

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

Яковлева Виктора Алексеевича

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».

В процессе работы над диссертацией Салман В.Д. решила актуальную научную задачу, заключающуюся в разработке научно-методического аппарата для создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах с учетом особенностей избирательного процесса на основе использования гомоморфного шифрования с распределенным дешифрованием.

Актуальность данной задачи определяется необходимостью создания современной высокозащищенной от множества атак системы дистанционного электронного голосования для республики Ирак и других арабских государств с парламентской правовой системой. Полученные в ходе диссертационных исследований результаты обладают научной новизной и практической значимостью. Их применение позволяют повысить эффективность и безопасность системы дистанционного электронного голосования.

Наиболее значимые научные результаты заключаются в следующем:

1. Разработана модель перспективной системы ДЭГ для арабских государств с парламентской правовой системой, в том числе для республики Ирак, которая базируется на современной концепции построения надежных информационных систем на основе распределенной сети блокчейн-узлов и применении криптографических преобразований. Представленная модель системы ДЭГ республики Ирак строится в виде объединения подсистем ДЭГ провинций, каждая из которых имеет собственный узел на консорциум

блокчейне, содержащем информацию о голосовании на избирательных участках и округах данной провинции. Такая конструкция сети позволяет организовать защищенный от многих угроз протокол голосования.

2. Разработан протокол функционирования перспективной системы ДЭГ на основе гомоморфного шифрования с распределенным дешифрованием, учитывающий специфические угрозы ДЭГ в арабских государствах, в том числе угрозы, связанные с человеческим фактором, который обеспечивает тайну голосования; повышенную защищенность от нарушения анонимности голосующего; аутентификацию избирателя; уникальность; точность голосования и подтверждение голосования.

3. Разработан метод защиты от атаки некорректного заполнения избирательного бюллетеня в системе дистанционного электронного голосования, который в отличие от известных методов позволяет контролирующему органу убедиться в том, что избиратель правильно выбрал количество кандидатов из диапазона возможных значений и этот метод является более безопасным, так как в ходе проверки корректности заполнения бюллетеня в целом не раскрывается общая сумма голосов, отданных за кандидатов.

За время обучения в аспирантуре Салман В.Д. успешно освоила программу аспирантской подготовки, овладела навыками проведения научных исследований, активно участвовала в работе научно-технических конференций и семинаров, постоянно совершенствовал свои знания в области защиты телекоммуникационных и компьютерных сетей, в том числе систем дистанционного электронного голосования. Хорошая подготовка, способность решать сложные научно-исследовательские задачи, высокая работоспособность, настойчивость и упорство помогли Салман В.С. разработать диссертацию на соискание ученой степени кандидата технических наук. Соискатель Салман В.Д. общительна, корректна и доброжелательна в отношениях с коллегами.

Результаты диссертационных исследований Салман В.Д. представлены в 13 публикациях, прошли апробацию на международных и республиканских научно-технических конференциях, реализованы в СПб ГУТ.

Представленная диссертационная работа носит характер завершеного научного исследования, в котором получено новое решение актуальной научной задачи, работа соответствует требованиям ВАК РФ, 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».

Научный руководитель,
профессор кафедры защищенных систем связи (ЗСС) СПбГУТ,
доктор технических наук, профессор

 Яковлев Виктор Алексеевич

04 октября 2023 года

Организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Юридический адрес: наб. р. Мойки, д. 61, литера А, Санкт-Петербург, 191186

Почтовый адрес: пр. Большевиков, д. 22, корп. 1, Санкт-Петербург, 193232

Тел.: (812) 3263156, факс (812) 3263159, e-mail: rector@sut.ru, web-сайт: www.sut.ru

Подпись (-и)

 заверяю

заместитель начальника

Административно-кадрового управления

 /Н.А. Аксёнова/ 04/10/2023 г.

