ОТЗЫВ

официального оппонента кандидата физико-математических наук Левиной Аллы Борисовны на диссертацию 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)» представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Актуальность темы.

Дистанционное электронное голосование, в настоящее время, стремительно развивается и внедряется в различны странах/регионах. Вопросы безопасности и достоверности протоколов ДЭГ являются ключевыми вопросами при принятии решения - использовать данные протоколы или нет. Сама идея электронного голосования является относительно новой и существует ряд протоколов уже внедренных или проходящих апробацию, но несмотря на существующие протоколы все равно их использование пока является спорным вопросом, так как не все существующие проколы могут гарантировать целостность и сохранность данных, вносимых избирателем.

В связи с этим, представленная тема данного диссертационного исследования несомненно является актуальной.

Степень обоснованности научных положений, выводов и рекомендаций.

В работе Салман Васан Давуд Салман предложен протокол защищенной системы ДЭГ для арабских государств, представлена модель ДЭГ с учетом специфики голосования в арабских странах и приведен метод проверки кор-

ректности заполнения избирательного бюллетеня, позволяющий контролирующему органу убедиться в правильном выборе количества кандидатов из диапазона возможных значений.

Научные положения, выносимых на защиту, обоснованы, автор корректно использует известные научные методы обоснования полученных результатов, выводов и рекомендаций. Им были изучены и проанализированы известные достижения в рассматриваемой области. В работе диссертант грамотно использует математический аппарат, а для подтверждения теоретических положений проводит компьютерное моделирование и экспериментальные исследования.

Положения, выносимые на защиту, логичны и подтверждаются проведенным исследованием.

Выводы соответствуют поставленным задачам, а также полученным результатам и логично вытекают из основного содержания диссертационного исследования. Материалы диссертации прошли достаточную апробацию на научных конференциях, также подтверждаются, приложенным к диссертации актом о внедрении результатов диссертации.

Оценка новизны и достоверности.

В качестве новых научных результатов можно полагать следующие результаты:

1. Разработана модель системы дистанционного электронного голосования с учетом специфики голосования в арабских странах и требований по обеспечению ее безопасности;

2. Разработан протокол функционирования перспективной системы дистанционного электронного голосования с учетом особенностей процесса голосования в арабских странах;

3. Разработан метод проверки корректности заполнения зашифрованного избирательного бюллетеня избирателем.

Результаты исследования подтверждаются перечнем апробаций результатов работы на научных конференциях, наличием 4 опубликованных научных работ в рецензируемых научных изданиях из Перечня ВАК, 1 научной работы, опубликованной в журнале из международной базы Scopus, 8 статей в журналах, включенных в РИНЦ.

Работе присущи недостатки:

К основным из них относятся следующие:

1. 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.
2. Не приведено отличие предложенной системы ДЭГ на основе блокчейн технологии от уже существующих систем, так же не проведен сравнительный анализ предложенного подхода с существующими.
3. 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.
4. 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.
5. 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?

Отмеченные недостатки не снижают качество исследований и не влияют на главные теоретические и практические результаты диссертации.

Диссертация является законченным научно-квалификационным трудом, выполненным автором самостоятельно на хорошем научном уровне. Полученные автором результаты достоверны, выводы и заключения обоснованы. По каждой главе и работе в целом сделаны четкие выводы. Автореферат соответствует основному содержанию диссертации. Диссертационная работа отвечает требованиям Положения о присуждении ученых степеней, а ее автор Салман Васан Давуд Салман–заслуживает присуждения ей ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Доцент кафедры «Информационная Безопасность», Санкт-Петербургский государственный электротехнический университет СПбГЭТУ «ЛЭТИ»
кандидат физ-мат наук, доцент
Алла Борисовна Левина
Тел.: 89112433693
Email: alla_levina@mail.ru

13.02.2024

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина)»
197022, г. Санкт-Петербург, ул. Профессора Попова, д. 5, литера Ф
(812) 346-27-58; omola@etu.ru