РЕАЛИЗАЦИЯ БЕЗОПАСНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ПО ПРОТОКОЛУ ДВУХ АГЕНТСТВ НУРМИ-САЛОМАА-САНТИН

Е.О. Высоцкий, А.М. Кадан

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

Тема электронного голосования (ЭГ) стала популярной по нескольким причинам. Это, в первую очередь, удобство и доступность: ЭГ предлагает удобство голосования из любого места с доступом в интернет. Это уменьшает барьеры для участия в выборах, особенно для людей с ограниченной подвижностью или теми, кто находится далеко от центра голосования.

В докладе представлена реализация подхода, предполагающего использование технологий безопасного электронного голосования при проведении различных процедур, связанных с определением предпочтений различных групп участников. В качестве таких процедур могут рассматриваться: проведение анкетирования для определения предпочтений членов группы, голосование внутри коллектива по актуальным вопросам, прочие процедуры. При проведении этих процедур важными являются такие аспекты, как секретность (обеспечение анонимности голосования каждого участника); безопасность (надежность и защищенность от любых видов вмешательства); доступность (для всех, включая лиц с ограниченными возможностями); однозначность (исключена возможность двойного голосования или голосования от имени другого человека); прозрачность (для участника – возможность проверить, что голос его был правильно учтен, а для группы в целом –

получить доступ к аудиту и проверке системы); надежность (способность выдерживать большие объемы трафика); независимый аудит (включая проверку программного обеспечения, безопасности данных и соблюдения процедур); соответствие законодательству (полностью соответствовать действующему законодательству страны, на территории которой она используется) [1].

Целью доклада является обсуждение методов безопасного электронного голосования на основе криптографических протоколов и представление реализации пилотного проекта на их основе. Для реализации протокола безопасного голосования выбран протокол двух агентств Нурми-Саломаа-Сантин [2] с возможностью биометрической идентификации участника электронного голосования. На основе данного протокола разработано приложение в архитектуре клиент-сервер.

Серверная компонента включает два сервера, обеспечивающих реализацию алгоритма ЭГ. Клиентская часть обеспечивает веб интерфейс, через который пользователь может осуществлять регистрацию, аутентификацию с возможностью биометрической идентификации, а также принимать участие в голосовании. Первое серверное приложение: отвечает за регистрацию пользователей, аутентификацию и обработку запросов на сканирование и сохранение данных лица пользователя. Реализовано с использованием Flask и SQLite. Второе серверное приложение: обрабатывает запросы на генерацию и сохранение меток для пользователей, шифрование и сохранение голосов, а также предоставляет результаты голосования. Реализовано с использованием Flask и SQLite.

Список литературы.

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С / Б. Шнайер. – Wiley, 2016. – 1024 с.

2. Salomaa, A. Verifying and recasting secret ballots in computer networks. New Results and New Trends in Computer Science / A. Salomaa. – Berlin: Springer-Verlag, 1991. – P. 283–289.