Отзыв

на автореферат диссертации Салман Васан Давуд Салман на тему: Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере республики Ирак), представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Предлагаемая автором модель построена на основе распределенной сети узлов блокчейн-консорциума (БЧ) с использованием смарт-контрактов. При этом, для каждой провинции создается узел голосования. На каждый узел замыкаются избирательные участки и округа провинций. На узле голосования провинции есть несколько смарт контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка. Разработанный автором протокол системы дистанционного электронного голосования (ДЭГ) разработан с учетом особенностей угроз системе ДЭГ в арабских странах. В протоколе используется гомоморфное шифрование и схема распределенного дешифрования с использованием системы разделения секретного ключа. В работе также предложен метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом.

В первой главе представлен общий обзор существующих систем электронного голосования и определены специфические для Ирака необходимые свойства такой системы.

Во второй главе рассмотрена возможная модель системы электронного голосования для различных уровней и выбраны основные компоненты такой модели. В этой же главе в качестве базового криптографического примитива для реализации заявляемого протокола выбран алгоритм Эль Гамаля.

В третьей главе рассмотрен сам предлагаемый протокол голосования, описывается алгоритм шифрации бюллетеня и дешифрации его двух частей на БЧ и серверах голосования.

В четвертой главе рассмотрен вариант использования протокола аутентификации без разглашения для решения проблемы проверки правильности заполнения бюллетеня избирателем.

При общей положительной оценке диссертации необходимо отметить следующие недостатки:

1. По представленной формуле (3) не ясно каким образом формируется общий бюллетень избирателя при голосовании за/против нескольких кандидатов (важно отметить, что если для всех кандидатов используется одно и тоже случайное число r_i и один и тот же элемент G, как это указано в (3) , то узел БЧ легко определит результаты голосования избирателя).
2. Очевидно, что существенным недостатком схемы является необходимость решения задачи дискретного логарифма для определения результатов голосования за каждого из кандидатов.
3. Следует также отметить, что из имеющегося в автореферате описания оказывается, что узел БЧ должен быть доверенным узлом системы так как в соответствии с приведенным выше замечанием 1 на нем легко определить результат голосования каждого из избирателей.

Однако указанные замечания не снижают значимости и важности полученных результатов, и не оказывают существенного влияния на положительную оценку работы.

В целом, судя по автореферату, диссертация на тему «Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере республики Ирак)», представляет собой законченное научное исследование, содержащее новые варианты протокола электронного голосования, отвечает требованиям ВАК, предъявляемым к диссертационным работам, представляет практическую ценность, а ее автор – Салман Васан Давуд Салман, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

к.т.н., доцент ФБИТ
Угиверситет ИТМО

[redacted] Волошина Наталия Викторовна

«12» февраля 2024 г.

Наименование организации: федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО».
Адрес организации: 197101, Санкт-Петербург, Кронверкский пр., д. 49, лит. А,
Тел.: +7 (812) 607-02-83,
Факс: +7 (812) 232-23-07,
E-mail: od@itmo.ru .

Подпись Волошиной
удостоверяю
НАЧАЛЬНИК [redacted]
ШИПИК В.А.