УДК 004.056:342.84

ОЦЕНКА ВЕРОЯТНОСТИ ДЕАНОНИМИЗАЦИИ УЧАСТНИКА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Голованов А. А. (Университет ИТМО), **Иогансон И. Д.** (Университет ИТМО)
Научный руководитель – д. т. н., доцент Беззатеев С. В.
(Университет ИТМО)

В данной работе рассматриваются уязвимости протокола анонимизации и оценивается вероятность деанонимизации участников электронного голосования.

Введение. С увеличением вовлеченности технологий в различные сферы жизни общества возникает необходимость отходить от традиционных способов организации механизмов социального управления. Однако для полноценного переноса общественных процессов на информационные технологии требуется решить массу проблем.
Одним из таких механизмов является голосование. Важнейшей проблемой перехода от традиционного голосования к электронному является сложность обеспечения анонимности избирателей. Для решения данной задачи существует множество протоколов анонимизации, некоторые из которых успешно применяются для организации анонимных сетей. Однако подобные решения несовершенны, они не могут обеспечить абсолютную анонимность.
Целью данной работы является оценка вероятности деанонимизации участников электронного голосования.

Основная часть. При передаче по анонимному каналу сообщения объединяются в пучок и проходят через несколько узлов, чья основная задача – перемешать этот пучок. Только сами узлы знают по какому принципу были перемешаны анонимные сообщения. Однако, так как узлы не являются доверенными, существует механизм проверки, позволяющий любому убедиться в том, что сообщения не были подменены. В результате проверки узел раскрывает часть процесса обработки пучка сообщений. При этом узлы согласуются раскрывать этот процесс так, чтобы по одним только результатам проверки было невозможно идентифицировать источник сообщения. Однако если часть узлов скомпрометирована злоумышленником, это будет возможно.
Нами выведены формулы для оценки вероятности деанонимизации участников электронного голосования, исходя из параметров системы.

Выводы. Результаты работы могут быть использованы для оценки рисков информационной безопасности систем электронного голосования.

Голованов А. А. (автор) Подпись: _____

Беззатеев С. В. (научный руководитель) Подпись: _____