ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора Александра I»
(ФГБОУ ВО ПГУПС)
Московский пр., д.9, Санкт-Петербург, 190031
Телефон: (812) 457-86-28, факс: (812) 315-26-21
E-mail: dou@pgups.ru, http://www.pgups.ru
ОКПО 01115840, ОГРН 1027810241502,
ИНН 7812009592/ КПП 783801001

_____ № _____

УТВЕРЖДАЮ
Первый проректор – проректор
по научной работе
ФГБОУ ВО ПГУПС
доктор технических наук
профессор
Титова Т.С.

[redacted]

«04» 02 2024 г.

[redacted]

Отзыв ведущей организации

на диссертацию 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»

I. Актуальность темы исследования

Информационно-коммуникационные технологии в современном мире стремительно развиваются и оказывают влияние на общество, в частности на такие его сферы как образование, здравоохранение, банковское дело, медиа, транспорт, производство, торговля и другие. Научно-технический прогресс и расширение применения информационно-коммуникационных технологий затронули и такую важную сферу социальной деятельности, как различные виды голосования.

Дистанционное электронное голосование подразумевает переход к системе онлайн-голосования, базирующейся на интернет-платформе с использованием криптографических методов. В связи с этим, такая система должна отвечать

требованиям информационной безопасности и обеспечивать защиту информации. А именно, обеспечивать тайну голосования, анонимность голосующего, аутентификацию избирателя, уникальность, точность и подтверждение голоса. Таким образом, разработки в области дистанционного электронного голосования должны опираться на результаты из множества других областей, в том числе: программного обеспечения, криптографии, политики, права, экономики и социальных наук. В странах арабского мира, в частности в республике Ирак, систем ДЭГ нет и есть необходимость построения таких систем.

Все вышеперечисленное подтверждает актуальность и важность избранной автором темы исследования.

II. Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

Полученные в диссертационном исследовании результаты обладают научной новизной, заключающейся в:

1) модели перспективной системы дистанционного электронного голосования, созданной с учетом специфики голосования в арабских странах;

2) протоколе перспективной системы дистанционного электронного голосования, разработанного с учетом особенностей угроз системам дистанционного электронного голосования в арабских странах и основанного на гомоморфном шифровании и распределенном дешифровании;

3) методе проверки корректности заполнения избирательного бюллетеня в целом.

III. Обоснованность и достоверность научных положений и выводов

Обоснованность положений и выводов, сформулированных в диссертации, обеспечивается учетом большого количества факторов, влияющих на решение поставленной научной задачи, а также аргументированным выбором основных допущений и ограничений, принятых в качестве исходных данных при ее постановке.

Достоверность научных положений и выводов подтверждена практическим внедрением при решении конкретных задач, о чём свидетельствуют акты о

внедрении и реализации результатов исследования, а также положительным рецензированием научных работ Салман В.Д.С. при их опубликовании в журналах из перечня ВАК РФ и при широком обсуждении результатов исследования на научных конференциях.

IV. Значимость для науки и практики результатов, полученных автором диссертации

Значимость результатов диссертационной работы Салман В.Д.С. для науки заключается в:

1) Разработке нового подхода к построению системы дистанционного электронного голосования на основе использования технологии блокчейна и применения криптографических преобразований, что обеспечивает защиту системы от многих угроз безопасности;

2) протоколе системы дистанционного электронного голосования, который в отличие от многих протоколов использует подход, основанный на применении криптосистемы шифрования с единым для всех избирателей ключом шифрования и разными ключами дешифрования бюллетеней, распределенными между независимыми серверами, что обеспечивает повышенную анонимность избирательного процесса;

3) методе проверки корректности заполнения избирательного бюллетеня, который расширяет класс методов проверки и основывается на доказательстве с нулевым разглашением секрета, что обеспечивает повышение безопасности избирательного процесса, поскольку в ходе процедуры проверки не раскрывается суммарное число голосов, отданное избирателями за кандидатов.

Значимость для практики результатов диссертационного исследования подтверждена соответствующими актами о внедрении и состоит в том, что:

1) предлагаемую модель системы дистанционного электронного голосования, можно использовать для перехода от системы голосования с использованием бумажных бюллетеней к безопасной и экологичной системе дистанционного электронного голосования, предлагающей возможность сокращения времени подсчета голосов за счет использования распределенной сети блокчейн-узлов и смарт-контрактов.

2) предлагаемый протокол можно применять на выборах, когда требуется обеспечение выполнения требований информационной безопасности голосования в условиях угроз со стороны человеческого фактора;

3) предлагаемый метод проверки корректности заполнения бюллетеня может быть использован для доказательства корректности заполнения бюллетеня в различных системах дистанционного электронного голосования.

V. Рекомендации по использования результатов и выводов диссертации

Вследствие узкоспециализированной прикладной направленности результатов диссертационного исследования, их в дальнейшем целесообразно использовать в компаниях, производящих системы дистанционного электронного голосования для арабских государств с парламентской правовой системой.

VI. Общая оценка диссертационной работы

Положения, выносимые на защиту, дают чёткое представление о выполненных исследованиях. Для решения поставленных в диссертации задач использовались:

- криптографические методы на основе схем гомоморфного шифрования (Эль-Гамаля) в числовом поле и на эллиптической кривой;
- схема доказательства с нулевым разглашением секрета;
- методы доказательства корректности заполнения бюллетеня;
- технология блокчейна-консорциума.

Подходы диссертанта к решению поставленной научной задачи логичны и систематизированы, исследование выполнено последовательно, выводы строго доказаны, что в совокупности гарантирует корректность и непротиворечивость полученных результатов. Таким образом, все научные положения диссертационного исследования достоверны и обоснованы.

Вместе с тем, диссертации присущи некоторые недостатки:

1) На рис. 3.1 допущена редакционная неточность. Представлена схема взаимодействия участников системы ДЭГ на этапе инициализации. Данный этап завершается тем, что избиратели получают открытый ключ для голосования.

Однако на рисунке показаны действия, выполняемые на последующих этапах: отправка зашифрованного бюллетеня с доказательством правильности его заполнения, а также отправка результатов голосования в ЦИК.

2) Анализ угроз для системы ДЭГ (параграф 3.4) не содержит такую угрозу, как искажение голосов избирателей на этапе следования зашифрованного бюллетеня по каналу связи от избирателя к блокчейну. Таким искажением может быть, например, изменение голоса "за" на "против" путем искажения второй части криптограммы, полученной по схеме Эль-Гамаля. Возникают вопросы: каковы шансы нарушителя реализовать эту угрозу? Возможно ли одновременно исказить зашифрованный голос и подделать доказательство правильности заполнения бюллетеня? Что конкретно в системе ДЭГ позволяет предотвратить успешную реализацию такой угрозы?

3) В параграфе 3.5 представлена демонстрация разработанного программного обеспечения. На наш взгляд, тестирование проводится на слишком малой выборке: симулируется работа трех серверов и девяти избирателей. Также при тестировании выбраны малые значения параметров криптографического протокола, в том числе $p = 11460087211$. В результате складывается неполное представление о работоспособности, устойчивости, эффективности и защищенности системы ДЭГ в условиях проведения реальных выборов, где количество избирателей исчисляется миллионами, сервера обрабатывают огромное количество запросов одновременно и необходимо соблюдать все основные требования к выбору параметров криптосистем.

Тем не менее, отмеченные недостатки не влияют на общее положительное впечатление от диссертационной работы.

VII. Заключение

Работа соответствует паспорту специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» по следующим пунктам: п. 3 – Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса; п. 5 – Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в

открытых компьютерных сетях, включая Интернет; п. 19 – Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Диссертация Салман Васан Давуд Салман «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 завершенную научно-квалификационную работу, содержащую в себе решение научной задачи, имеющей важное значение для развития теории и практики создания перспективных защищенных систем дистанционного электронного голосования информации в арабских государствах с учетом специфики угроз безопасности информации в этих странах. Работа соответствует критериям, предъявляемым в отношении кандидатских диссертаций, которые установлены пп. 9–14 Положения о присуждении ученых степеней (утв. Постановлением Правительства РФ от 24.09.2013 № 842), 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».

Отзыв обсужден и одобрен на заседании кафедры «Информатика и информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I» 15.01.2024 г., протокол № 7.

И.о. заведующего кафедрой «Информатика и информационная безопасность»
д.т.н, профессор [redacted] Ходаковский Валентин Аветикович

доцент кафедры «Информатика и информационная безопасность»
к.т.н., доцент [redacted] Гофман Максим Викторович