Акционерное общество
«Региональный центр защиты
информации «ФОРТ»

АО «РЦЗИ «ФОРТ»

ул. Коли Томчака, д.9,
лит. Б, пом. 1-Н,
г. Санкт-Петербург, 196006

Тел.: (812) 313-62-90,

e-mail: info@rczifort.ru

05-02-24 №21-МС-05-02-24/8

На № 05/99 от 18.02.2022

Экз. № 1

УТВЕРЖДАЮ
Генеральный директор, к.т.н.
[redacted] М.Ю. Сохен
02 2024 г.

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

Актуальность темы исследования.

Дистанционное электронное голосование (ДЭГ) - переход к системе онлайн-голосования, базирующейся на интернет-платформе с использованием криптографических методов. Однако использование открытой среды (Интернета) для функционирования системы ДЭГ создает много рисков надежности системы ДЭГ и безопасности ее функционирования, поэтому в системе ДЭГ должны выполняться требования обеспечения тайны голосования, анонимности голосующего, аутентификации избирателя, уникальности и точности голосования, является задачей ближайшей перспективы, а разработка защищённых блокчейн-систем актуальной задачей.

При построении системы голосования должны учитываться угрозы безопасности информации, характерные для данного региона или группы стран. Такие угрозы в основном связаны с технологией обработки бумажных бюллетеней и влиянием субъективного (человеческого) фактора, в частности, возможными атаками со стороны административного ресурса системы.

Поэтому, исследование и разработка современных и безопасных систем дистанционного электронного голосования для арабских государств, является актуальной научно-практической задачей. Актуальность решения этой задачи усилилась в последнее время в связи с пандемией коронавируса, охватившей весь мир.

На защиту вынесены следующие научные результаты:

1. Модель системы дистанционного электронного голосования (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.

2. Протокол функционирования перспективной системы дистанционного электронного голосования на основе гомоморфного шифрования с распределенным расшифрованием, учитывающий угрозы безопасности информации актуальные для арабских государств, и обеспечивающий повышение защищенности от угроз, связанных с субъективным (человеческим) фактором.

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

Теоретическая ценность работы состоит в следующем:

1. Разработан подход к построению системы ДЭГ на основе использования технологии блокчейна и применении криптографических преобразований, обеспечивающих защиту системы ДЭГ от многих угроз ее

безопасности. Предлагается систему ДЭГ республики Ирак создавать в виде объединения подсистем ДЭГ провинций, построенных по принципу блокчейн-консорциума. Взаимодействие избирательной комиссии провинции и избирательных участков провинции предлагается осуществлять с использованием смарт-контрактов. В смарт-контрактах хранятся зашифрованные голоса избирателей избирательного участка, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть.

2. В протоколе перспективной системы ДЭГ в отличие от многих протоколов ДЭГ, использован подход, основанный на применении криптосистемы шифрования с единым для всех избирателей ключом шифрования и разными ключами расшифрования бюллетеней, распределенными между независимыми (принадлежащими разным партиям) серверами, что обеспечивает повышенную анонимность избирательного процесса.

3. Метод проверки корректности заполнения избирательного бюллетеня расширяет класс методов проверки корректности заполнения бюллетеня, основанного на доказательства с нулевым разглашением секрета, и обеспечивает повышение безопасности избирательного процесса поскольку в ходе процедуры проверки не раскрывается суммарное число голосов, отданное избирателем за кандидатов.

Практическая значимость работы состоит в том, что:

1. Модель системы ДЭГ предлагается использовать для перехода от системы голосования с использованием бумажных бюллетеней к безопасной и экономичной системе дистанционного электронного голосования с возможностью сокращения времени подсчета голосов за счет использования распределенной сети блокчейн-узлов с использованием смарт-контрактов и применения гомоморфного шифрования.

2. Предлагаемый протокол может применяться на выборах, где требуется выполнение требований обеспечения информационной

безопасности голосования в условиях угроз со стороны административного ресурса и других угроз, связанных с субъективным (человеческим) фактором. Функционирование протокола апробировано на разработанном макете системы ДЭГ, что подтверждает его реализуемость.

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

Практическая значимость подтверждается тем, что результаты диссертационного исследования внедрены в образовательный процесс Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Значимость результатов диссертационной работы подтверждена актом реализации Независимой Высшей избирательной комиссии республики Ирак, как составная часть тематики работ, проводимых комиссией по применению современных выборных технологий при переходе от традиционной системы голосования к системе дистанционного голосования особенно в части реализации процедур регистрации и голосования. Подтверждена целесообразность внедрения результатов работы в будущие проекты.

Обоснованность и достоверность полученных результатов выносимых на защиту, на сколько можно судить по автореферату, обусловлены и подтверждаются корректностью математического обоснования проведенных исследований и системным подходом к решению поставленных задач, в том числе: использованием методов анализа криптографических схем гомоморфного шифрования в числовом поле и на эллиптической кривой; методов доказательства с нулевым разглашением секрета; методов доказательства корректности заполнения бюллетеня, технологии блокчейн-консорциума. Моделирование функционирования предложенного протокола ДЭГ выполнено на основе комплекса приложений, разработанного на языке программирования Python 3.10 с использованием библиотеки PyQt5.

Результаты исследований прошли **апробацию**, в достаточной степени опубликованы, имеют хорошую реализацию и внедрение. Основные результаты диссертационной работы опубликованы в 13 печатных трудах, из них 4 статьи опубликовано в рецензируемых научных изданиях, рекомендованных ВАК, 1 статья в рецензируемом издании, входящем в международные базы данных SCOPUS, 8 статей опубликованы в других изданиях и материалах научных конференций.

Реферат оформлен достаточно хорошо. Обнаружено всего две ошибки (на страницах 8 и 10).

К недостаткам данной работы, судя по автореферату, можно отнести:

1. Не рассмотрен вопрос надежности системы ДЭГ в случае отказа одного из серверов, участвующих в расшифровке зашифрованных бюллетеней избирателей.

2. Не описаны угрозы, которые блокируются, (предотвращаются) на основе применения разработанного протокола.

3. В автореферате используется криптографические термины из зарубежных источников переведенных на русский язык в то время, как в России принята терминология, определяемая «Справочником криптографических терминов» изданным Академией криптографии РФ в 2006 году.

4. Из автореферата не ясно, каким образом «Показано, что имеющийся в настоящее время задел в построении квантово-устойчивых криптоалгоритмов и планируемая в ближайшей перспективе международная стандартизация этих криптоалгоритмов, дают уверенность в том, что эта проблема будет преодолена и применение квантово-устойчивых криптоалгоритмов в системах ДЭГ обеспечат необходимый уровень информационной безопасности».

Указанные недостатки не имеют определяющего значения для оценки теоретической и практической значимости работы.

ВЫВОД:

На основании содержания автореферата можно сделать вывод о том, что диссертационная работа Салман В.Д.С. является законченной научно-квалификационной работой, выполненной на актуальную тему, в которой содержится решение научной задачи, имеющей значение для технической отрасли знаний. Критерии, которым должна соответствовать диссертация на соискание ученой степени, установленные Положением о присуждении ученых степеней, утвержденным постановлением Правительства Российской Федерации № 842 в редакции от 01.10.2018 г., соблюдены. Салман В.Д.С. заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Отзыв на автореферат диссертации Салман В.Д.С. рассмотрен на заседании НТС АО «РЦЗИ ФОРТ».

Заместитель председателя НТС АО «РЦЗИ ФОРТ»
кандидат технических наук, доцент

Борисенко Николай Павлович

Ученый секретарь НТС АО «РЦЗИ ФОРТ»
кандидат технических наук

Попов Вениамин Вениаминович