Отзыв официального оппонента

Александровой Елены Борисовны 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)», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертационной работы

В настоящее время дистанционное электронное голосование представляется одной из альтернатив традиционной системе голосования и направлено на повышение эффективности избирательного процесса и упрощение выборных процедур, в том числе для конечных пользователей. Использование для этих целей информационных технологий позволяет нивелировать влияние человеческого фактора на точность результатов, однако требует решения новых задач, связанных с обеспечением информационной безопасности (защита от утечки чувствительных данных, скупки голосов, реализация принципа тайного голосования и др.).

Модель системы дистанционного электронного голосования должна быть адекватна законодательству и учитывать специфику выборного процесса конкретного государства, поэтому в условиях отсутствия готовых к внедрению решений для организации выборов в республике Ирак можно говорить о своевременности и актуальности задачи разработки научно-методического аппарата для построения безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертационной работе

Обоснованность сформулированных положений и выводов, достоверность результатов, полученных в диссертации, определяются корректной постановкой задачи исследования, учетом большого числа факторов, влияющих на ее решение, в том числе особенностей законодательства; обоснованным выбором основных допущений и ограничений, принятых в качестве исходных данных; использованием современного математического аппарата полей Галуа, эллиптических кривых, гомоморфных преобразований; доказательством корректности предлагаемых решений; обсуждением результатов диссертационной работы на конференциях. Полученные результаты раскрыты в диссертационной работе достаточно полно.

Апробация результатов исследования

Основные научные результаты диссертационной работы докладывались и обсуждались на:

конференции «Национальная безопасность России: актуальные аспекты» (Санкт-Петербург, 2020);

конференции «Новые импульсы развития: вопросы научных исследований» (Саратов, 2020);

Всероссийской научно-теоретической конференции «Теория и практика обеспечения информационной безопасности» (Москва, 2021);

3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (Турция, Анкара, 2021),

международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, 2021, 2022, 2023).

Научная новизна результатов диссертационной работы

Научная новизна диссертационного исследования состоит в разработке модели и алгоритмов перспективной системы дистанционного электронного голосования, обеспечивающих безопасность процесса голосования. Наиболее существенными новыми научными результатами, полученными соискателем, являются:

1. Модель перспективной системы дистанционного электронного голосования, учитывающая специфику голосования в арабских странах и отличающаяся применением распределенной сети узлов блокчейн-консорциума с использованием смарт-контрактов.

2. Протокол перспективной системы дистанционного электронного голосования, основанный на гомоморфном шифровании, что обеспечивает выполнение основных требований безопасности информации, а также защиту от специальных атак со стороны административного ресурса системы.

3. Метод проверки корректности заполнения избирательного бюллетеня, гарантирующий правильность выбора избирателем количества кандидатов из диапазона возможных значений и скрытность суммарного числа голосов в бюллетене, что позволяет защититься от атак, при которой анализируется статистика хода голосования до окончания выборов.

Теоретическая и практическая ценность полученных результатов

Теоретическая ценность работы заключается в предложенном подходе к построению системы дистанционного электронного голосования при проведении парламентских выборов в республике Ирак в виде объединения подсистем дистанционного электронного голосования провинций, построенных по принципу блокчейн-консорциума. Взаимодействие избирательной комиссии и избирательных участков провинции предлагается осуществлять с использованием смарт-контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает

нагрузку на блокчейн-сеть. Использование перспективных криптографических протоколов доказательства с нулевым разглашением для проверки корректности заполнения избирательного бюллетеня расширяет класс методов проверки корректности заполнения бюллетеня и обеспечивает защищенность избирательного процесса.

Практическая ценность результатов диссертационной работы состоит в том, что предложенные решения позволяют перейти к безопасной и экономичной системе дистанционного электронного голосования и могут применяться на выборах, проводимых в условиях угроз со стороны административного ресурса и других угроз, связанных с человеческим фактором. Предложенный метод проверки корректности заполнения бюллетеня не ограничивается разработанной в диссертационной работе системой и может быть использован в различных системах дистанционного электронного голосования.

Значимость результатов диссертационного исследования подтверждается актом внедрения в образовательный процесс Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, а также 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.

Публикации по теме диссертации

Автореферат и работы, опубликованные соискателем, дают полное представление о содержании самой диссертации и результатах, полученных в процессе проведения исследований. Диссертантом опубликовано 13 работ по теме диссертации, в том числе четыре статьи в рецензируемых научных журналах, входящих в перечень изданий, рекомендуемых ВАК Министерства науки и высшего образования Российской Федерации, одна статья в рецензируемом издании, входящем в международную базу данных SCOPUS, восемь статей в журналах и сборниках конференций, включенных в РИНЦ.

Характеристика содержания диссертационной работы

Диссертация изложена на 177 страницах, включает введение, четыре главы, заключение, 21 рисунок, 40 таблиц, список литературы из 114 наименований, четыре приложения.

В главе 1 проведен анализ принципов построения систем голосования в республике Ирак и других арабских государствах, приведены требования к системе голосования, технологии и основные этапы выборов, выделены особенности избирательных систем в арабских государствах с парламентской правовой системой.

В главе 2 рассматриваются способы построения современных систем ДЭГ, предлагается модель системы ДЭГ с учетом особенностей избирательного процесса в республике Ирак.

В главе 3 разработан протокол ДЭГ на основе схемы Эль-Гамаля, приведены его основные этапы, дан перечень основных угроз и способы противодействия.

В главе 4 предложен метод защиты от некорректного заполнения избирательного бюллетеня.

В заключении приведены основные результаты диссертационной работы.

Структура работы логична и отвечает задачам исследований. Разработанная модель и алгоритмы описаны достаточно полно.

Текст автореферата соответствует материалу диссертации.

Замечания по тексту диссертационной работы

1. На этапе 3, описанном на стр. 51-52 (рис. 2.3), зашифрованный бюллетень, по-видимому, должен передаваться на сервер, а не в 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 агрегируются результаты и вычисляется итог голосования.

2. 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.

3. 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?

4. 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.

5. При описании алгоритмов в главе 4 несколько нарушена стройность изложения, поскольку одни схемы изложены для мультипликативной группы простого поля, а другие – для группы точек эллиптической кривой. Переход в работе между двумя этими структурами привел к ряду ошибок при изложении протоколов. В частности, значения a_2 и b_2, вычисляемые в таблице 4.5,

«забыты» автором при проверке корректности в таблице 4.6. Кроме того, переход к эллиптическим кривым требует и модификации криптографических протоколов, описанных в предыдущей главе.

6. В тексте диссертации присутствуют опечатки, а также неточности в части используемых обозначений и терминологии. В частности:

– употребляемый автором термин «дешифрование» целесообразно заменить на «расшифрование», поскольку по смыслу подразумевается легитимная операция получения открытого текста с помощью ключа; постквантовые схемы инкапсуляции ключа названы схемами асимметричного шифрования;

– умножение точки эллиптической кривой на число уместно обозначать без операции приведения по модулю (kP, а не $kP(mod\ p)$);

– при описании схемы шифрования Эль-Гамаля (стр. 94–95) введены две образующие: g и G (при этом в тексте диссертации не уточнено, отлично ли G от g). Если $G \neq g$, то корректность метода формирования доказательства (формулы (4.16), (4.17) на стр. 114) будет нарушена;

– наличие коллизий в обозначениях: например, в табл. 4.5 (стр. 113) буквой M обозначена и точка эллиптической кривой, и операция умножения точки на число.

7. В приведенных численных примерах присутствуют погрешности:

– в п. 3.5 (стр.103) указано, что при моделировании системы ДЭГ использовался 1024-битный ключ, однако в параметрах указана характеристика поля p длиной 34 бита. Также, с учетом введенной характеристики $p = 11460087211$, целесообразно в качестве образующей g указать не значение $2799360000000 > p$, а наименьший положительный вычет $g' \equiv g\ (mod\ p) = 3098720516$, т.к. элемент $g \in \mathbb{F}_p^*$ и, следовательно, $g < p$;

– в Приложении 4 (стр.167) не пояснено, почему $q = 17$. Если это порядок подгруппы группы точек кривой, то для него должно выполняться условие: $q \mid \#E(\mathbb{F}_p)$), а для указанной в примере кривой $\#E(\mathbb{F}_p) = 60$.

Отмеченные замечания в целом не снижают общее положительное впечатление о работе.

Заключение

Диссертационное исследование Салман Васан Давуд Салман является законченной самостоятельной научно-квалификационной работой, в которой содержится решение актуальной научной задачи создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах, учитывающей особенности избирательного процесса и использующей перспективный математический аппарат гомоморфного шифрования с распределенным расшифрованием. Работа выполнена на достаточно высоком уровне. Полученные автором результаты достоверны, выводы и заключения обоснованны.

Содержание и основные научные результаты соответствуют паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автореферат достаточно полно отражает основное содержание диссертационной работы. Оформление работы соответствует требованиям, предъявляемым к диссертациям.

На основании изложенного считаю, что диссертация 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)» полностью соответствует критериям, изложенным в п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 № 842, предъявляемым к кандидатским диссертациям, 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.

Официальный оппонент
профессор Высшей школы кибербезопасности федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого», доктор технических наук, доцент

[redacted] Александрова Елена Борисовна

Сведения об организации:
федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого»
195251, Санкт-Петербург, Политехническая ул., д. 29
телефон: (812) 552-76-32
e-mail: helen@ibks.spbstu.ru