РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО СЕВЕРО-ЗАПАДНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора по Северо-Западному федеральному округу)

ул. Галерная, д.27, Санкт-Петербург, 190000
тел.: (812) 5719566; факс (812) 5712731
E-mail: rsockanc78@rsoc.ru

_____ № _____
на № _____ от _____

СПбГУТ
Диссертационный совет Д 99.2.038.03

ОТЗЫВ

на автореферат диссертации 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.

Дистанционное электронное голосование является новой формой политического участия граждан на выборах всех уровней. Оно имеет много преимуществ перед традиционным «бумажным» голосованием;

-Повышение явки избирателей, что подтверждается статистическими данными;

- Вовлечение в процесс голосования наиболее активной части граждан— молодежи;

--Повышение удобства участия в выборах маломобильным гражданам, гражданам, находящимся в труднодоступных районах и за рубежом;

-Снижение издержек на организацию процесса голосования в том числе затрат на бумажную продукцию;

- Уменьшение времени подсчета голосов,

Однако дистанционное голосование имеет и ряд недостатков:

- Повышенные риски информационных сбоев, кибератак, поскольку передача данных (бюллетеней) осуществляется через незащищенную среду-Интернет.

- Недоверие многих граждан к электронным технологиям, что вызвано, в первую очередь, с социально-психологическими факторами, связанными с недостаточным уровнем образования в области информационных технологий и уровнем недоверия доверия избирателей к обеспечению тайны голосования, анонимности голосующего и сохранности бюллетеня.

В странах арабского мира с парламентской формой управления системы дистанционного электронного голосования отсутствуют. Прямой «перенос» проработанных технологий дистанционного электронного голосования из стран, где они уже применяются, в страны арабского мира не всегда возможен. Это объясняется тем, что система дистанционного голосования должна соответствовать законодательству страны применения и учитывать специфические угрозы безопасности информации при проведении процедуры голосования.

Поэтому тема диссертационной работы В. Салман, в которой решена научная задача разработки научно-методического аппарата построения системы дистанционного электронного голосования на парламентских выборах в арабских государствах, обеспечивающая защиту от угроз инфомационной безопасности с учетом особенностей избирательного процесса в этих странах является актуальной.

Научная новизна полученных результатов:

Судя по автореферату в работе проведен подробный анализ современных систем дистанционного электронного голосования, применяемых в различных странах. На этой основе сделан выбор перспективного направления построения

модели и протокола системы дистанционного электронного голосования на основе криптографических методов гомоморфного шифрования для стран арабского мира с парламентской формой управления.

По результатам работы на защиту выносятся три научных положения, обладающие новизной, теоретической и практической значимостью:

Модель перспективной системы дистанционного электронного голосования создана с учетом специфики голосования в арабских странах, которая в отличие от известных систем ДЭГ строится на основе распределенной сети узлов блокчейна-консорциума (БЧ) с использованием смарт-контрактов. Такая архитектура системы ДЭГ позволяет реализовать на ней функционирование протокола голосования, обеспечивающего выполнение требований информационной безопасности процесса голосования.

Протокол системы дистанционного электронного голосования разработан с учетом особенностей угроз системе ДЭГ в арабских странах и основан на гомоморфном шифровании и распределенном дешифровании, что обеспечивает выполнение требований безопасности информации: тайна волеизъявления; анонимность голосующего; аутентификация избирателя; уникальность и точность голосования, подтверждение факта голосования. Отличается от известных тем, что обеспечивает дополнительную защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы. Это достигается за счет применения распределенного дешифрования, при котором никто из участников системы не имеет доступа к ключу дешифрования.

Метод проверки корректности заполнения избирательного бюллетеня в целом, в отличие от известных методов, позволяет контролирующему органу убедиться в том, что избиратель правильно выбрал количество кандидатов из диапазона возможных значений. При этом обеспечивается скрытность суммарного числа голосов в бюллетене, поданном избирателем,

Обоснованность и достоверность, выносимых на защиту положений, выводов и рекомендаций подтверждаются обоснованным учетом актуальных угроз, обусловленных субъективными факторами, правильным выбором

основных методов обеспечения защищенности информации от них, использованием современного математического аппарата методов криптографической защиты информации.

Практическая значимость результатов:

Работа имеет большую практическую направленность, 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.

Недостатки работы:

Судя по автореферату, к недостаткам можно отнести:

1. 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?
2. Недостаточно раскрыт вопрос важности информационного обеспечения выборов, что способствует гласности выборов, уменьшает уязвимость системы от угроз со стороны административного ресурса.

Указанные замечания не влияют на общую положительную оценку диссертационной работы

Выводы:

В целом, судя по автореферату, диссертация 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)», представляет собой законченное научное исследование, содержащее новые методические и практические решения в области создания защищенных систем дистанционного электронного голосования, отвечает требованиям ВАК, предъявляемым к

диссертационным работам, представляет несомненную практическую ценность, а ее автор – Салман Васан Давуд Салман, заслуживает присуждения ученной степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность..

Отзыв составил:

Заместитель руководителя, Потехин И.Ю.

кандидат физико-математических наук

21.02.2024

Управление Роскомнадзора по Север-Западному федеральному округу

Почтовый адрес: ул. Галерная, д.27, Санкт-Петербург, 190098

Тел.: (812) 678-95-26.

e-mail: i.potehin@rkn.gov.ru