

# **Системы электронного голосования**

А.В.Лунин  
ОАО «ИнфоТеКС»

29 января 2011 г.

# **Идея компьютеризации избирательного процесса**

патент 90.446

Томас Эдисон

«электронное устройство для  
голосования»

1869 год, штат Массачусетс

# Широкое внедрение систем электронного голосования

## ПОЗВОЛИТ:

- повысить оперативность подсчета результатов голосования,
- уменьшить накладные расходы на проведение выборов,
- увеличить явку избирателей,
- облегчить участие в выборах граждан, находящихся за границей, а также избирателей с ограниченными возможностями.

# Угрозы

- форсированное внедрение недостаточно защищенных технических решений в масштабах страны и чрезмерная степень «доверия» электронике со стороны официальных лиц имеет или потенциально может иметь серьезные негативные последствия, подрывающие доверие граждан к избирательному процессу

# Этапы процедуры электронного голосования

## Дистанционное электронное голосование

### ШАГ 1

#### Регистрация

(получение возможности использовать ДЭГ)



мобильный телефон



персональный компьютер



терминал электронных социальных карт

### ШАГ 2

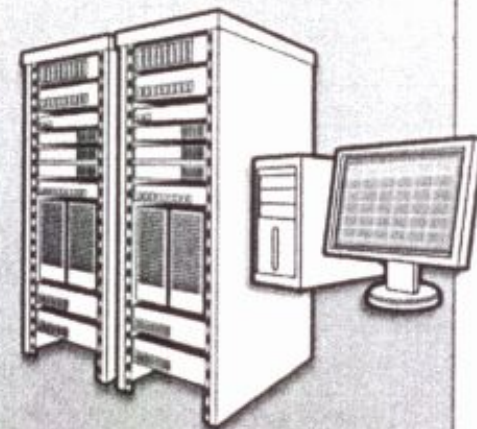
#### Голосование

1. Активация технического средства голосования
2. Получение электронного бюллетеня
3. Выбор альтернативы.
4. Подтверждение выбора.
5. Отправка голоса для регистрации и подсчета



### ШАГ 3

#### Регистрация и подсчет голосов



Комплекс обработки данных избирательной комиссии

Под *электронным голосованием (electronic voting, e-voting)* понимается процесс голосования, в котором электронные технические средства используются по крайней мере на этапе подачи голоса.

(определение, данное Советом Европы)

Схемы электронного голосования можно условно разделить на:

*традиционные (conventional)* (где голосование производится на избирательных участках, оборудованных специальными техническими средствами)

*удаленные (remote)* (не требующие личной явки избирателя на избирательный участок).

# *протоколы электронного голосования*

Участвуют:

- *избиратель или пользователь (voter, user);*
- *клиент (client application);*
- *сервер регистрации (registration server);*
- *сервер анонимизации (anonymization server);*
- *сервер подсчета голосов (vote counting server).*

# *требования к протоколам электронного голосования*

- *анонимность (privacy);*
- *корректность (eligibility, correctness, integrity);*
- *честность (fairness);*
- *верифицируемость (verifiability);*
- *всеобщая верифицируемость (universal verifiability);*
- *устойчивость (robustness);*
- *невозможность контроля (receipt-freeness):.*



# *специфические угрозы, которым подвергаются данные протоколы*

- нарушение конфиденциальности;*
- фальсификация результатов со стороны избирательной комиссии;*
- скупка голосов.*

# *Выявленные проблемы при разработке протоколов*

- теоретическое обоснование стойкости протокола с точки зрения требований по информационной безопасности опирается на предположения, которые трудно реализовать на практике
- протокол обладает высокой (с точки зрения эксплуатируемых технических средств) коммуникационной сложностью

# *протокол электронного голосования формализуется следующим образом*

Пусть имеется  $m$  участников многостороннего протокола – избирателей  $V_i$ ,  $i=1, \dots, m$ , каждый из которых вырабатывает свой секрет  $x_i$ .

Необходимо вычислить функцию  $f$ , зависящую от этих величин, не разглашая ни одной из них, но делая значение функции  $f$  общедоступным.

Для определенности каждый отдельно взятый случай применения схемы электронных выборов будем называть электронным голосованием.

$n$  – число государственных избирательных комиссий  $C_1, \dots, C_n$ .

# ***Известные схемы ЭГ***

- Схема электронных выборов Merritt, основана на асимметричном шифровании.*
- Схема электронных выборов Cramer-Franklin-Schoenmakers-Yung, основана на функции хэширования.*
- Гомоморфная схема депонирования бюллетеней Педерсена, основана на дискретном логарифмировании.*

# **Проблема возможного контроля над избирателями**

*Две потенциально возможные ситуации.*

- **Первая – принуждение избирателя совершается до начала голосования.**

*Возможная защита – аппаратный ДСЧ*

- **Вторая - кто-то пытается контролировать волю избирателя после голосования.**

*Возможная защита – отказуемое шифрование (*deniable encryption*)*

# Пример способа тайного голосования, обеспечивающий высокую достоверность результатов

# Патент на изобретение №2242793

## Способ электронного голосования

Патентообладатель: ОАО «ИнфоТеКС»

Приоритет изобретения 06 февраля 2003 г.

Зарегистрировано 20 декабря 2004 г.

# Типовое представление результатов тайного голосования

## Общие итоги

<b>Проголосовало</b>	<b>5</b>
<b>За Блюз</b>	<b>3</b>
<b>За Джаз</b>	<b>2</b>

## Список проголосовавших

**Голосующий 1**  
**Голосующий 2**  
**Голосующий 3**  
**Голосующий 5**  
**Голосующий 6**



# Типовое представление результатов поименного голосования

## Общие итоги

<b>Проголосовало</b>	<b>5</b>
<b>За Блюз</b>	<b>3</b>
<b>За Джаз</b>	<b>2</b>

## Персональные результаты

<b>Голосующий 1</b>	<b>Блюз</b>
<b>Голосующий 2</b>	<b>Блюз</b>
<b>Голосующий 3</b>	<b>Джаз</b>
<b>Голосующий 5</b>	<b>Блюз</b>
<b>Голосующий 6</b>	<b>Джаз</b>

# Основная проблема существующих способов голосования заключается в противоречии между следующими двумя требованиями

- Достоверность результатов голосования
- Тайна голосования

# Представление результатов голосования для предлагаемого способа

## Общие итоги

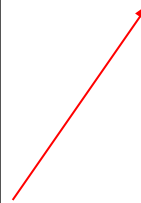
Проголосовало всего	5
За Блюз	3
За Джаз	2

## Список проголосовавших

Голосующий 1
Голосующий 2
Голосующий 3
Голосующий 5
Голосующий 6

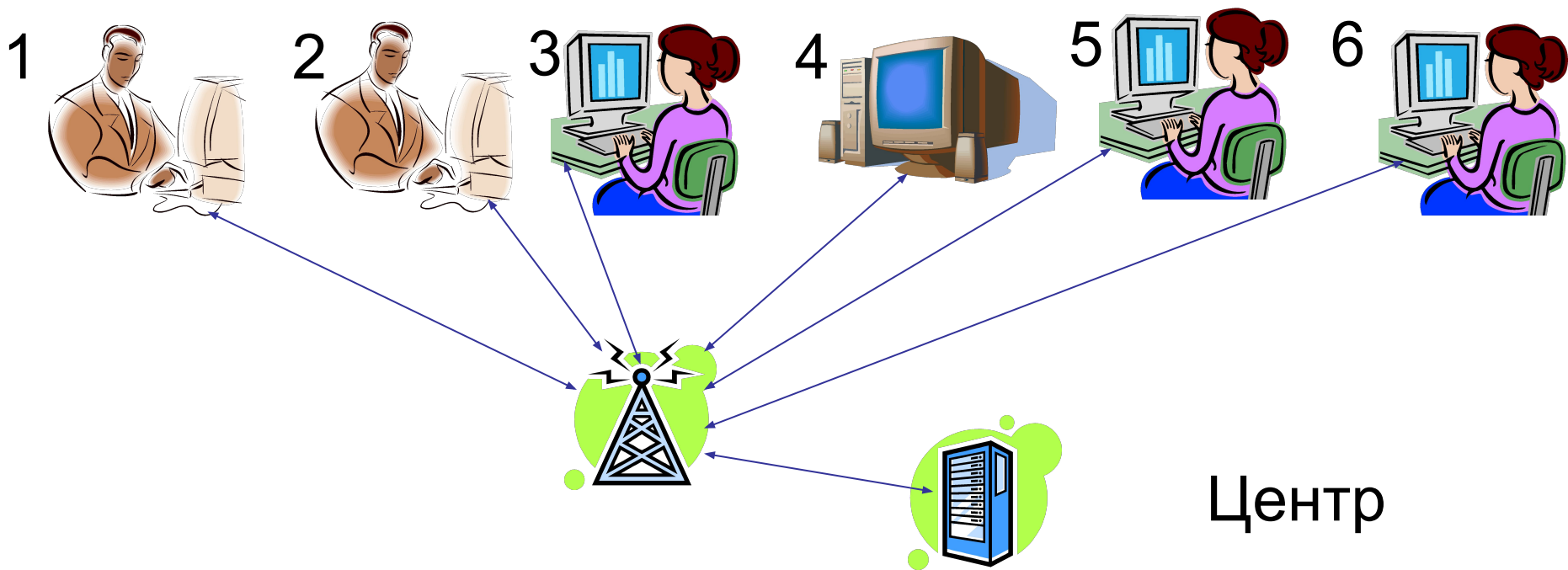
## Персональные результаты

акд513	Блюз
дсв863	Джаз
мсф338	Джаз
нтр452	Блюз
юкс725	Блюз



# Техническое оснащение: компьютеры, сетевое оборудование, специальное ПО, ЭЦП

Голосующие



# Центр получает от голосующего следующую информацию

Сохраняется в Центре



Голосующий 1

Голосовал	Голосующий 1
Выбор	Блюз
Подпись	ЭЦП Голос. 1



Центр

Текущие  
результаты  
голосования

Блюз	х
Джаз	у

# Центр высылает голосующему свою КВИТАНЦИЮ

Сохраняется у голосующего

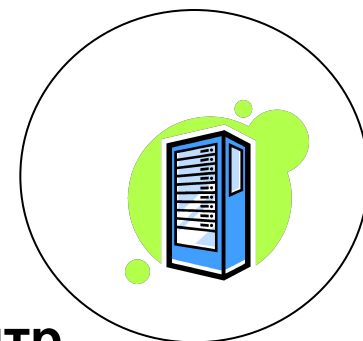
Сохраняется в Центре

Голосовал	Голосующий 1
Выбор	Блюз
Подпись	ЭЦП Голос. 1



Голосующий 1

Голосовал	Голосующий 1
Псевдоним	акд513
Выбор	Блюз
Подпись	ЭЦП Центра



Центр

акд513	Блюз
--------	------

Текущие  
результаты  
голосования

Блюз	х
Джаз	у

# Голосующий высылает Центру свою квитанцию

Сохраняется у голосующего

Голосовал	Голосующий 1
Псевдоним	акд513
Выбор	Блюз
Подпись	ЭЦП Центра

Сохраняется в Центре

Голосовал	Голосующий 1
Выбор	Блюз
Подпись	ЭЦП Голос. 1



Голосующий 1

Мой выбор зафиксирован правильно
ЭЦП Голосующего 1

Центр



акд513	Блюз
--------	------

Блюз	х+1
Джаз	у

Текущие  
результаты  
голосования

ИНФОФОРУМ

7 февраля 2011 г.

# Голосование закончено



## Голосующий 1

Голосовал	Голосующий 1
Псевдоним	акд513
Выбор	Блюз
Подпись	ЭЦП Центра



## Голосующий 6

Голосовал	Голосующий 6
Псевдоним	дсв863
Выбор	Джаз
Подпись	ЭЦП Центра

7 февраля 2011 г.



## Доступно всем

### Персональные результаты

акд513	Блюз
дсв863	Джаз
мсф338	Джаз
нтр452	Блюз
юкс725	Блюз

### Конечные результаты голосования

Блюз	3
Джаз	2

Проголосовали  
1, 2, 3, 5, 6



# Возможные злоупотребления

## ○ Злоупотребления Центра

- 1. Добавление неголосовавшего избирателя
- 2. Исключение голосовавшего избирателя
- 3. Изменение персонального результата

## ○ Злоупотребления избирателей

- 4. Избиратель ложно утверждает, что его выбор искажен
- 5. Избиратель голосовал, но утверждает, что не голосовал, и в список включен неправильно
- 6. Избиратель не голосовал, но утверждает, что голосовал, и в список не включен неправильно

# 1. Центр добавил неголосовавшего избирателя



Избиратель, добавленный в список (Голосующий 4), потребует предъявления своей квитанции

## Доступно всем

### Персональные результаты

акд513	Блюз
дсв863	Джаз
мсф338	Джаз
нтр452	Блюз
юкс725	Блюз
яку725	Джаз

### Конечные результаты голосования

Блюз	3
Джаз	3

Проголосовали  
1, 2, 3, 5, 6, 6

## 4. Избиратель ложно утверждает, что его выбор искажен



Центр

### Голосующий 1

Избиратель должен предъявить квитанцию Центра, в которой указан другой выбор голосующего

Голосовал	Голосующий 1
Псевдоним	акд513
Выбор	Джаз
Подпись	ЭЦП Центра

7 февраля 2011 г.

### Доступно всем

#### Персональные результаты

акд513	Блюз
дсв863	Джаз
мсф338	Джаз
нтр452	Блюз
юкс725	Блюз

#### Конечные результаты голосования

Блюз	3
Джаз	2

Проголосовали 1, 2, 3, 5, 6
--------------------------------

ИНФОФОРУМ

27

# **Задачи программы ускоренного технического переоснащения избирательной системы Российской Федерации (проект от 14 октября 2010 года)**

- создание системы дистанционного электронного голосования для реализации избирательных прав граждан, не имеющих возможности явиться на избирательный участок;

- дооснащение избирательных участков комплексами электронного голосования (КЭГ).

# Заключение

В настоящее время в мире не существует ни одной научно обоснованной и экспериментально отлаженной технологии электронного голосования, удовлетворяющей минимальным требованиям информационной безопасности.

# Заключение

Внедрение технологии электронного голосования в масштабах России является сложнейшей научно-технической задачей.

Потребуется разработать и теоретически обосновать протокол электронного голосования, использующий отечественные криптографические примитивы.

# Заключение

Необходима экспериментальная проверка функционирования системы на примере нескольких избирательных округов, начиная с использования ее для проведения муниципальных выборов, с переходом в случае положительных результатов эксперимента на региональный, и только потом – на федеральный уровень.

Спасибо за  
внимание!