VII Уральский форум
«Информационная безопасность банков»

Fraud-мониторинг для ДБО.

Повышение эффективности и противостояние угрозам банковского фрода.

Компания «БИФИТ»

1. Компания «БИФИТ»

На 01.02.2015 г. 38,5% российских банков используют систему «iBank 2»

- **Более 300 банков**
- **Защищаем от хищений с 2008 года**
- **Основные направления по безопасности:**
  - **Аппаратные средства защиты**
  - **Fraud-мониторинг и детектор угроз**
  - **Security lab**

2. Практика компании БИФИТ

3. Случай 1

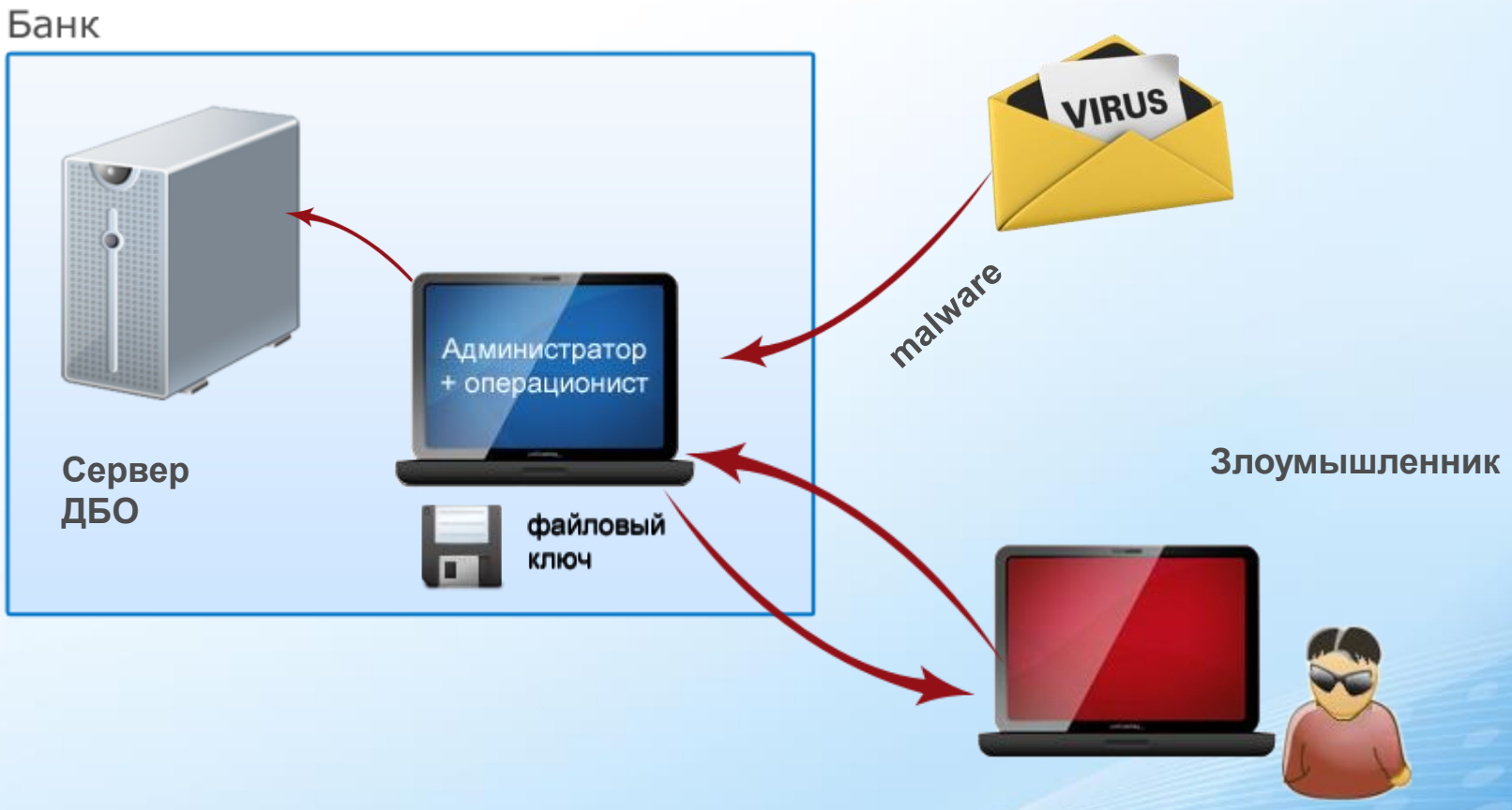
- 2 небольших региональных банка

- конец 2013 года и конец 2014 года

- Несколько скомпрометированных клиентов – юридических лиц

- Сумма хищения более 10 000 000 рублей

4. Случай 1


Банк
VIRUS
malware
Администратор
+ операционист
Сервер
ДБО
файловый
ключ
Злоумышленник

5. Случай 2

Массовые атаки на банки

- Начало 2014 года

- Письма по системе iBank2 с аттачем

- Аттач – файл с расширением scr

- Начало 2015 года

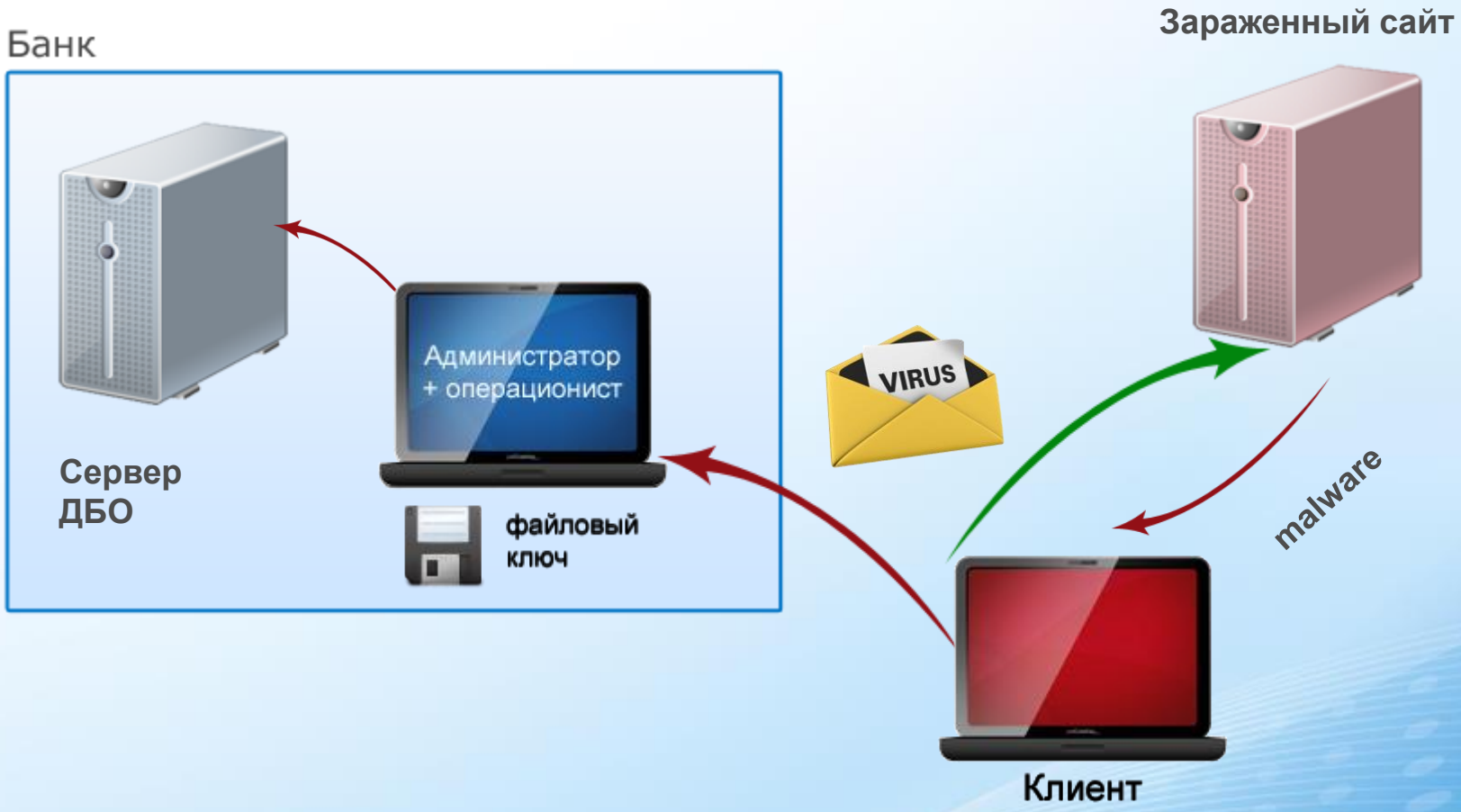
- Попытка хищения при помощи трояна удаленного управления

- Дополнительно - письмо с аттачем

- Аттач – doc – файл с эксплойтом CVE-2014-1761

BIFIT

6. Случай 2

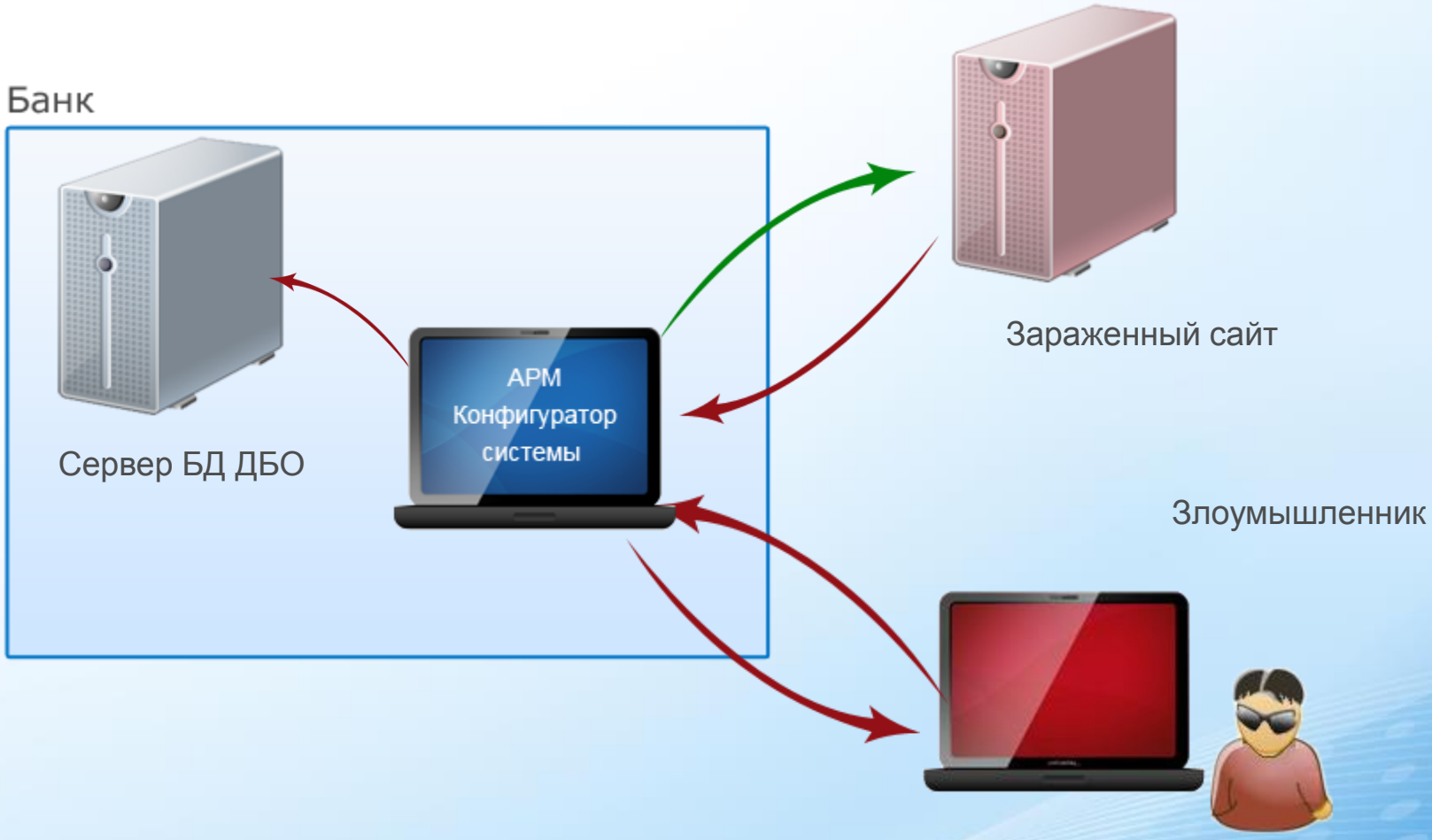

Банк
Зараженный сайт
Администратор
+ операционист
Сервер
ДБО
файловый
ключ
VIRUS
malware
Клиент

7. Случай 3

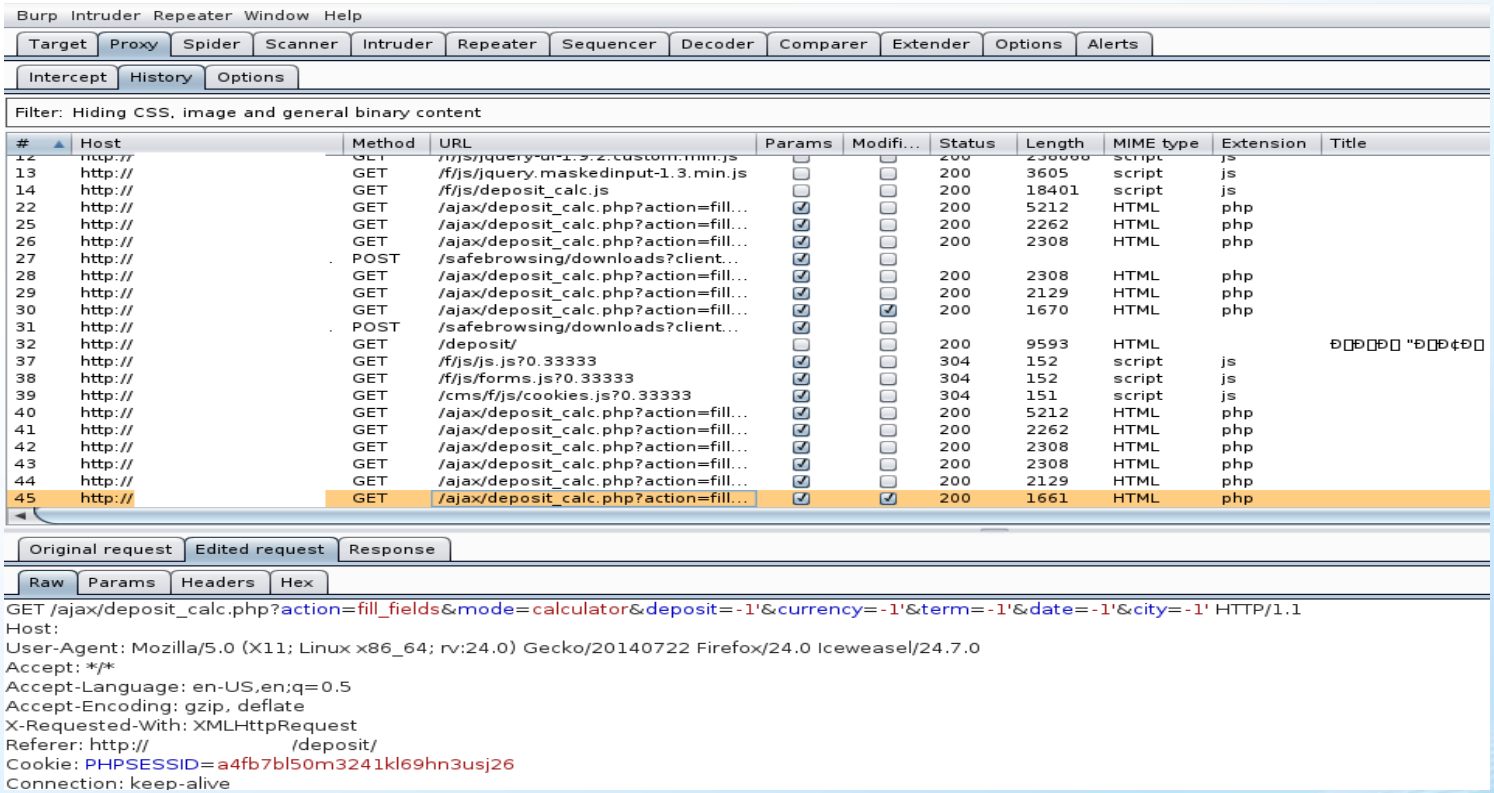
- Конец 2014 года
- Средний банк
- Компрометация сети банка через стороннее ПО.
- Получен доступ к базе данных системы iBank2.
- Хищение у юридических и физических лиц.
- Сравнительно небольшая общая сумма хищения (до 1 млн рублей).

BIFIT

8. Случай 3


Банк
Сервер БД ДБО
АРМ
Конфигуратор
системы
Зараженный сайт
Злоумышленник

9. Результат аудита

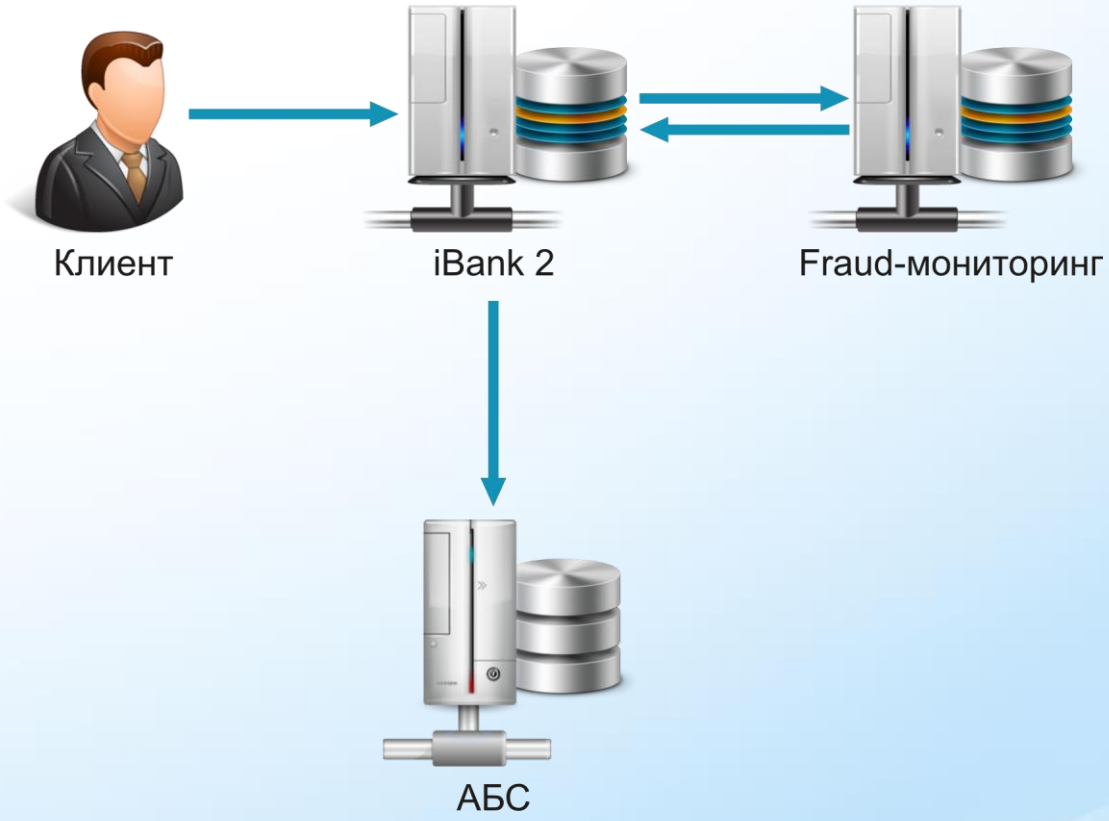


10. Что делать?

- Аудит
- Тестирование на проникновение
- Обучение сотрудников
- Использование программных и технических средств защиты информации
- Мониторинг
- Application Firewall
- Антифрод

BIFIT

11. Антифрод – еще одна ступень защиты



12. Как бы сработал антифрод в случае 1

1. Анализ окружения клиента
   - Новое устройство
   - Новые параметры сети
2. Анализ платежного документа
   - Новый ключ электронной подписи
   - Новый получатель
3. Анализ рабочего места администратора и операциониста
   - Зловредная программа на рабочем месте
   - Удаленный доступ к рабочему месту

BIFIT

13. Как бы сработал антифрод в случае 2

1. Анализ окружения клиента

- Зловредная программа на рабочем месте клиента

3. Анализ рабочего места администратора и операциониста

- Зловредная программа на рабочем месте сотрудника банка

14. Как бы сработал антифрод в случае 3

1. Анализ окружения клиента

    - Новое устройство

    - Новые параметры сети

2. Анализ платежного документа

    - Новый ключ электронной подписи

    - Новый получатель

15. Что дальше? Планы БИФИТ

1. Улучшение защиты системы iBank 2 на стороне банка
    - Защита базы данных системы iBank 2
    - Улучшение защиты рабочих мест сотрудников банка
    - Определение факта удаленного управления

2. Информирование банков об актуальных угрозах
    - Рассылка
    - Вебинары

3. Рекомендации банкам по построению защищенной инфраструктуры применительно к системе iBank 2.

Вопросы

Левин Алексей
levin@bifit.com

BIFIT

VII Уральский форум
«Информационная безопасность банков»

Fraud-мониторинг для ДБО.

Повышение эффективности и противостояние угрозам банковского фрода.

Левин Алексей
levin@bifit.com

BIFIT