



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»
(ГУАП)

ул. Большая Морская, д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057,
E-mail: info@guap.ru, http://new.guap.ru, ОГРН 1027810232680, ИНН/КПП 7812003110/783801001

№ _____
На № _____ от _____

ОТЗЫВ

**на автореферат диссертации Салман В.Д. 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**

Разработка безопасных систем дистанционного электронного голосования является важной научно-практической задачей. Актуальность её решения в последнее время возросла в связи с ростом объемов передаваемой и обрабатываемой информации, а также пандемией коронавируса. В связи с этим тема диссертации Салман В.Д. актуальна, прежде всего, с практической точки зрения.

Целью диссертации является обеспечение защищенности от угроз безопасности информации в системах дистанционного электронного голосования на парламентских выборах.

Автором проанализированы особенности избирательного процесса на парламентских выборах в республике Ирак и арабских государствах, рассмотрены основные преимущества внедрения дистанционного электронного голосования (ДЭГ), проанализированы принципы построения современных систем ДЭГ, сделан вывод о преимуществах гомоморфного шифрования и приведено обоснование выбора данной схемы для дальнейшего исследования.

Салман В.Д. разработана модель системы ДЭГ для арабских государств с парламентской правовой системой, основанная на распределенной сети блокчейн-узлов, реализован протокол функционирования перспективной системы дистанционного электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием, представлено математическое описание преобразований предложенного протокола голосования и разработан метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом.

Приведенные в автореферате результаты экспериментов показывают достаточно высокую эффективность предлагаемого подхода к защите информации.

Достоверность полученных результатов подтверждается корректным применением математического аппарата, соответствием результатов имитационного моделирования теоретическим предложениям и практической реализацией в избирательной комиссии республики Ирак.

В качестве недостатков работы следует отметить следующее:

1. 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.

2. 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.

Отмеченные выше недостатки, по-видимому, отражают способ представления результатов в автореферате и не затрагивает существа диссертационной работы.

Полученные в работе Салман В.Д. результаты представляются оригинальными, имеющими научное и практическое значение.

Считаю, что диссертация удовлетворяет требованиям ВАК, автор заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.6.

Профессор кафедры аэрокосмических компьютерных и программных систем Института аэрокосмических приборов и систем федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (ГУАП), доктор технических наук, доцент



А.В. Рабин

«19» февраля 2024 г.

Контакты:

Тел. +7 (812) 494-70-90; E-mail: alexey.rabin@guap.ru

Web-сайт: <https://guap.ru/>. Адрес: 190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.

Подпись Рабина Алексея Владимировича, доктора технических наук, доцента, профессора кафедры аэрокосмических компьютерных и программных систем Института аэрокосмических приборов и систем ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

«ЗАВЕРЯЮ».



Заверяю
И.О. Рабин А.В.
И.О. Рабин А.В.
02 2024