Digital Security

Типовые уязвимости систем ДБО

Алексей Тюрин

к.т.н., руководитель департамента аудита ИБ

Digital Security

ДБО защищены?

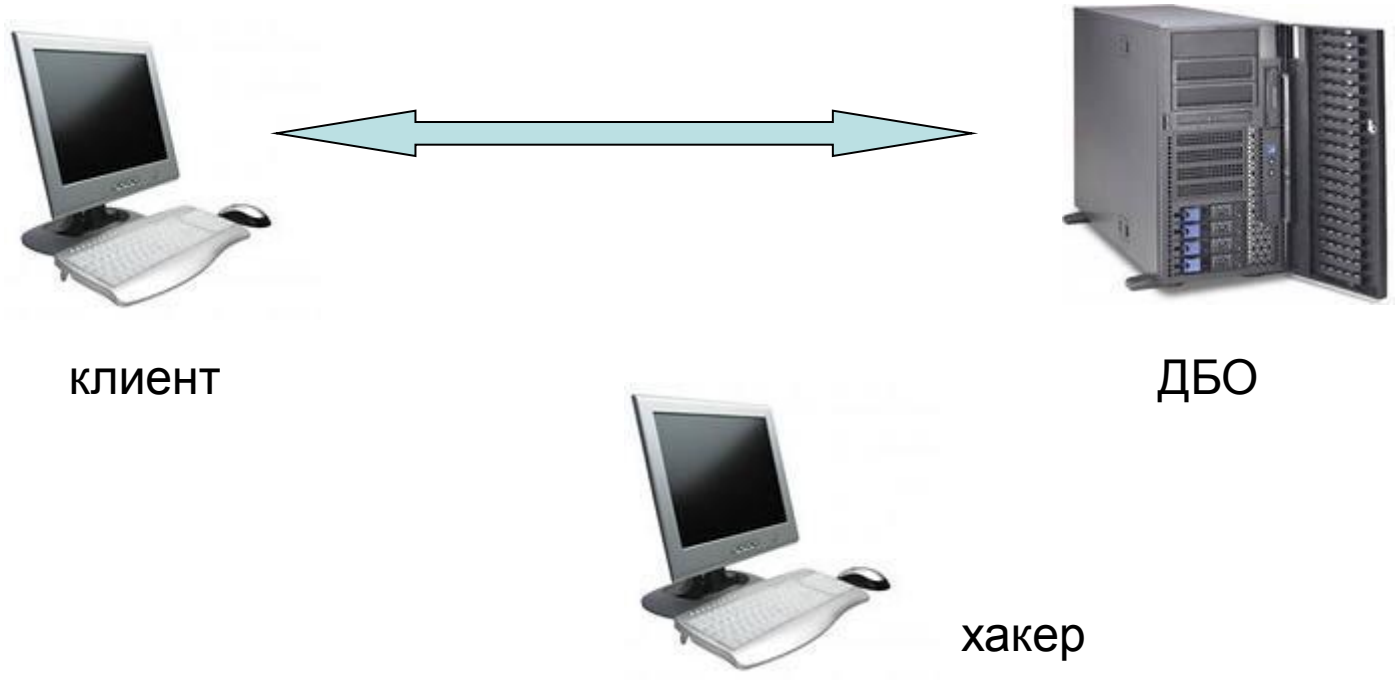
1) Мы имеем опыт проведения тестов на проникновение почти всех систем ДБО, представленных на российском рынке.

2) В ходе работ были выявлены множественные уязвимости в каждой из систем ДБО.

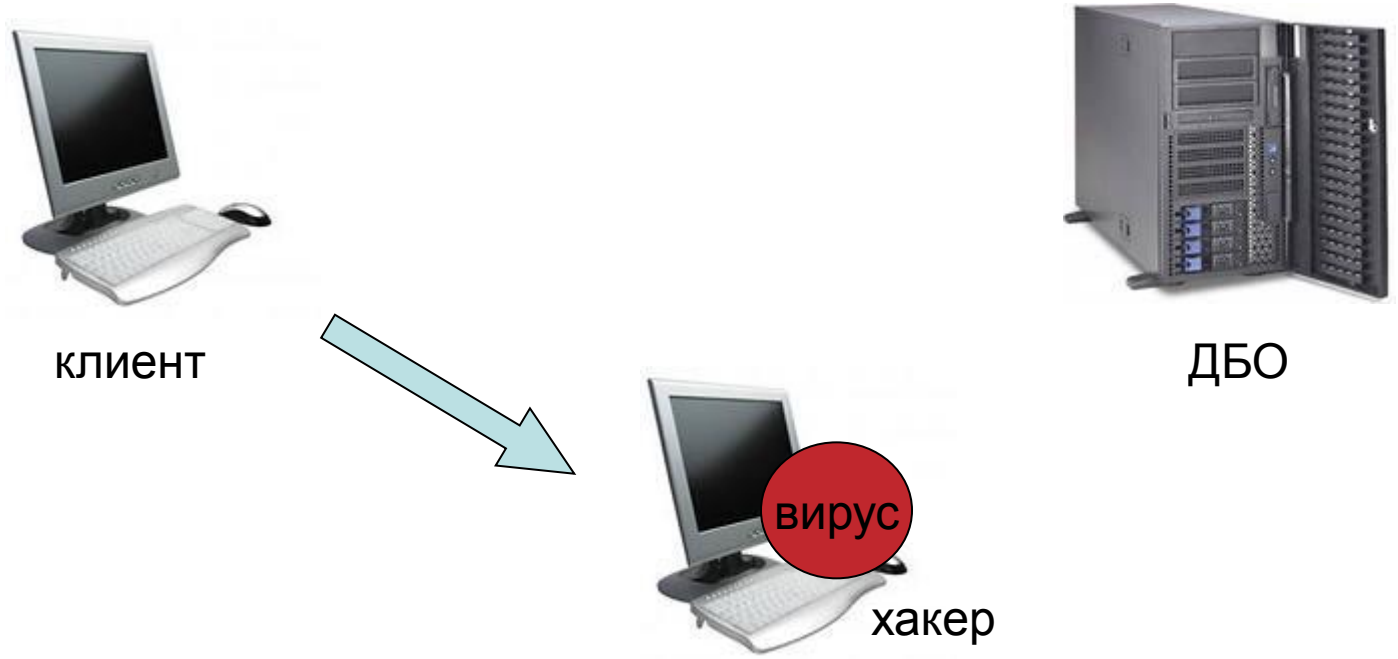
3) В результате **всех работ** были выявлены векторы атак, с помощью которых можно украсть деньги у клиентов банков (иногда – **у всех клиентов**!)

ActiveX. Пример 1. Заражение клиента банковским трояном

ActiveX-компоненты – специальные надстройки, устанавливаемые в браузер (ОС) для взаимодействия с ЭЦП и токенами у клиента банка.

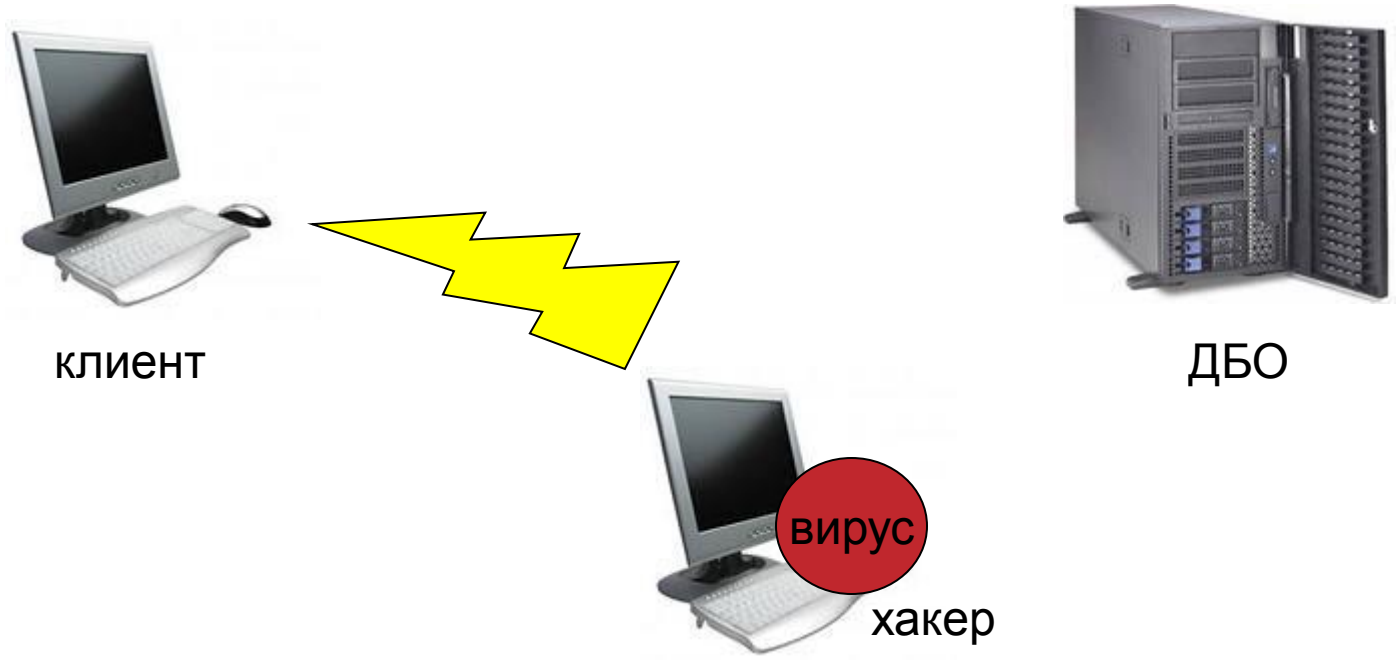


ActiveX. Пример 1. Заражение клиента банковским трояном



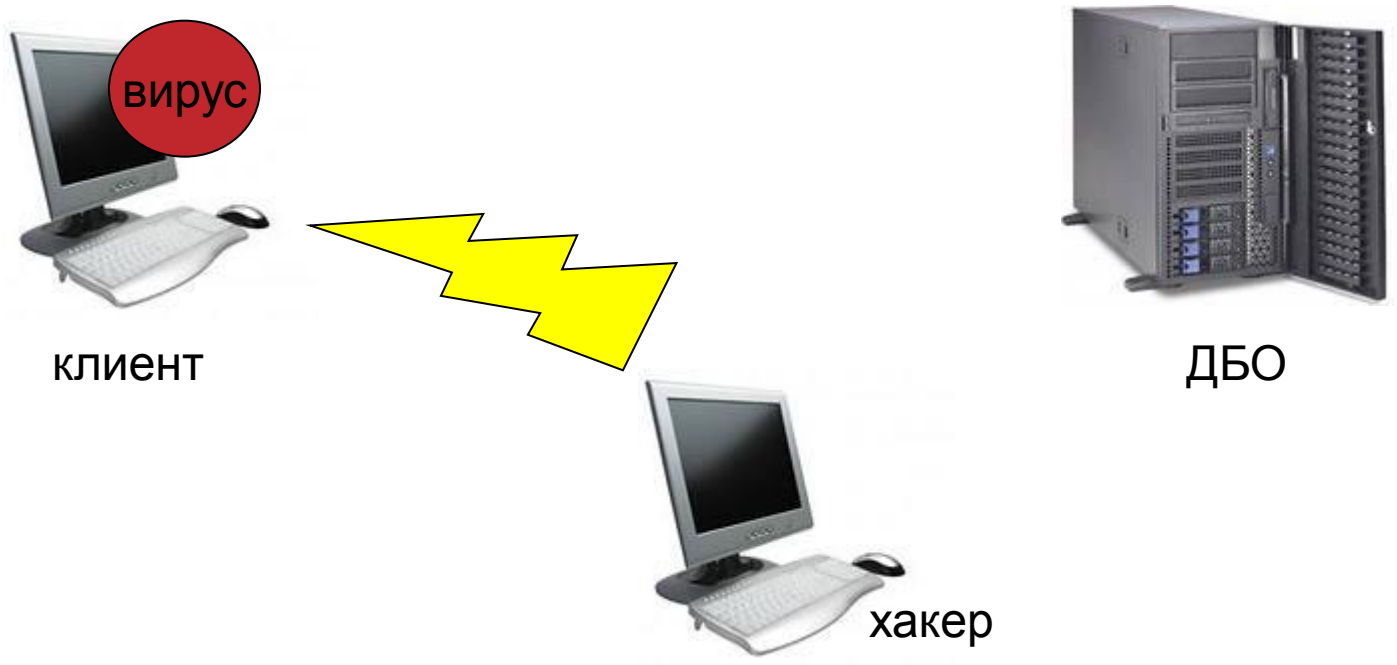
Вирус у клиента = полный контроль над клиентом = кража денег у клиента

ActiveX. Пример 1. Заражение клиента банковским трояном



Вирус у клиента = полный контроль над клиентом = кража денег у клиента

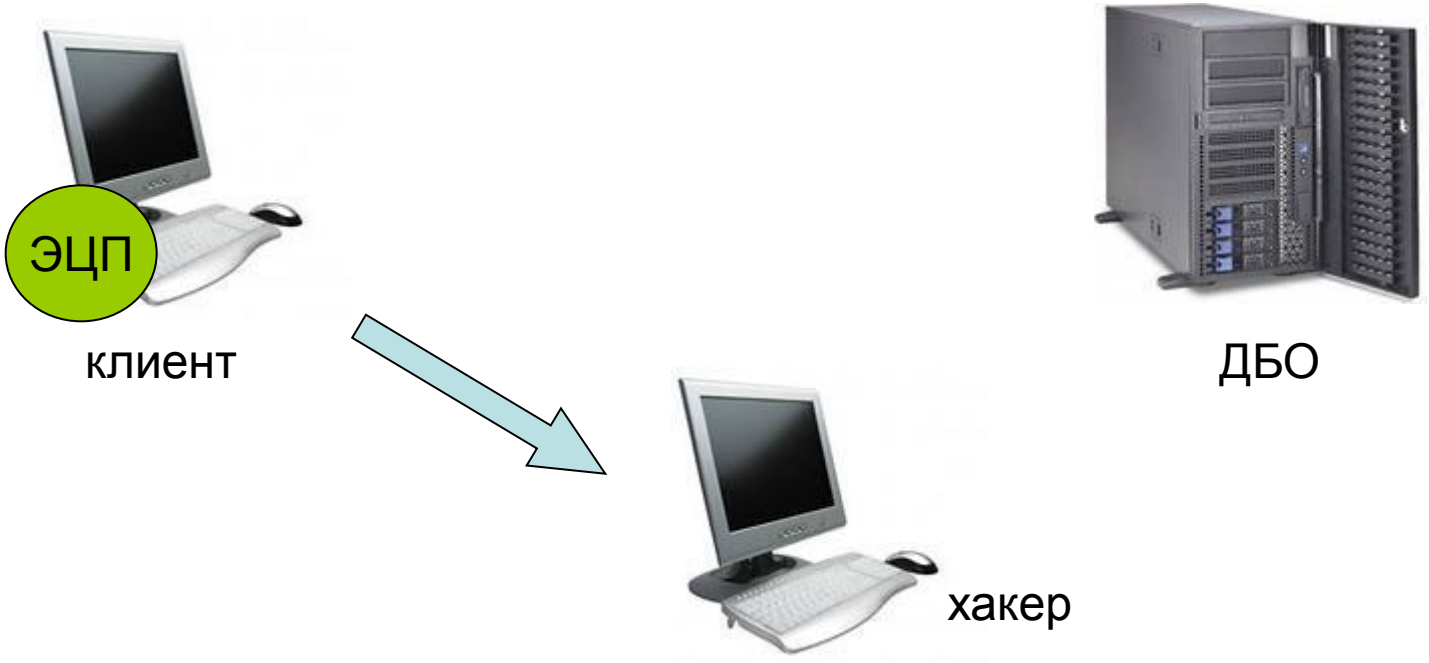
ActiveX. Пример 1. Заражение клиента банковским трояном



Вирус у клиента = полный контроль над клиентом = кража денег у клиента

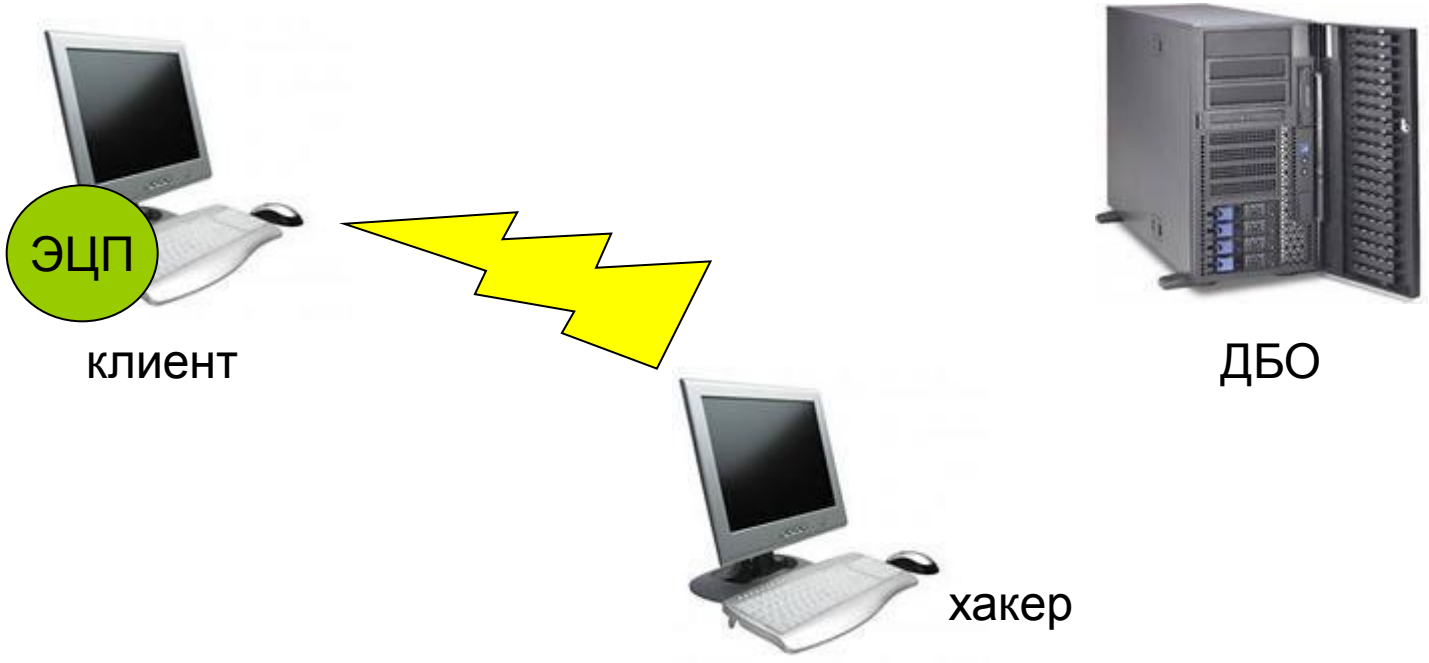
ActiveX. Пример 2. Кража ЭЦП клиента через ActiveX

Все еще не используете токены? Тогда мы идем к вам!



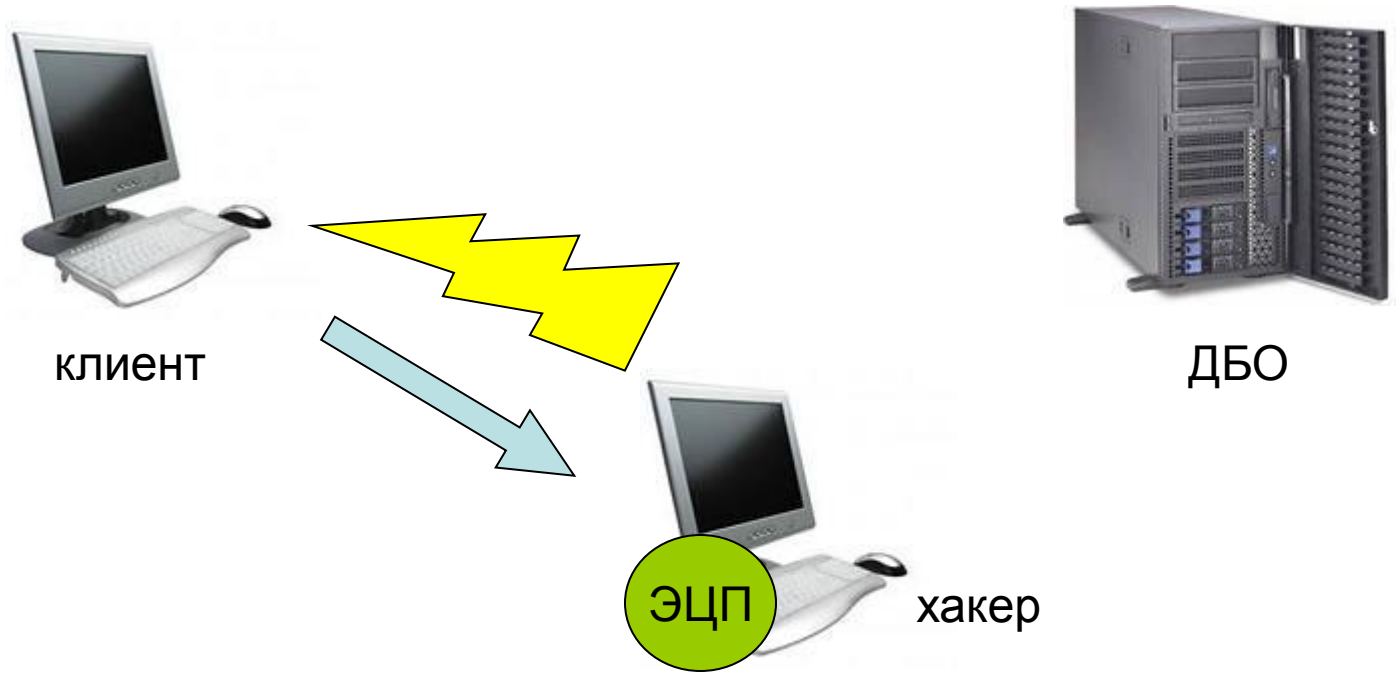
ActiveX. Пример 2. Кража ЭЦП клиента через ActiveX

Все еще не используете токены? Тогда мы идем к вам!



ActiveX. Пример 2. Кража ЭЦП клиента через ActiveX

Все еще не используете токены? Тогда мы идем к вам!



«Заманиваем» клиентов

Любой сайт

клиент

хакер

ДБО защищены?

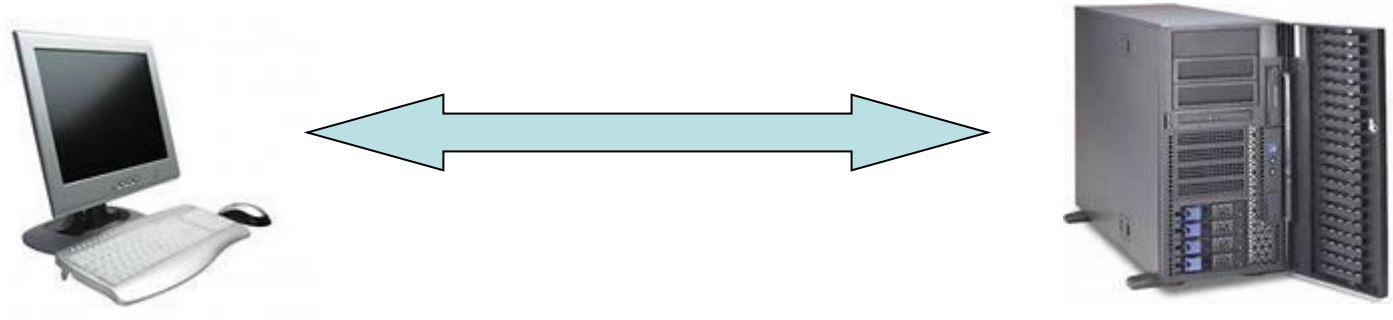
В 99% компонентов ActiveX различных систем ДБО нами были выявлены критичные уязвимости!

Почему?

1) Не поставлен процесс тестирования и анализа безопасности у разработчиков систем ДБО

2) Уязвимости в ActiveX не так знакомы программистам, как уязвимости из OWASP TOP 10

Пример 3. Внутри банка. Насколько вы доверяете вашим операторам?

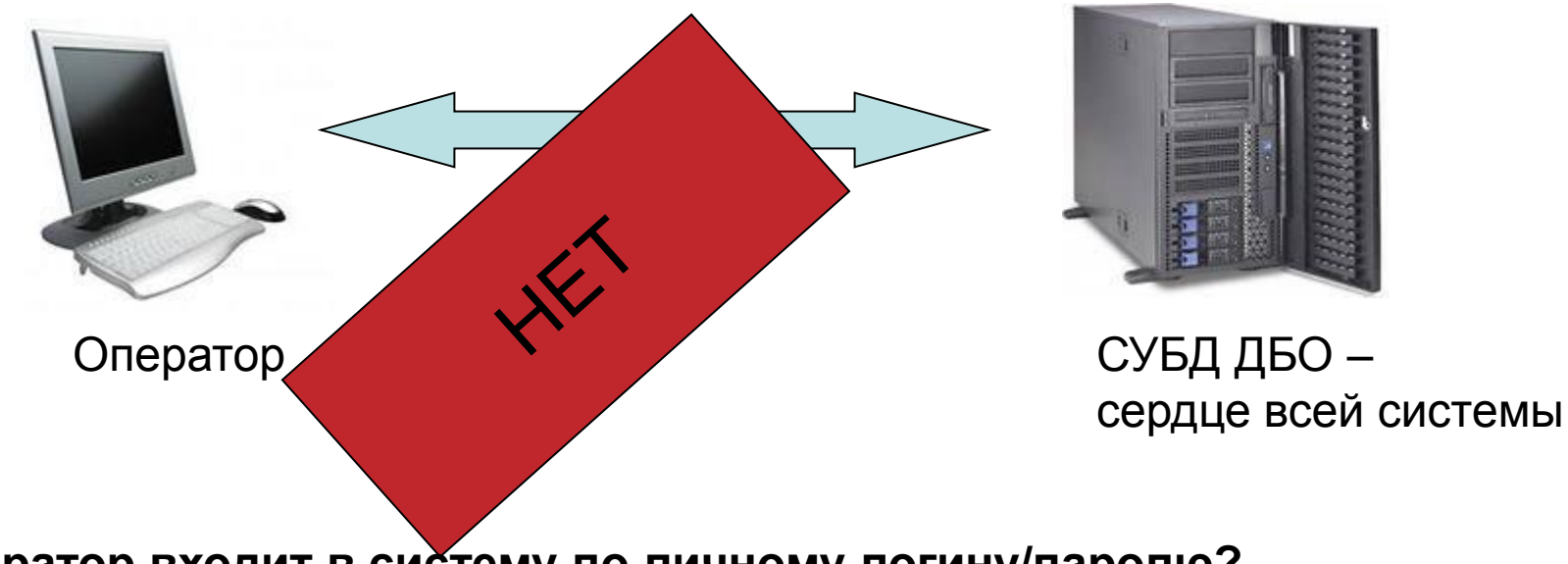


Оператор

СУБД ДБО –
сердце всей системы

Оператор входит в систему по личному логину/паролю.
Есть ролевая модель (администраторы, операторы).

Пример 3. Внутри банка. Насколько вы доверяете вашим операторам?



Оператор входит в систему по личному логину/паролю?
Есть ролевая модель (администраторы, операторы)?

Пример 3. Внутри банка. Насколько вы доверяете вашим операторам?

Оператор

Логин и пароль от dba

СУБД ДБО –
сердце всей системы

1) Оператор входит под привилегированной учетной записью СУБД.
2) Оператор ограничен на клиентской стороне возможностями в интерфейсе АРМ.
3) Зашифрованный пароль хранится в текстовом файле.

Пример 3. Внутри банка. Насколько вы доверяете вашим операторам?

Оператор

Логин и пароль от dba

СУБД ДБО –
сердце всей системы

1) Опе
2) Опе
интер
3) Защ

ью СУБД.
ми в

1) Общеизвестная специфика системы
2) Пароль от СУБД зашифрован

ДБО защищены?

1) Общеизвестная специфика системы
2) Пароль от СУБД зашифрован

Пароль от СУБД зашифрован – **это защита?..**

1) Зашифрованное – можно расшифровать.

2) Файл с паролем от привилегированной учетной записи СУБД ДБО должен быть доступен для чтения оператору.

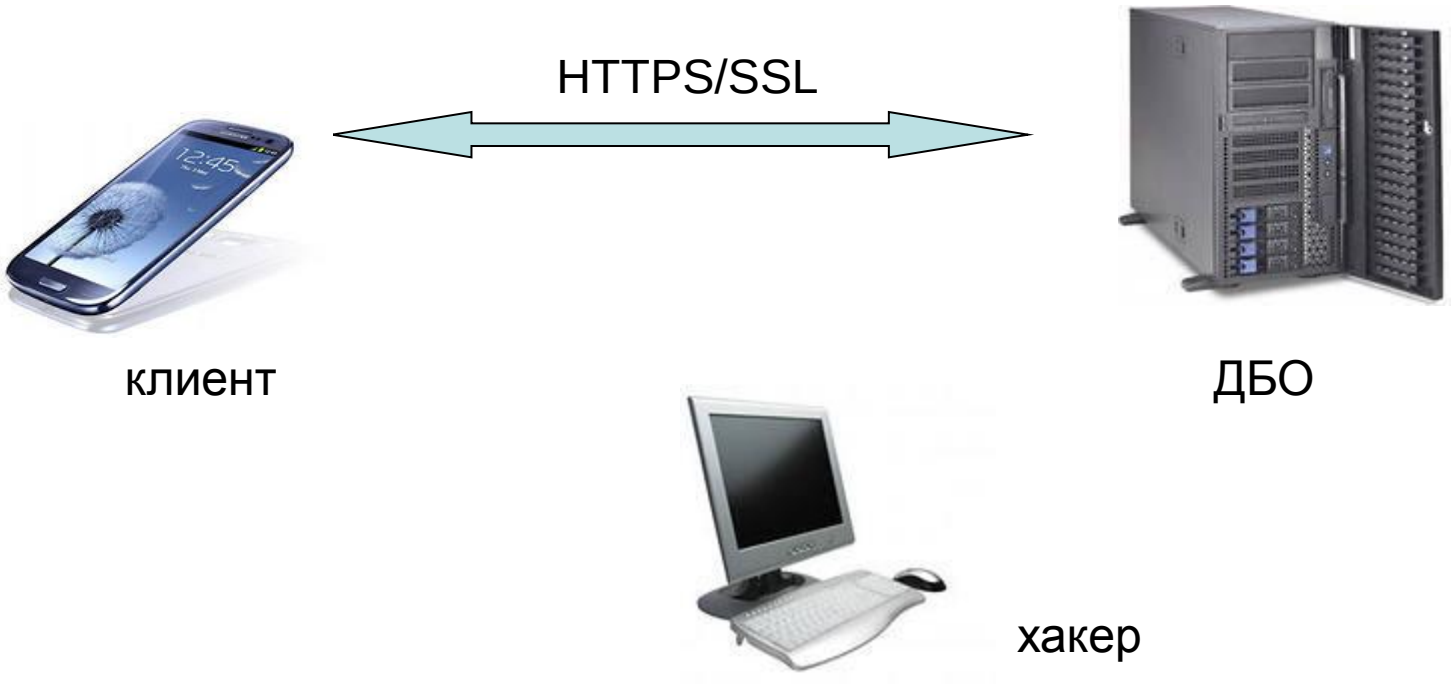
ДБО защищены?

Насколько вы доверяете вашим операторам?

Оператор = > Администратор СУБД ДБО = > Возможность украсть деньги у любого клиента банка

*Но построить защищенную систему можно (подробности лично, после выступления).

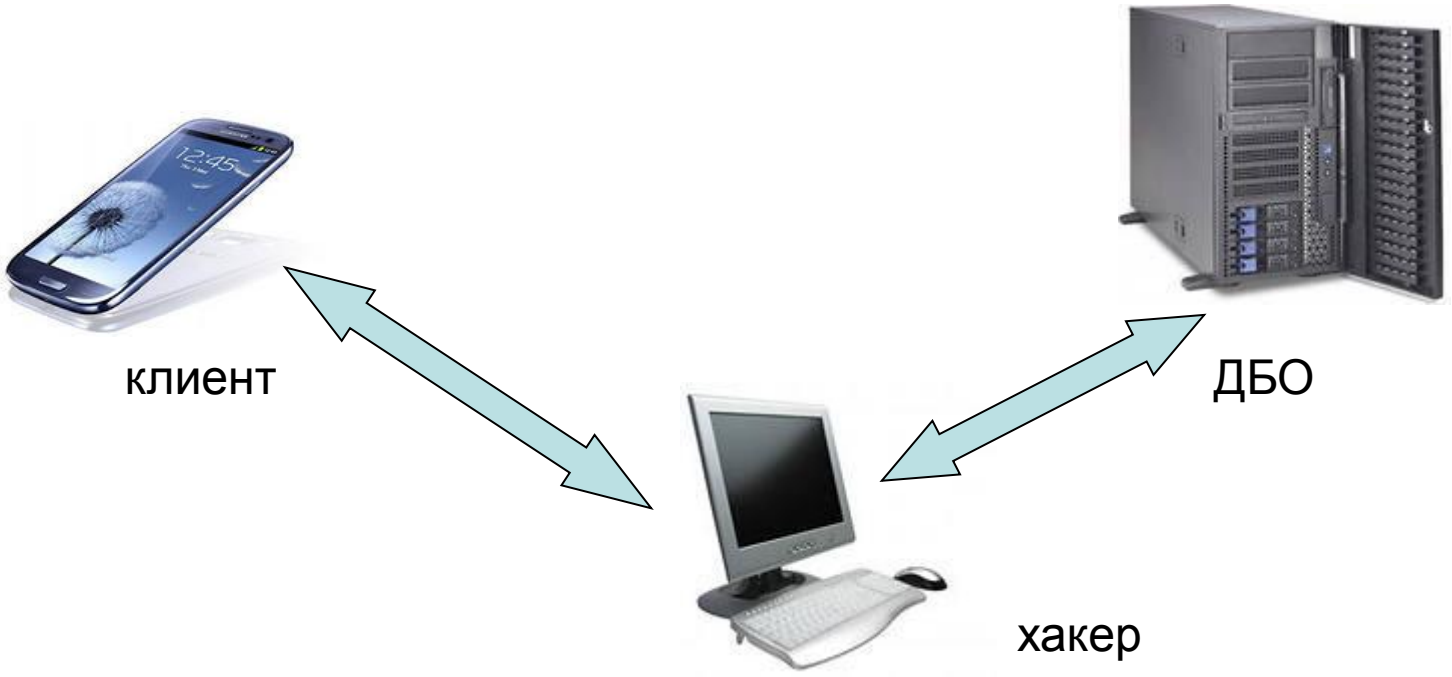
Пример 4. Мобильный банк. Атака типа «человек посередине» (MiTM)



Пример 4. Мобильный банк. Атака типа «человек посередине» (MiTM)

Пример 4. Мобильный банк. Атака типа «человек посередине» (MiTM)

Уязвимости, связанные с SSL (самоподписанные сертификаты, некорректная проверка имён хостов и т. д.) – примерно в 10-15% приложений



*Подробнее в исследовании Digital Security «Анализ безопасности мобильных банковских приложений за 2012 год»

Пример 4. Мобильный банк. Атака типа «человек посередине» (MiTM)

Хакер имеет полный контроль над трафиком между ДБО и клиентом =>
=> **кража аутентификационных данных, кража денег клиента**

*Подробнее в исследовании Digital Security «Анализ безопасности мобильных банковских приложений за 2012 год»

Пример 5. Опасные XSS

В 95% систем ДБО были выявлены уязвимости, позволяющие злоумышленнику внедрять свой код JavaScript (XSS).

Не слишком ли много для столь критичного продукта?

XSS позволяет полностью контролировать то, что отображается у пользователя, и то, что отправляется на сервер.

Злоумышленник может эмулировать действия клиента.
Злоумышленник может обойти защиту с использованием токенов.

Пример 5. Опасные XSS

хакер

клиент

браузер

ДБО

Пример 5. Опасные XSS

хакер

XSS

клиент

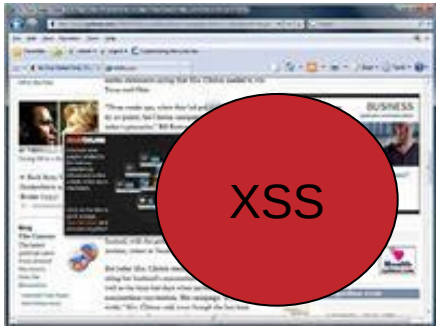
браузер

ДБО

Пример 5. Опасные XSS

хакер

клиент



браузер

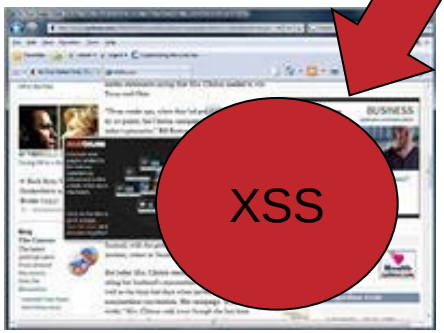
ДБО

Пример 5. Опасные XSS

Удаленное управление,
подмена отображаемых данных
=> **Кража денег**

хакер

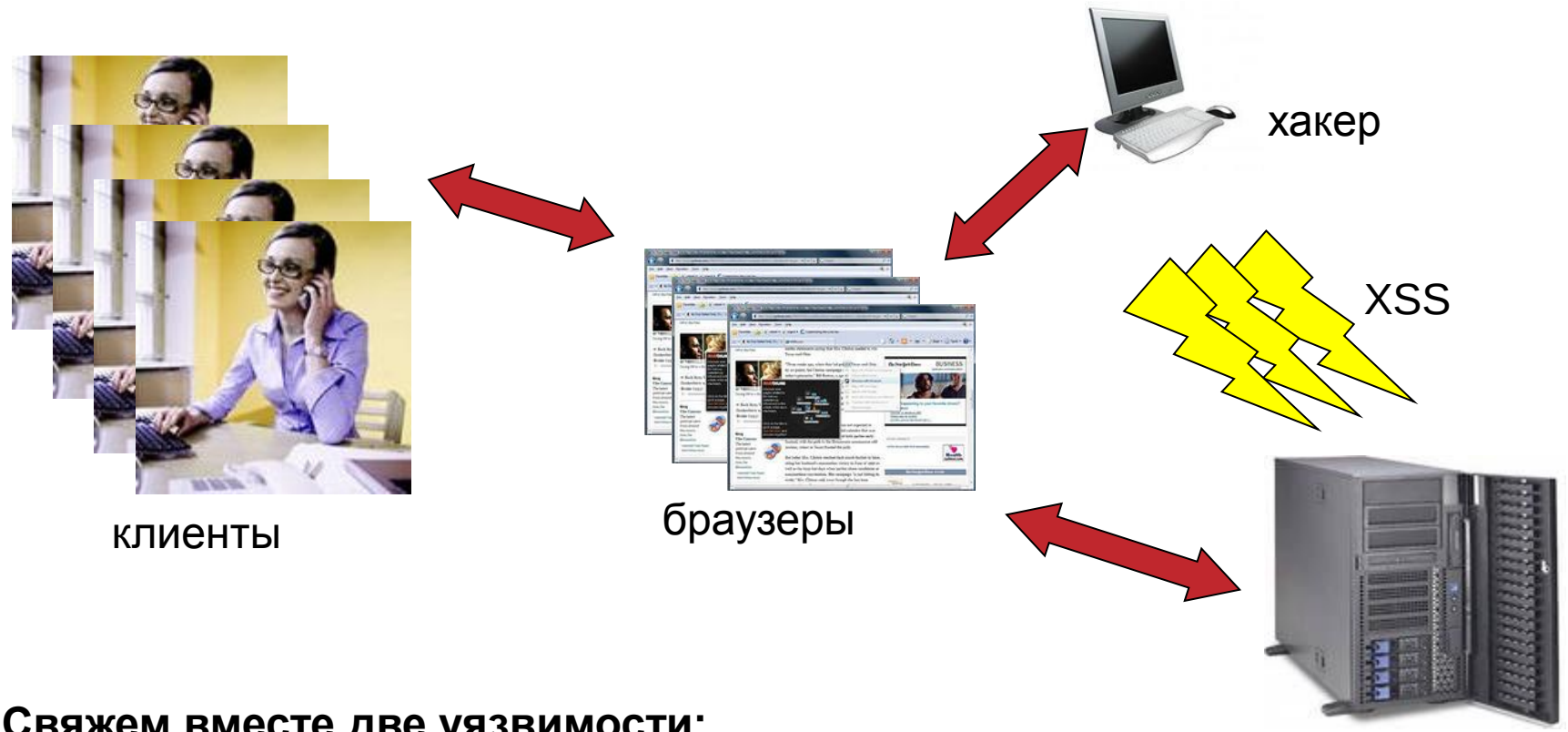
клиент



браузер

ДБО

Пример 5. Опасные XSS



Свяжем вместе две уязвимости:

1) Хранимая XSS

2) Некорректное разграничение доступа между клиентами

Пример 5. Опасные XSS

кли

Хранимая XSS + Некорректное разграничение доступа =
Заражение всех клиентов банка JavaScript-кодом

КРАЖА ДЕНЕГ У ВСЕХ/ЛЮБОГО КЛИЕНТА БАНКА

Присутствует в 10-15% систем ДБО!

ДБО

Свяжем вместе две уязвимости:

1) Хранимая XSS
2) Некорректное разграничение доступа между клиентами

Digital Security

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

www.twitter.com/antyurin
a.tyurin@dsec.ru