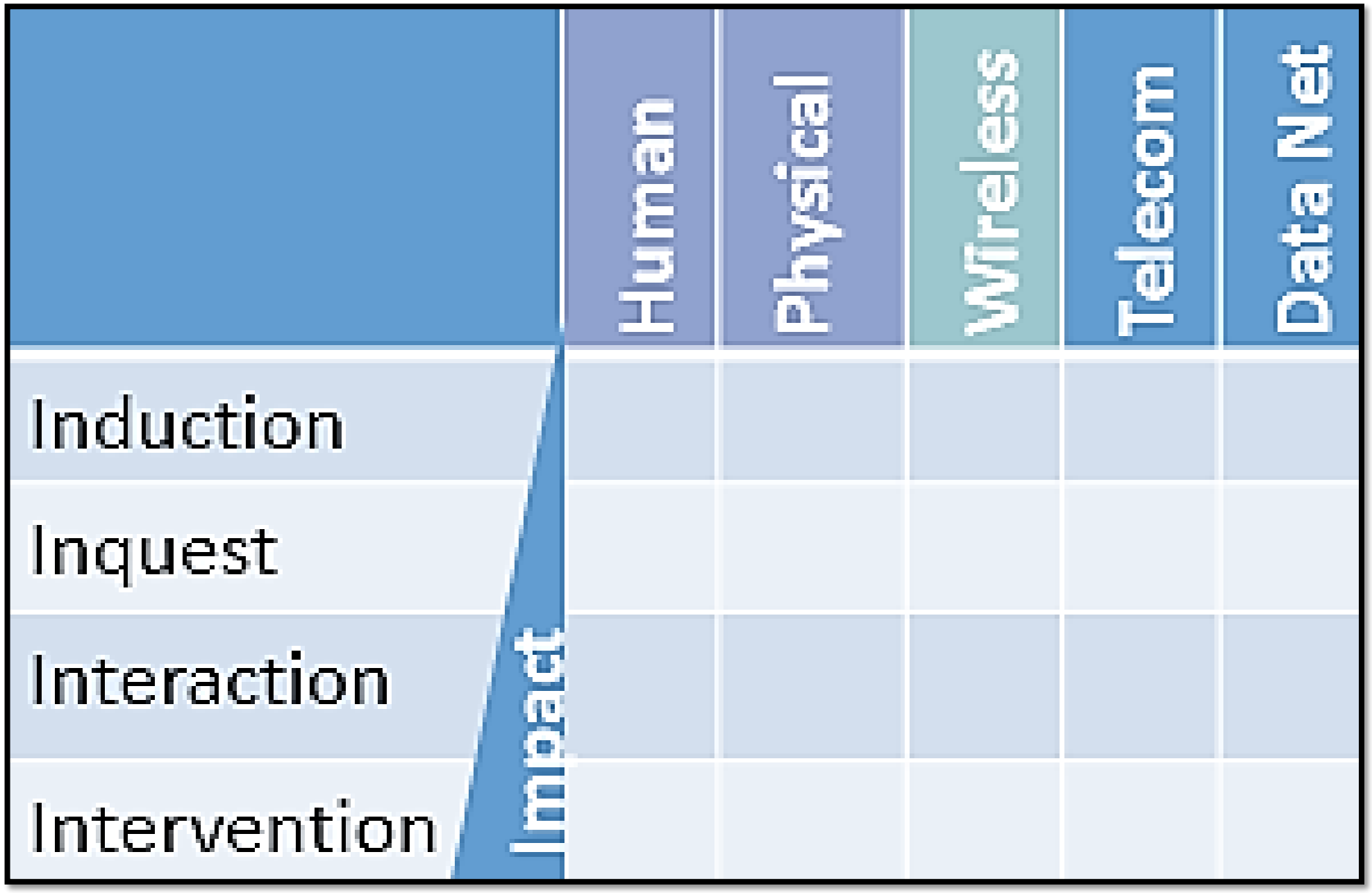
# Полезные аналитические инструменты

- Реестры/таблицы, outline, mindmap
- Сценарии, MisUsecases
  - Рабочий инструмент аналитика – интервью, презентация результатов
- Диаграмма потоков данных (DFD)
  - Подход ориентирован на ПО
  - Возможность автоматизированного анализа
- Деревья атак/отказов (FTA)
  - Трассировка на причины и следствия



# Обоснование полноты исследования

- Проблема «стандартного сценария исследования»
- Перебрать все возможные варианты
- Упорядочить/выбрать работы исходя из ограничений и приоритетов



# Ресурс-Взаимодействие-Контроллер

| | |
|---|---|
| Виды | интерактивный<br>идентификация/авторизация,<br>подотчетность, достоверность,<br>конфиденциальность,<br>Процессный<br>целостность, доступность,<br>неотказуемость |
| Методы | Разделение – убрать/устранить ресурс<br>Устранить последствия угрозы<br>Устранить угрозу |
| Количественная оценка | менее 100% - недостаточная,<br>100% - баланс,<br>более 100% ИБ – избыточные |
| Ограничения контроля, контроллеров | Конфликты средств ИБ<br>Средства ИБ как ресурс ИС и возможность взаимодействия - дополнительные вектора атак |

# Аналитические Ашипки

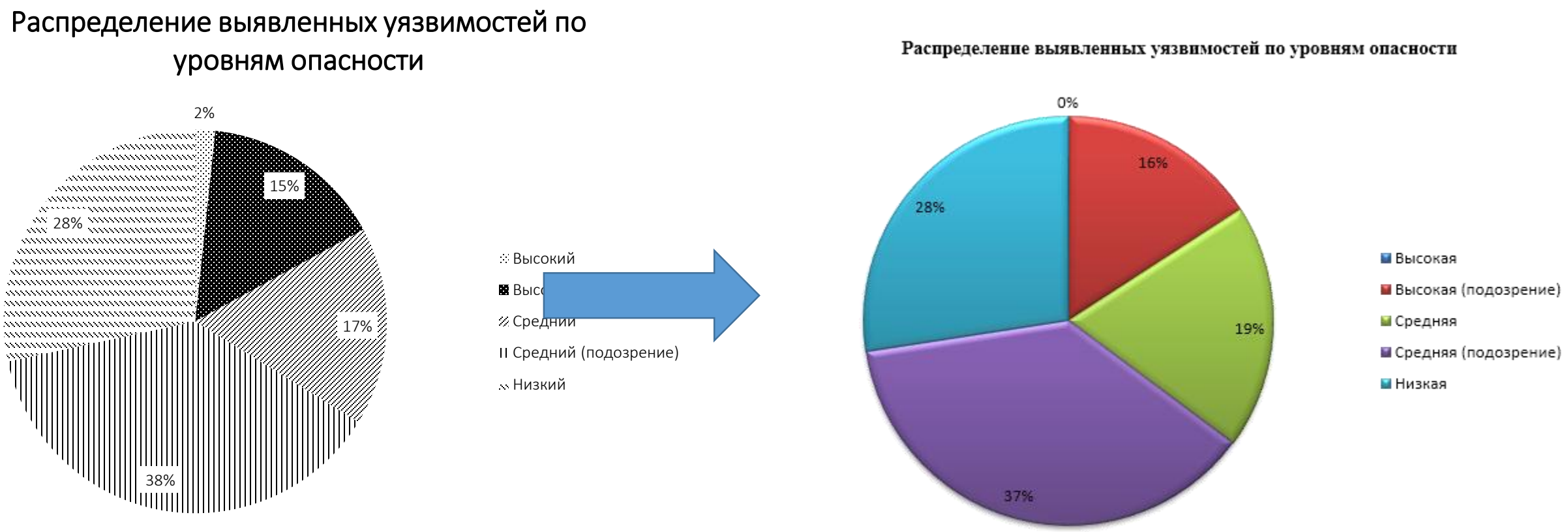
- Не выработан единый словарь
  - «ЕТС обслуживается СЭ и обеспечивает БРПС в ЗУД»
- Не учитывается время
  - продолжительность замеров
  - Сравниваются замеры сделанные в разное время
- Не учтен вероятностный характер тестирования – часть объектов исследования может быть недоступна в момент исследования
- Неправильное отношение к артефактам
  - Попытка с самого начала писать итоговый отчет
  - Сырой отчет сканера не для заказчика
  - Отсутствие промежуточных схем и перечней
  - Избыточно-детальный отчет (инженерный подход вместо аналитического)

# Выжимаем максимум из ИА

- Инструментальный анализ будет полезен если:
  - Проведена подготовительная аналитическая работа
  - Результатам дана интерпретация
- Отработка замечаний к результатам – «из 2 зол»
  - Статус – «не определен» лучше чем отсутствие информации
  - Фиксация аномалий – отклонений в поведении, причины и последствия которых вне границ исследования
- Аналитик «в теме» проекта может и должен уточнить по результатам
  - Уточнение потребностей
  - Глобальные изменения, затрагивающие компоненты ИС
  - Время, через которое в данной ИС нужно делать повторные работы
  - Предположения об объектах и процессах не исследованных инструментально – степень их уязвимости и потенциальный ущерб

# Вперёд и вверх - аналитика

- Развитие качества услуги (квартал, полгода, год)
  - Устранение выявленных уязвимостей
  - Появление новых сервисов
  - Модификация методик и инструментов
- Фундамент для исследовательских работ - Разработка моделей угроз/нарушителя
  - ИС в целом
  - Критичных подсистем в контексте ИС



# Исследование комплексных атак

- «Низкоорбитальная Ионная Пушка» позволяет (добровольно) подключить компьютер посетителя к DDoS атаке на ГИС
- Хостинг вне юрисдикции РФ, атакующие и цели – на территории РФ

## Альтернативный сценарий

Владелец ресурса может без ведома «активистов» направить атаку с их ПК на любую ИС

# Анализ угроз технологии → нормативные требования

**Функция ПО:**

1шт. Включить светодиод

**Разрешения**:

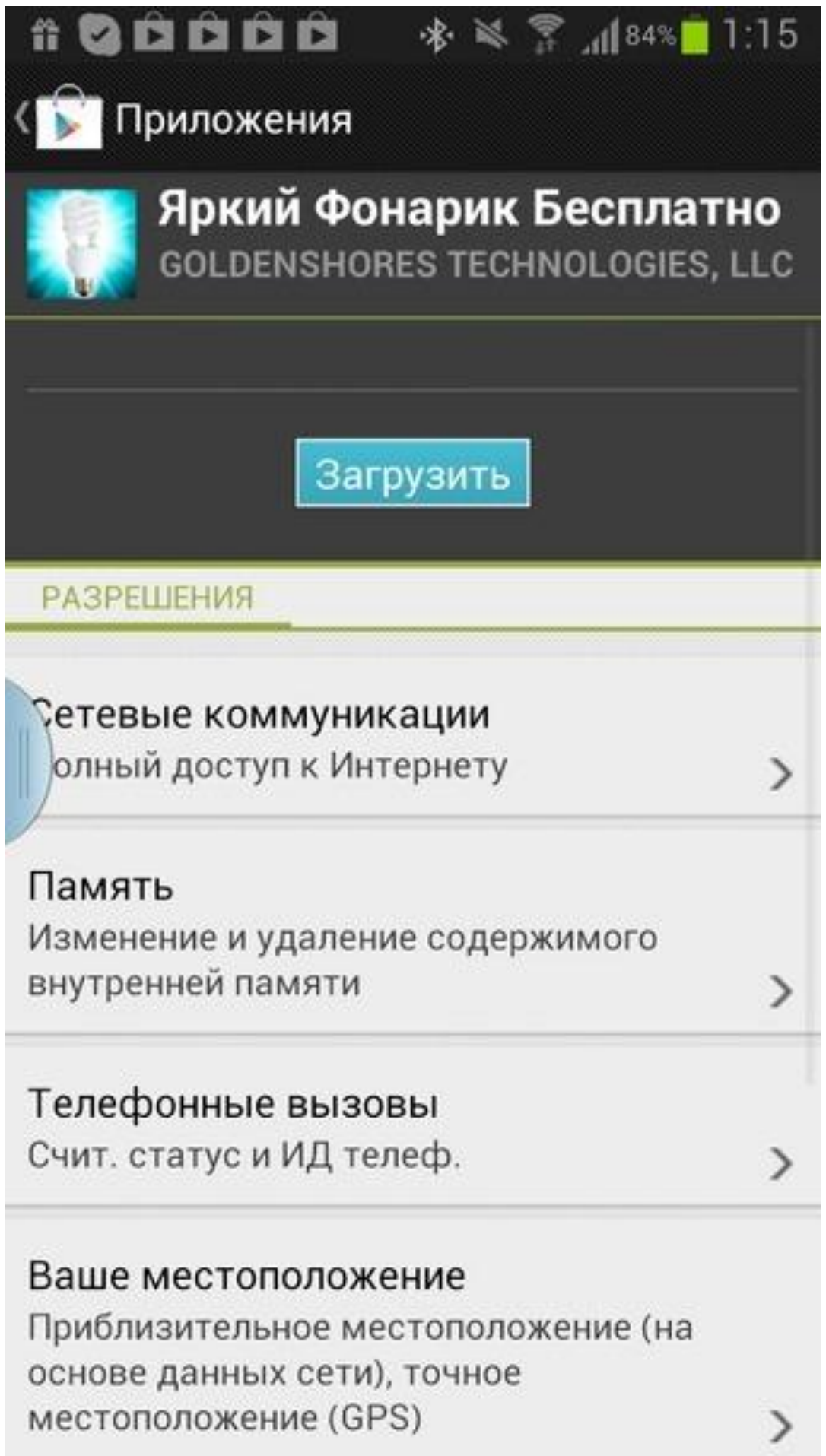
Полный доступ к Интернет

Полный доступ к памяти устройства

Доступ к гео-позиционированию

Полный доступ к истории звонков и СМС

Скачиваний: более 1 000 000



# Спасибо за внимание!

Алексей Качалин
kachalin@advancedmonitoring.ru
@kchln

info@advancedmonitoring.ru
http://advancedmonitoring.ru/
@am_rnd