Применение гомоморфных криптосистем в протоколах электронного голосования

Цель: исследование существующих систем электронного голосования, используемых в различных странах мира, разработка протокола и системы тайного электронного голосования.

Задачи:

- исследовать существующие протоколы и системы электронного голосования;
- разработать протокол и систему для проведения тайных электронных выборов;
- разработать соответствующее программное обеспечение;
- оценить экономический эффект от внедрения разработанной системы в процедуру выборов на территории РФ
- провести оценку качества разработанной системы.

Системы электронного голосования используются в 23 странах мира

Используемые протоколы

Слепая подпись

Основные недостатки:

- Высокий риск сговора ЦИК и ЦУР
- Медленная первоначальная настройка
- Большое количество сторон в процедуре голосования
- Высокий риск подделки подписи ЦИК злоумышленником

Микс-сети

Основные недостатки:

- Ненадежность узлов
- Медленная первоначальная настройка
- Большое количество сторон в процедуре голосования
- Высокий риск атаки «Человек посередине»
- Отсутствие конфиденциальности при малом числе избирателей
- Очень медленный подсчет результатов голосования

Новый подход к анонимизации голоса избирателя – **Гомоморфное шифрование**

Анонимность голоса достигается за счет обработки уже зашифрованного на стороне избирателя бюллетеня с помощью гомоморфных операций используемой криптосистемы.

Основные достоинства:

- Решает проблемы протоколов на основе слепой подписи и микс-сетей
- Всего две стороны в процедуре голосования: ЦИК и избиратель
- Эффективность вычислений
- Простота реализации
- Криптостойкость схемы зависит только от криптостойкости используемой криптосистемы
- Быстрый подсчет результатов голосования

Экспоненциальная версия ElGamal

Генерация ключевой пары:

1. Генерация двух больших простых чисел p и q. q – порядок группы G с генератором п.
2. Выбирается случайное число a $\in Z_q^*$
3. Вычисляется $y = g^a \bmod p$
4. Открытым ключом будет кортеж (y, p, q)
5. Закрытый ключ – число a.

Шифрование сообщения $m \in Z_q$:

1. Выбирается случайное число r $\in Z_q^*$
2. Вычисляется шифртекст как:

$$c = (\alpha, \beta) = (g^r (\bmod p), y^r g^m (\bmod p)$$

$c = (\alpha, \beta) = (g^r (\bmod p), y^r m (\bmod p)$ –обычная версия алгоритма.

Расшифровка шифртекста c:

$$g^m = \beta y^{-r} = \beta (g^a)^{-r} = \beta \alpha^{-a} \ (mod\ p)$$

Использование экспоненциальной версии алгоритма позволило мне применить аддитивный гомоморфизм для суммирования голосов, не рассекречивая их.

$$Enc(m_1) * Enc(m_2) = Enc(m_1 + m_2)$$

$$\prod c_i = \left(\prod g^{r_i}, \prod y^{r_i} g^{m_i}\right) = \left(g^{\sum r_i} \ (mod\ p), \quad y^{\sum r_i} g^{\sum m_i} \ (mod\ p)\right)$$

Для получения итогового результата $\sum m_i$, необходимо вычислить дискретный логарифм.

Доказательство знаний с нулевым разглашением

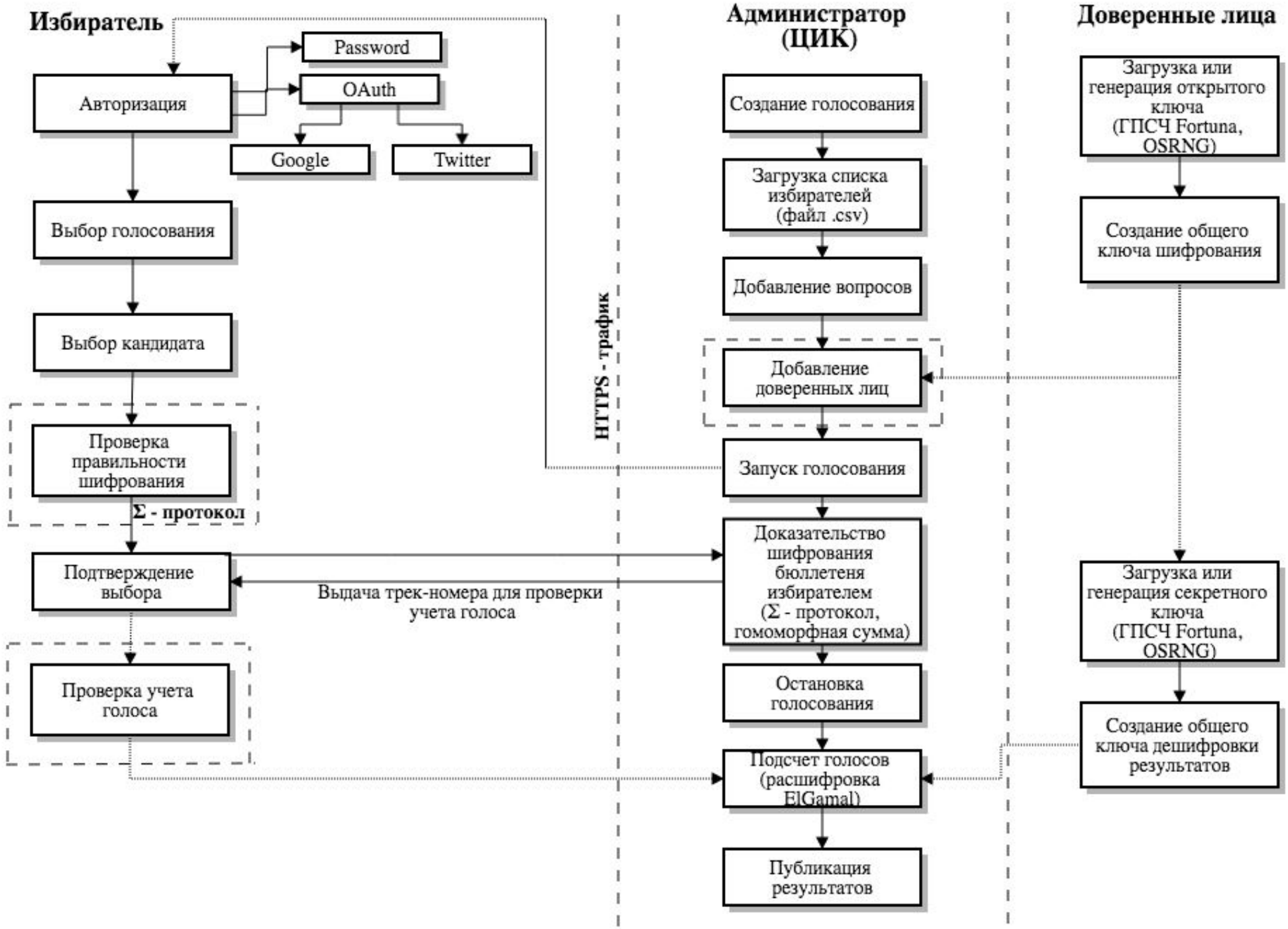
Необходимо для доказательства правильности шифрования бюллетеня избирателем (убедиться в том, что каждый шифртекст (зашифрованный вопрос и ответ в бюллетене избирателя) $c = (\alpha, \beta)$ содержит значение точно от 0 до q-1).

Для этого необходимо, чтобы удовлетворялось равенство логарифмов хотя бы для одного члена логической суммы:

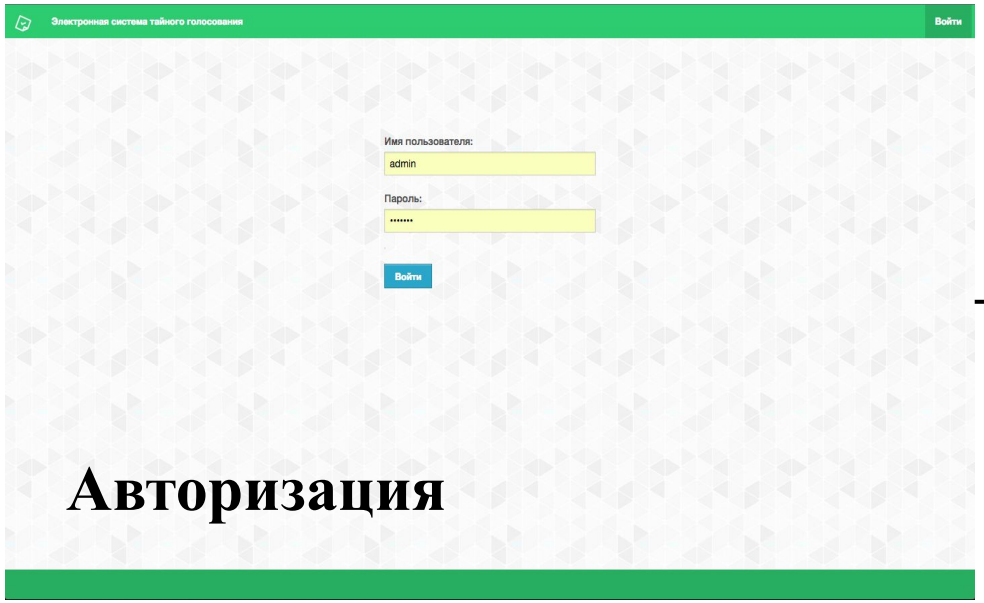
$$(\log_g \alpha = \log_y \beta) \vee (\log_g \alpha = \log_y \frac{\beta}{g}) \vee \ldots$$

$$\vee (\log_g \alpha = \log_y (\frac{\beta}{g^{q-1}}))$$

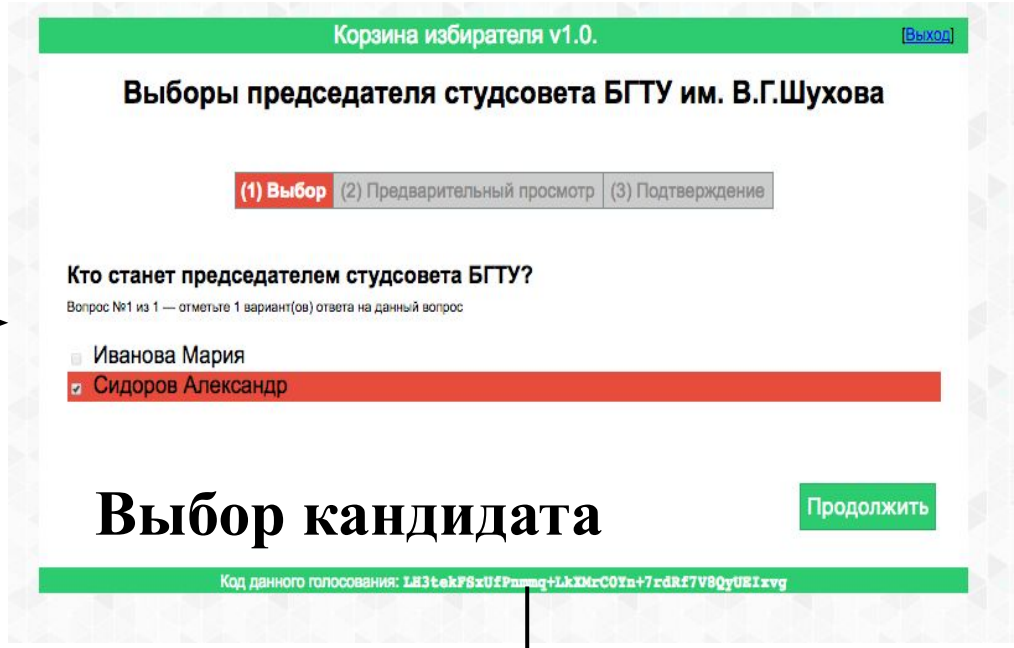
В разработанной системе я использовал Σ – протокол доказательства знаний с нулевым разглашением, который обладает необходимыми свойствами полноты, корректности и нулевого разглашения, которыми должны обладать протоколы доказательства нулевых знаний.


Избиратель
Password
OAuth
Авторизация
Google
Twitter
Выбор голосования
Выбор кандидата
Проверка правильности шифрования
Σ - протокол
Подтверждение выбора
Проверка учета голоса
HTTPS - трафик
Администратор (ЦИК)
Создание голосования
Загрузка списка избирателей (файл .csv)
Добавление вопросов
Добавление доверенных лиц
Запуск голосования
Доказательство шифрования бюллетеня избирателем (Σ - протокол, гомоморфная сумма)
Выдача трек-номера для проверки учета голоса
Остановка голосования
Подсчет голосов (расшифровка ElGamal)
Публикация результатов
Доверенные лица
Загрузка или генерация открытого ключа (ГПСЧ Fortuna, OSRNG)
Создание общего ключа шифрования
Загрузка или генерация секретного ключа (ГПСЧ Fortuna, OSRNG)
Создание общего ключа дешифровки результатов

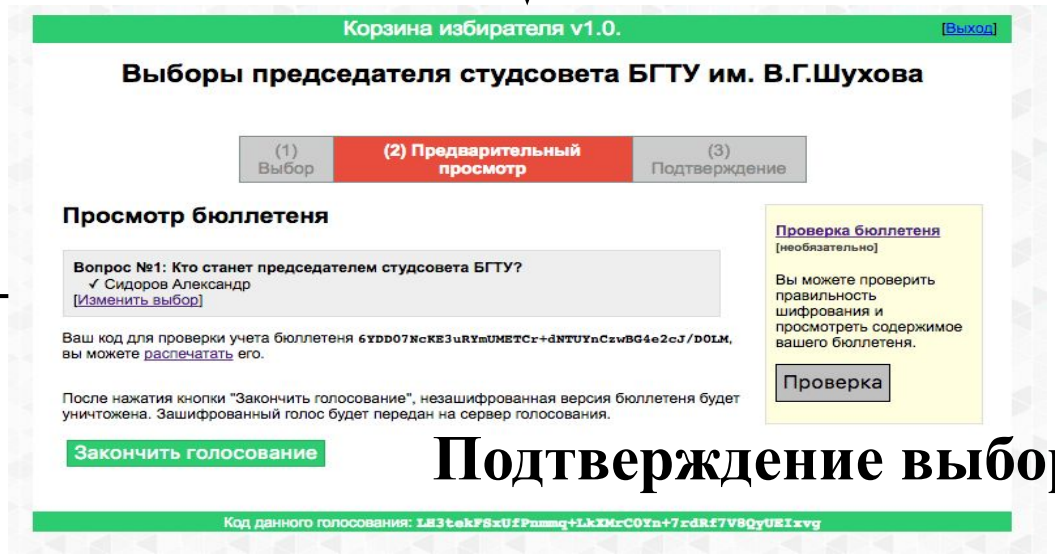
Голосование избирателя



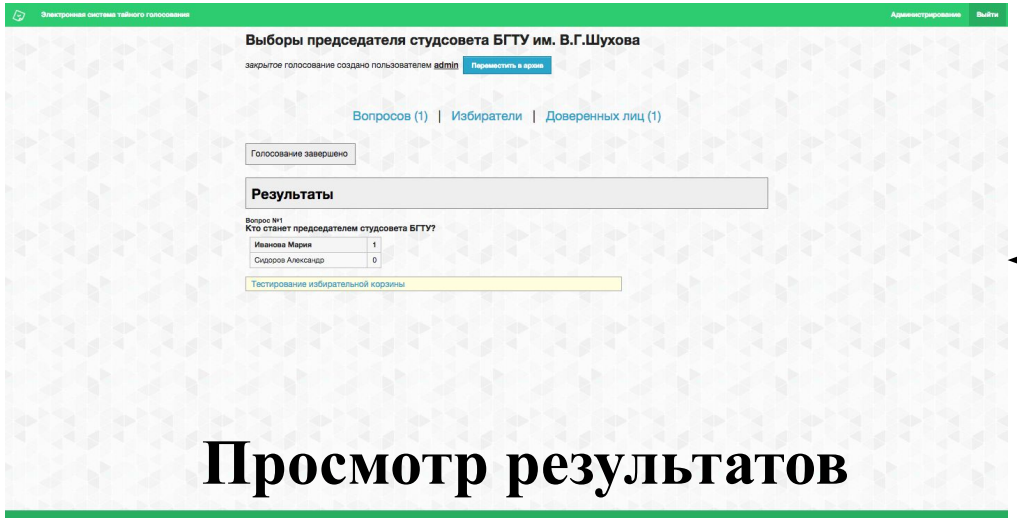
Авторизация



Выбор кандидата



Подтверждение выбора



Просмотр результатов

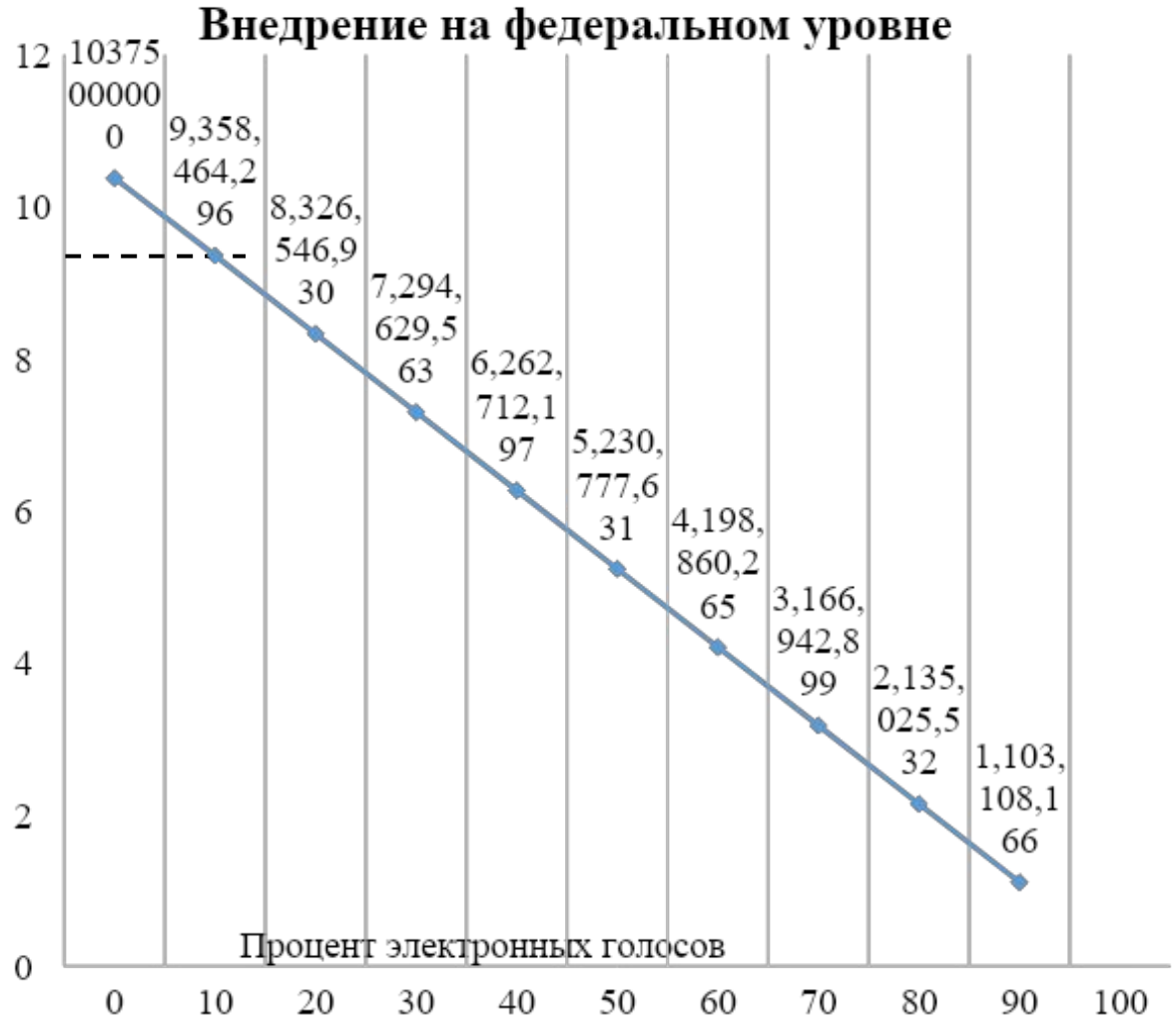
Сравнение созданной системы с уже существующими по основным свойствам электронных выборов

	Эстония	Франция	Норвегия	Разработанная система
Конфиденциальность голосования	+	+	+	+
Отслеживаемость голоса	-	-	-	+
Протокол голосования	слепая подпись	микс-сеть	микс-сеть	гомоморфное шифрование
Проверка правильности шифрования бюллетеня избирателем	+	-	+	+
Универсальная проверяемость	-	-	-	+
Анонимность при малом числе избирателей	-	-	-	+
Необходимость регистрации на процедуру голосования	+	-	+	+
Возможность изменения голоса избирателем	+	+	+	+

Стоимость внедрения на федеральном уровне

% избирателей, использующих систему	Стоимость проведения выборов стандартным способом, руб.	Стоимость проведения выборов с помощью системы, руб.	Полная стоимость выборов, руб.
10	9 351 343 496	7 120 800	9 358 464 296
20	8 312 305 330	14 241 600	8 326 546 930
30	7 273 267 163	21 362 400	7 294 629 563
40	6 234 228 997	28 483 200	6 262 712 197
50	5 195 190 831	35 586 800	5 230 777 631
60	4 156 152 665	42 707 600	4 198 860 265
70	3 117 114 499	49 828 400	3 166 942 899
80	2 078 076 332	56 949 200	2 135 025 532
90	1 039 038 166	64 070 000	1 103 108 166
100	0	71 173 600	71 173 600

Экономический эффект от внедрения системы



Результаты экспериментов на время выполнения этапов голосования

Число избирателей: 140 000
Доверенных лиц: 7
Кандидатов: 789
Тип выбора: 1 из 789

	Слепая подпись	Микс-сеть	Гомоморфное шифрование
Прогрев системы	**190,4 ч.**	20,9 ч.	**2,06 сек.**
Голосование	**21,4 сек.**	**0,009 сек.**	14,97 сек.
Доказательство шифрования бюллетеней	1,32 ч.	**14,08 мин.**	**44,1 ч.**
Подсчет результатов	25,63 сек.	**2,32 ч.**	**22,78 сек.**

Число избирателей: 27000
Доверенных лиц: 10
Кандидатов: 21
Тип выбора: 1 из 21

	Слепая подпись	Микс-сеть	Гомоморфное шифрование
Прогрев системы	1,81 м.	**4,42 ч.**	**0,6 сек.**
Голосование	**0,603 сек.**	**0,009 сек.**	0,411 сек.
Доказательство шифрования бюллетеней	31,93 мин	**2,77 мин.**	**2,36 ч.**
Подсчет результатов	1,89 сек.	**37,22 мин.**	**1,19 сек.**

Результаты работы

- Проанализированы существующие системы электронного голосования, определены их основные недостатки;
- Разработан протокол электронного голосования, позволяющий проводить анонимные выборы даже при малом количестве избирателей и обладающий свойством проверки учета голосов;
- Разработана демонстрационная система голосования, позволяющая проводить анонимные выборы с участием доверенных лиц, выполнять проверку правильности шифрования бюллетеня, а также проверку учета голоса избирателем.
- Разработаны модульные тесты, которые позволят найти и устранить ошибки при дальнейшем расширении системы;
- Доказана экономическая обоснованность процедуры электронного голосования на территории Российской Федерации;
- Доказано быстродействие работы системы при обработке данных избирателей для максимального количества избирателей на одну копию системы.

Благодарю за внимание!