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)», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность

Определяющим трендом развития инфотелекоммуникационных систем в мире является развитие и совершенствование систем дистанционного электронного голосования (ДЭГ), имеющих важные преимущества перед традиционными системами, связанные с возможностью отказа от использования бумажных бюллетеней и сокращения сроков подсчета голосов. Кроме того, использование ДЭГ обеспечивает повышение явки избирателей за счет привлечения к голосованию малоподвижных граждан и молодых избирателей, а также создание других сервисов голосующим. Однако в процессе функционирования системы ДЭГ возникает множество внутренних и внешних угроз безопасности протоколов обмена информацией, циркулирующей в интересах обеспечения анонимности и предотвращения фальсификации итогов голосования в условиях, когда в голосовании принимают участие множество уполномоченных избирателей и счетных комиссий, а передача информации осуществляется на основе глобальной сети Интернет. Кроме того система ДЭГ должна учитывать специфику законодательства стран, в которых она применяется.

В связи с указанными обстоятельствами тема диссертации, посвященной решению научной задачи по разработке научно-методического аппарата для создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах, с учетом особенностей избирательного процесса и специфики угроз в этих странах является актуальной.

Из анализа представленных в автореферате материалов следует, что полученные при выполнении диссертации результаты обладают научной новизной, а именно:

– 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 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,

Достоверность результатов, полученных с использованием разработанных в диссертации модели и протокола, обоснованность выносимых на защиту научных положений, выводов и рекомендаций обеспечивается учетом достаточно большого количества факторов, влияющих на решение поставленной научной задачи; обоснованным выбором основных допущений и ограничений, принятых при ее постановке; использованием современного математического аппарата и корректным выбором применяемых показателей.

Следует отметить, что полученные результаты исследования соответствуют теме диссертации, поставленной цели и задачам.

Практическая значимость разработанной модели системы ДЭГ состоит в том, что она может быть использована для перехода от системы голосования с применением бумажных бюллетеней к безопасной и экономичной системе дистанционного электронного голосования с возможностью сокращения времени подсчета голосов. Предлагаемый протокол может применяться на выборах, где требуется выполнение требований обеспечения информационной безопасности голосования в условиях угроз со стороны административного ресурса, а также других угроз, связанных с субъективным (человеческим) фактором.

Необходимо отметить высокий уровень публикаций соискателя по теме исследований. Также заслуживает внимания тот факт, что полученные результаты получили одобрение в 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.

При общей положительной оценке диссертации необходимо отметить следующие недостатки.

1. В автореферате недостаточно внимания уделено описанию назначения и использования смарт-контрактов в разработанной модели системы ДЭГ провинции.

2. В третьей главе упоминается, что в работе проведен анализ наиболее опасных, по мнению автора, угроз безопасности информации в разработанной системе ДЭГ и оценке степени их предотвращения (блокирования). Описание этих угроз не проведено.

Однако указанные недостатки не снижают значимости и важности полученных результатов, и не оказывают влияния на положительную оценку работы.

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.

Профессор кафедры информационной безопасности
Воронежского института МВД России
доктор технических наук, профессор [redacted] Авсентьев Олег Сергеевич

«5» февраля 2024 г.

Организация: Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации».
http://vi.mvd.ru/request_main.
Адрес: Патриотов проспект, дом 53, Воронеж, 394065, Россия.
Тел.: (473) 264-90-15, 264-90-17
Email: vrnin@mvd.ru.

Подпись Авсентьева
удостоверяю
начальник отделения
делопроизводства и режима
Воронежского института
МВД России
[redacted]