ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА 99.2.038.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 06 марта 2024 г. № 2

О присуждении Салман Васан Давуд Салман, гражданке Республики Ирак, ученой степени кандидата технических наук.

Диссертация «Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере республики Ирак)» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 22 декабря 2023 года, протокол № 7 объединенным диссертационным советом 99.2.038.03, созданным на базе федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства науки и высшего образования Российской Федерации, федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства науки и высшего образования Российской Федерации, федерального государственного бюджетного образовательного учреждения

высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Салман Васан Давуд Салман, 29 января 1986 года рождения, в 2016 году окончила федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технологический университет» с присвоением квалификации магистра по направлению подготовки «Информатика и вычислительная техника». В 2023 году окончила освоение программы подготовки научных и научно-педагогических кадров в аспирантуре федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Диссертация выполнена на кафедре защищенных систем связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Научный руководитель – доктор технических наук, профессор, Яковлев Виктор Алексеевич, основное место работы: федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», кафедра защищенных систем связи, профессор кафедры.

Оппоненты: 1. Александрова Елена Борисовна, доктор технических наук, доцент, основное место работы: федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Высшая школа кибербезопасности, профессор; 2. Левина Алла Борисовна, кандидат физико-математических наук, доцент, основное место работы: федеральное

государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), кафедра информационной безопасности, доцент кафедры, дали положительные отзывы о диссертации.

Ведущая организация – федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», г. Санкт-Петербург, в своем положительном заключении, подписанном Ходаковским Валентином Аветиковичем, доктором технических наук, профессором, и.о. заведующего кафедрой «Информатика и информационная безопасность» и Гофманом Максимом Викторовичем, кандидатом технических наук, доц., доцентом кафедры «Информатика и информационная безопасность», утвержденном Титовой Тамилой Семеновной, доктором технических наук, профессором, первым проректором – проректором по научной работе, указала, что 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.

Соискатель имеет 13 опубликованных работ, в том числе по теме диссертации 13, из них в рецензируемых научных изданиях, рекомендованных

ВАК, – 4, а также: 1 работу в изданиях, индексируемых в международных базах цитирования; 8 статьи в других научных журналах, сборниках научных статей, трудов и материалах конференций. Из них 7 работ опубликовано соискателем без соавторства. Общий объём авторского вклада в работы составляет 4,86 печ.л. из общего количества 6,15 печ.л. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах.

Наиболее значительные научные работы по теме диссертации.

Публикации в рецензируемых научных изданиях, рекомендованных ВАК:

1. Салман В.Д. Анализ гомоморфных криптосистем Бенало и Пэйе для построения системы электронного голосования // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 102–109. DOI:10.31854/1813-324X-2021-7-2-102-109.

2. Салман В.Д. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.Д. Салман, В.А. Яковлев // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 21–27. DOI:10.31854/1813-324X-2023-9-1-21-27.

3. Салман В.Д. Модель и протокол перспективной системы дистанционного электронного голосования для Республики Ирак с учетом особенности избирателей системы // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2023. – №. 2. – С. 91-101.

4. Салман В.Д. Способ защиты от атаки некорректного заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.Д. Салман, В.А. Яковлев // Труды учебных заведений связи. – 2023. – Т. 9. – № 4. – С. 95–111. DOI:10.31854/1813-324X-2023-9-4-95-111.

Публикации в изданиях, индексируемых в МБЦ:

5. Salman W. Analysis of the traditional voting system and transition to the online voting system in the republic of Iraq / Salman W., Yakovlev V., Alani S. // 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, – 2021. – С. 1-5. DOI: 10.1109/HORA52670.2021.9461387.

Публикации в других изданиях:

6. Салман В.Д. Требования к системам электронного голосования // Национальная безопасность России: актуальные аспекты. – 2020. – С. 14-17.

7. Салман В.Д. Анализ системы голосования в республике Ирак и пути перехода к системе электронного голосования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 400-404.

8. Салман В.Д. Подход к улучшению существующей иракской системы голосования с использованием дистанционного голосования // Теория и практика обеспечения информационной безопасности. Москва. – 2021. – С. 11-19.

9. Салман В.Д. Способ обеспечения анонимности электронного голосования от атаки отслеживания голосов отдельных избирателей / В.Д. Салман, В.А. Яковлев, Д.А. Орлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. С. 723–726.

10. Салман В.Д. Исследование системы электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием / В.Д. Салман, В.А. Яковлев, Д.С. Шевцов // Защищенные системы связи. – 2022. – № 2. – С.86-92.

11. Салман В. Д. Оценка сложности метода проверки корректности заполнения избирателем бюллетеня в системе дистанционного электронного голосования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 880–885.

12. Салман В.Д. Метод проверки корректности заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.Д. Салман, В.А. Яковлев // Актуальные проблемы инфотелекоммуникаций в науке и

образовании (АПИНО 2023) XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 885–890.

13. Салман В.Д. Гомоморфная криптосистема для подсчета голосов // Новые импульсы развития: вопросы научных исследований Г. Саратов. – 2020. – № 1-1. – С. 94-100.

На диссертацию и автореферат поступили отзывы: официального оппонента Александровой Е.Б.; официального оппонента Левиной А.Б.; ведущей организации ПГУПС; Авсентьева О.С., д.т.н., проф., профессора кафедры информационной безопасности Воронежского института Министерства внутренних дел Российской Федерации; Борисенко Н.Н., к.т.н., доц., заместителя председателя научно-технического совета и Попова В.В., к.т.н., ученого секретаря АО «Региональный центр защиты информации «ФОРТ»; Волошиной Н.В., к.т.н., доцента факультета безопасности информационных технологий Национального исследовательского университета ИТМО; Гайдамака Ю.В., д.ф.-м.н., проф., профессора кафедры теории вероятностей и кибербезопасности Российского университета дружбы народов имени Патриса Лумумбы; Гречишникова Е.В., д.т.н., проф., директора по научно-техническому развитию и Санина Ю.В., к.т.н., доц., ведущего научного сотрудника НИО АО «Научно-исследовательский институт «РУБИН»; Потехина И.Ю., к.ф.-м.н., заместителя руководителя службы по надзору Управления Роскомнадзора по Северо-Западному федеральному округу; Рабина А.В., д.т.н., доц., профессора кафедры аэрокосмических компьютерных и программных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.

Все отзывы положительные. Высказаны следующие критические замечания. На этапе 3, описанном на стр. 51-52 (рис. 2.3), зашифрованный бюллетень, по-видимому, должен передаваться на сервер, а не в избирательный комитет (ИК), иначе нет смысла в агрегировании результатов. При описании схемы голосования (стр. 52-54) не указано, как конкретно шифруется весь бюллетень при голосовании за нескольких кандидатов. Это не позволяет в полной мере понять,

как именно агрегируют результаты и вычисляется итог голосования. Одним из требований к предлагаемой системе дистанционного электронного голосования является блокирование голосования за лиц, не пришедших на выборы. Автор утверждает, что этот механизм реализуется за счет использования электронной подписи при передаче бюллетеня, однако данный этап, с одной стороны, отсутствует в предложенном протоколе, а с другой стороны, противоречит сформулированному в п. 1.6 требованию соблюдения анонимности избирателя. В тексте работы не приведена информация о правах доступа участников блокчейн-сети, а также о содержании используемых смарт-контрактов. Кроме того, используемый алгоритм консенсуса предполагает доверие к административным ресурсам системы (серверу голосования, избирательной комиссии). Предусматривает ли разработанная модель защиту от компрометации данных участников или превышения ими полномочий? В таблице 2.2 недостаточно аргументирован выбор системы гомоморфного шифрования. Неясно, например, почему подпись «вслепую», реализованная на основе той же схемы Эль-Гамаля, не обладает «простотой реализации». Выбор схемы Эль-Гамаля делается, в том числе, на основе временных характеристик, приведенных в таблице 3.2, стр. 90, однако в работе не сказано, при каких параметрах и на какой платформе осуществлялись замеры времени при анализе гомоморфных криптосистем. Не учитывается также уязвимость схемы шифрования Эль-Гамаля к атакам на основе подобранного шифртекста. В части 2.1.1 приводится описание схемы голосования на основе криптосистемы Эль-Гамаль, при этом описание самого алгоритма приводится только в части 2.1.3.1, такие же проблемы сохраняются по всей работы, структура представления материала построена от частного к общему, хотя более логично строить изложение материала от общего к частному. Не приведено отличие предложенной системы дистанционного электронного голосования (ДЭГ) на основе блокчейн-технологии от уже существующих систем, так же не проведен сравнительный анализ предложенного подхода с существующими. В контексте гомоморфного шифрования рассмотрены схемы Пэйе, Бенало и Эль-Гамаль, все данные криптосистемы являются частично

гомоморфными, но при этом не рассмотрен криптоситема NTRU, являющаяся, в настоящее время, единственной полностью гомоморфной криптосистемой, гомоморфизм сохраняется и по умножению, и по сложению. В части 2.5. «Разработка модели перспективной системы ДЭГ в республике Ирак (арабских государствах) с учетом условий и особенностей избирательного процесса», не хватает математизированного описания самой модели. Отсутствует обоснование, почему из множества криптоалгоритмов, удовлетворяющих целям, поставленным в данной работе, выбрана именно криптосистема Эль-Гамаль, связано ли это с тем, что стандарт подписи NIST, алгоритм DSA, основан на ней? 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, изменения 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 доказательства правильности заполнения бюллетеня? Что конкретно в системе ДЭГ позволяет предотвратить успешную реализацию такой угрозы? В параграфе 3.5 представлена демонстрация разработанного программного обеспечения. На наш взгляд, тестирование проводится на слишком малой выборки: 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. В автореферате недостаточно внимания уделено описанию назначения и использования смарт-контрактов в разработанной модели системы ДЭГ провинции. Не рассмотрен вопрос надежности системы ДЭГ в случае отказа

одного из серверов, участвующих в расшифровке зашифрованных бюллетеней избирателей. Не описаны угрозы, которые блокируются, (предотвращаются) на основе применения разработанного протокола. 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». 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; и один и тот же элемент G, как это указано в (3), то узел БЧ легко определит результаты голосования избирателя). Очевидно, что существенным недостатком схемы является необходимость решения задачи дискретного логарифма для определения результатов голосования за каждого из кандидатов. 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. Из автореферата не видно, как осуществляется избирателями или наблюдателями проверка учета поданных избирателями голосов. В автореферате на с. 17 говорится, что предложенный протокол был проанализирован на предмет его стойкости к различным угрозам, однако перечень угроз не приведен. В работе недостаточно полно рассмотрен вопрос обеспечения подлинности транзакций, передаваемых от избирателя в блокчейн, поскольку обеспечение ключами пользователей для этих целей не описано. Использование смарт-контрактов в системе ДЭГ провинции изложено сжато без достаточного обоснования необходимости и ожидаемых преимуществ. Из автореферата не видно, рассматривались ли угрозы со стороны средств массовой информации, которые могут влиять на осознанное волеизъявление граждан и как предполагается

осуществлять такой контроль в республике Ирак? Недостаточно раскрыт вопрос важности информационного обеспечения выборов, что способствует гласности выборов, уменьшает уязвимость системы от угроз со стороны административного ресурса. Во второй главе автор представляет модель системы дистанционного электронного голосования для арабских государств с парламентской правовой системой, основанную на распределенной сети блокчейн-узлов. Данная модель является первым научным результатом, выносимым на защиту. При четком и достаточно полном описании модели не рассмотрены её свойства. В четвертой главе описан разработанный автором метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом, являющийся третьим научным результатом, выносимым на защиту. Относительно данного метода не приведены ограничения на его использование.

Выбор оппонентов и ведущей организации обосновывается их широкой известностью своими достижениями в области информационной безопасности и связанных с проблематикой, представленной к защите диссертации, в частности, наличие значительного количества публикаций по тематике диссертации и способностью определить научную и практическую ценность работы (д.т.н., доцент Александрова Е.Б., является профессором высшей школы кибербезопасности СПбПУ; к.ф-м.н., доцент Левина А.Б. является доцентом кафедры «Информационная Безопасность»). Ведущая организация – ПГУПС (и.о. заведующего кафедрой «Информатика и информационная безопасность», д.т.н, профессор Ходаковский Валентин Аветикович, доцент кафедры «Информатика и информационная безопасность», к.т.н., доцент, Гофман Максим Викторович).

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны элементы научно-методического аппарата для создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах с учетом особенностей избирательного процесса в этих странах на основе использования гомоморфного шифрования с распределенным дешифрованием; **предложен**

подход к построению системы ДЭГ для арабских государств на основе использования технологии блокчейн-консорциума с использованием смарт-контрактов и применении криптографических преобразований, обеспечивающих защиту системы ДЭГ от угроз её безопасности, преимущественно связанных с субъективным фактором; **доказана** возможность обеспечения точности и безопасности голосования на основе предложенного метода проверки корректности избирательного бюллетеня в целом; **введено** новое понятие «проверка корректности заполнения избирательного бюллетеня в целом».

Теоретическая значимость исследования обоснована тем, что: доказана возможность построения безопасной модели и протокола системы дистанционного электронного голосования, обеспечивающих выполнение требований обеспечения информационной безопасности голосования в условиях угроз со стороны административного ресурса и других угроз, связанных с субъективным (человеческим) фактором. В отличие от известных систем ДЭГ предложенная модель построена на основе распределенной сети узлов блокчейн-консорциума (БЧ) с использованием смарт-контрактов; **применительно к проблематике диссертации результативно использованы** криптографические методы гомоморфного шифрования (схема Эль-Гамаля) с распределенным дешифрованием для мультипликативной группы простого поля и для группы точек эллиптической кривой; схема «доказательство с нулевым разглашением секрета»; методы доказательства корректности заполнения бюллетеня, технология блокчейна-консорциума, что в целом обеспечивает выполнение требований безопасности информации: тайна волеизъявления; анонимность голосующего; аутентификация избирателя; уникальность и точность голосования, подтверждение факта голосования. Предложенный подход к построению протокола в отличие от известных обеспечивает дополнительную защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы; **изложены** и обоснованы основные положения и требования по созданию системы ДЭГ для арабских государств; **раскрыты** источники и содержание угроз безопасности информации в системе

ДЭГ, основанной на интернет платформе, отмечена специфика потенциального влияния субъективного фактора на результаты голосования через администрацию системы ДЭГ; **изучены** принципы построения современных систем ДЭГ и их практическая реализация в разных странах; типовые угрозы в системе ДЭГ и способы их предотвращения (блокирования); **проведена модернизация** существующих методов проверки корректности заполнения избирательного бюллетеня, что обеспечивает скрытность суммарного числа голосов в избирательном бюллетене.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены элементы научно-методического аппарата по построению модели и протокола защищенной системы ДЭГ в образовательный процесс Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича и используются кафедрой защищенных систем связи в учебном процессе на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Криптографические протоколы» (рабочая программа дисциплины, регистрационный № 23.05/216-Д) при чтении лекций, проведении практических занятий и лабораторных работ; **определены** перспективы практического использования модели, протокола ДЭГ и метода проверки корректности заполнения бюллетеня на выборах, в условиях угроз со стороны административного ресурса и других угроз, связанных с субъективным (человеческим) фактором, что подтверждается 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; **создан** демонстрационный макет модели ДЭГ, включающий комплекс программ и интерфейсов для участников избирательного процесса. На основе моделирования процедуры голосования с

использованием макета подтверждена функциональность протокола голосования; **представлены** рекомендации по дальнейшему совершенствованию разработанного программно-аппаратного комплекса для проведения исследований производительности предложенной системы голосования и оценки устойчивости системы ДЭГ к атакам на основе квантового компьютера и разработке мер (методов) обеспечения безопасности системы ДЭГ в этих условиях.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты подтверждены корректным применением методов имитационного моделирования с использованием программного комплекса, разработанного на языке программирования Python 3.10 и библиотеки PyQt5 для создания графического интерфейса приложений; **теория** построения защищенной системы ДЭГ основана на общепринятых методах криптографической защиты информации с учетом достаточно большого количества факторов, влияющих на решение поставленной научной задачи, обоснованным выбором основных допущений и ограничений при ее решении; **идея** предложенного подхода к построению защищенной системы ДЭГ **базируется** на анализе практики и обобщении передового опыта в построении современных защищенных систем ДЭГ в разных странах и заключается в отказе от использования единого ключа расшифрования бюллетеней; **использованы** современные криптографические методы защиты информации (гомоморфное шифрование, разделение секрета, цифровая подпись, доказательства с нулевым разглашением секрета); технологии высокозащищенного реестра данных – блокчейна); **установлено** качественное совпадение авторских результатов с результатами, представленными в независимых источниках по данной тематике; **использованы** современные методы сбора и обработки информации и методы вычислительной математики, сертифицированное программное обеспечение для компьютеров моделирования.

Личный вклад соискателя состоит в том, что она непосредственно участвовала в получении и анализе первичных данных, необходимых для

исследования, выполняла анализ и обобщение полученных в работе теоретических и экспериментальных данных, исследовала приведенные в работе алгоритмы и методы, представляла результаты своих исследований для обсуждения на всероссийских и международных конференциях, осуществляла подготовку основных результатов исследования к публикации. Результаты теоретических и экспериментальных исследований получены автором самостоятельно.

В ходе защиты диссертации были высказаны следующие критические замечания: Недостаточно полно раскрыта угроза, связанная с субъективным фактором. Не понятно, может ли избирательная комиссия узнать после выборов кто и как проголосовал.

Соискатель Салман В.Д.С. в ходе заседания ответила на задаваемые ей вопросы, согласилась с замечаниями и привела собственную аргументацию: Субъективный фактор представляет собой внутреннюю угрозу, исходящую от администрации системы голосования, а также влияния на результаты голосования авторитетных лиц – религиозных деятелей и старейшин. Избирательная комиссия не может узнать кто и как проголосовал после выборов потому, что ключ дешифрования распределён между серверами, принадлежащими разным партиям и никогда не восстанавливается как единый ключ. Без знания ключа злоумышленнику расшифровать криптограмму невозможно.

Диссертационный совет установил, что диссертация «Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере республики Ирак)» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 3, 5 и 19. паспорта научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

На заседании 06 марта 2024 года объединенный диссертационный совет принял решение присудить Салман В.Д.С. ученую степень кандидата технических

наук за решение научной задачи по разработке модели и протокола защищенной системы дистанционного электронного голосования на парламентских выборах в арабских государствах, с учетом особенностей избирательного процесса на основе использования гомоморфного шифрования с распределенным дешифрованием.

При проведении тайного голосования объединенный диссертационный совет в количестве 18 человек, из них 5 докторов наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 23 человек, входящих в состав совета, проголосовали: за – 18, против – нет, недействительных бюллетеней – нет.

Председатель диссертационного совета,
доктор технических наук, доцент [redacted] Киричек Руслан Валентинович

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент [redacted] Владыко Андрей Геннадьевич

07 марта 2024 года