Экз. № 1

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ИНСТИТУТ «РУБИН»
ИНН 7802776390/КПП 780201001
ул. Кантемировская, дом 5,
г. Санкт-Петербург, 194100, РФ
Тел.: +7 (812) 670-89-89,
Факс: +7 (812) 596-35-81,
E-mail: inforubin@rubin-spb.ru

«УТВЕРЖДАЮ»
Генеральный директор
АО «НИИ «Рубин»
[redacted] С.С. Степанов
« 22 » января 2024 г.

**ОТЗЫВ** [redacted]

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)», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

В современном мире голосования на различных уровнях общественной деятельности проводятся в электронном виде с использованием современных технологий, в том числе и открытой среды – Интернета. Это приводит к возникновению большого количества рисков для безопасности функционирования системы дистанционного электронного голосования (ДЭГ), поэтому исследование и создание безопасных систем ДЭГ является актуальной научно-практической задачей и определяет **актуальность диссертационной работы** Салман Васан Давуд Салман, в которой на опыте и примерах проведения выборов в республике Ирак предлагается перспективная защищенная система ДЭГ для использования на парламентских выборах в стране.

Наибольший научный и практический интерес представляют следующие положения работы, вынесенные на защиту, отвечающие **критерию научной новизны**:

- модель системы ДЭГ для арабских государств с парламентской правовой системой, основанная на распределенной сети блокчейн-узлов, объединяющей подсистемы ДЭГ провинций, построенные по принципу блокчейн-консорциума с использованием смарт-контрактов;

- протокол функционирования перспективной системы ДЭГ на основе гомоморфного шифрования с распределенным дешифрованием, учитывающий угрозы безопасности информации, актуальные для арабских государств, и обеспечивающий повышение защищенности от угроз, связанных с субъективным (человечески) фактором;

- метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом.

Научные результаты, полученные автором, отличаются от известных тем, что модель перспективной системы ДЭГ построена на основе распределенной сети узлов блокчейн-консорциума с использованием смарт-контрактов, ее протокол обеспечивает дополнительную защищенность за счет применения распределенного дешифрования, а метод проверки корректности заполнения бюллетеня обеспечивает скрытность суммарного числа голосов, блокируя таким образом атаки на систему ДЭГ.

**Теоретическая значимость исследования** заключается в применении в ходе решения научной задачи по созданию защищенной системы ДЭГ криптосистемы шифрования с единым ключом шифрования и разными ключами дешифрования, распределенными между независимыми серверами, а также в расширении класса используемых методов проверки корректности заполнения бюллетеня избирателем.

**Практическая значимость исследования** заключается в использовании при создании защищенной системы ДЭГ распределенной сети узлов блокчейн-консорциума с использованием смарт-контрактов и гомоморфного шифрования; подтверждении реализуемости протокола разработанной системы ДЭГ на макете; акте реализации Независимой Высшей избирательной комиссии республики Ирак; апробации полученных

результатов в ходе проведения большого количества научно-технических конференций различного уровня.

**Обоснованность и достоверность** полученных результатов обеспечивается применением апробированного математического аппарата, обоснованным выбором и полнотой исходных данных, корректностью вводимых ограничений и допущений, непротиворечивостью полученных теоретических результатов экспериментам, адекватностью разработанной модели системы ДЭГ специфике процесса голосования в арабских странах, результатами численных экспериментов по статистической оценке предложенных решений.

Перечень и хронология публикаций автора, включающие 13 печатных работ, в том числе 4 статьи в ведущих рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России, одну работу в издании, индексированном в международной базе цитирования Scopus, и 8 статей в журналах и сборниках, включенных в РИНЦ, свидетельствуют о достаточно полном представлении результатов исследования научной общественности.

Тематика работы соответствует паспорту специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Задачи, поставленные в диссертационной работе, решены в полном объеме. Диссертация и автореферат изложены грамотным, четким и доказательным языком технических публикаций.

Основные научные результаты диссертации получены автором самостоятельно и свидетельствуют о достижении поставленной перед диссертационным исследованием цели.

Вместе с тем, изучив диссертацию и автореферат диссертации, а также ознакомившись с публикациями автора, считаем необходимым отметить **ряд недостатков**:

1. В работе недостаточно полно рассмотрен вопрос обеспечения подлинности транзакций, передаваемых от избирателя в блокчейн, поскольку обеспечение ключами пользователей для этих целей не описано.

2. Использование смарт-контрактов в системе ДЭГ провинции изложено сжато без достаточного обоснования необходимости и ожидаемых преимуществ.

Указанные недостатки носят частный характер и не оказывают существенного влияния на общее положительное впечатление от работы.

**Вывод:** Диссертационная работа 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)» представляет собой законченную научно-квалификационную работу, является актуальным и завершенным исследованием, обладающим внутренним единством, в котором на основании выполненных автором исследований содержится решение научной задачи, имеющей значение для развития технической отрасли знаний.

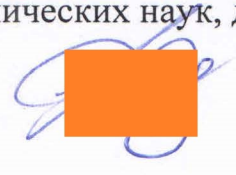
Диссертационная работа Салман Васан Давуд Салман соответствует требованиям п.п. 9, 10, 11 и 13 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации № 842 в ред. от 05.07.2021 г., а ее автор Салман Васан Давуд Салман достойна присуждения ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании научно-исследовательского отдела АО «НИИ «Рубин», протокол № 03(115)/24 - НИО от 18 января 2024 г.

Отзыв подготовили:
Директор по научно-техническому развитию
доктор технических наук, профессор

Евгений Владимирович Гречишников

Ведущий научный сотрудник НИО
кандидат технических наук, доцент



Юрий Васильевич Санин