ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ: КРИПТОГРАФИЧЕСКИЕ ВЫЗОВЫ И ПОТЕНЦИАЛЬНЫЕ РИСКИ

М. А. Казловский

fpm.kazlovskMA1@bsu.by;
Научный руководитель – С. В. Агиевич, кандидат физико-математических наук

Систематизируются основные криптографические механизмы, которые используются в системах электронного голосования, а также потенциальные атаки на системы электронного голосования и способы защиты от них. Полученные результаты могут быть использованы при проектировании и анализе систем электронного голосования.

Ключевые слова: электронное голосование; право голоса; анонимность избирателя; свобода выбора; защита от принуждения.

ВВЕДЕНИЕ

Системы электронного голосования предоставляют возможность голосовать дистанционно, используя глобальную сеть Интернет. Их использование позволяет снизить стоимость проведения голосования и уменьшить время, которое необходимо затратить на участие в этой процедуре. Более того, если система электронного голосования соответствует ряду строгих требований безопасности, то можно гарантировать высокую степени достоверности результатов голосования. Для соблюдения указанных требований используют нетривиальные криптографические механизмы, комбинации которых позволяют получить надежную системы.

Тем не менее следует признать, что несмотря на существование большого числа различных систем электронного голосования, широкого распространения ни одна из существующих систем не получила. На наш взгляд, такая ситуация обусловлена двумя факторами. Во-первых, системы голосования, которые удовлетворяют большинству требований безопасности, имеют сложную архитектуру, а их работа сопряжена с большим количеством трудоемких вычислений. Во-вторых, практически невозможно обеспечить выполнение некоторых требований безопасности с использованием только криптографических методов защиты.

МОДЕЛЬ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В любой системе электронного голосования выделяют несколько субъектов, то есть участников системы, которые решают различные задачи. Обычно к субъектам относят: избирателя (лицо, которые имеет

право и желание проголосовать), избирательную комиссию (лицо или группу лиц, которая отвечает за обработку результатов голосования) и регистрационную комиссию (лицо или группу лиц, которая отвечает за допуск избирателя к голосованию). Дополнительно к субъектам можно отнести наблюдателя (лицо, которое не принимает участия в процессе голосования, но контролирует корректность его проведения с помощью общедоступной информации) и противника (лицо, которое хочет нарушить корректность процедуры голосования).

В процессе электронного голосования выделяют отдельные этапы, на каждом из которых решаются различные задачи. Основными этапами большинства систем электронного голосования являются: инициализация (этап, на котором регистрационная и избирательная комиссии выполняют выработку и распределение долговременных криптографических параметров и ключей, формирование списка избирателей, а также осуществляют запуск всех необходимых для дальнейшей работы сервисов), регистрация (этап, на котором избиратель проходит аутентификацию перед регистрационной комиссией для проверки права голоса и получения необходимой для голосования информации), голосование (этап, на котором избиратель осуществляет формирование и отправку своего бюллетеня), подсчет (этап, на котором избирательная комиссия выполняет обработку всех поступивших бюллетеней и публикует результаты голосования) и аудит (этап, на котором наблюдатель проводит проверку корректности проведения всех остальных этапов).

Основной характеристикой любой системы электронного голосования является набор требований, которым она соответствует. Можно выделить базовые требования, к которым относят право голоса (в результатах голосования должно быть учтено не более одного бюллетеня от каждого избирателя, включенного в список допущенных к голосованию) и анонимность (связь содержания голоса в любом из отправленных в избирательную комиссию бюллетеней с личностью сформировавшего его лица не может быть найдена). Среди желательных требований рассматривают личную проверяемость (избиратель должен иметь возможность убедиться, что его голос учтен корректно), универсальную проверяемость (наблюдатель должен иметь возможность убедиться, что зарегистрированы только имеющие право голоса избиратели, а также что все бюллетени были корректно обработаны) и конфиденциальность выбора (содержание всех отправленных бюллетеней должно оставаться в тайне до завершения этапа голосования) [1, с. 5]. Существует и ряд дополнительных требований: анонимность в будущем (используемые криптографические алгоритмы должны гарантировать

анонимность избирателя даже при появлении квантового компьютера с большим числом кубитов), свобода выбора (система должна гарантировать, что избиратель не сможет создать криптографическое доказательство содержания своего голоса) и защита от принуждения (система должна гарантировать, что противник не может проверить, выполнил ли принуждаемый избиратель выдвинутые требования) [2, с. 46-47].

Базовые и часть желательных требований поддерживаются и на обычных офлайн выборах: право голоса реализуется через выдачу бюллетеней только находящимся в списке и прошедшим аутентификацию по паспорту избирателям, анонимность достигается за счет неразличимости бюллетеней и отсутствием контроля за процессом его заполнения, для обеспечения универсальной проверяемость используются контролирующие регистрацию и подсчет наблюдатели, а конфиденциальность выбора гарантируется благодаря использованию непрозрачного ящика, который может быть вскрыт только после завершения этапа голосования.

КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ В ЭЛЕКТРОННОМ ГОЛОСОВАНИИ

Для выполнения описанных выше требований используются разнообразные криптографические механизмы. К базовым механизмам можно отнести протокол аутентификации избирателя на этапе регистрации (например, протокол аутентификации Шнорра), протокол организации защищенного соединения между субъектами системы (например, протокол TLS) и алгоритм шифрования бюллетеней (например, алгоритм шифрования Эль-Гамаля).

Среди дополнительных механизмов можно выделить неинтерактивные доказательства с нулевым разглашением, которые используются для обеспечения проверяемости системы (например, доказательства Чаума-Педерсона [3]), алгоритмы разделения секрета, которые используются для повышения доверия к избирательной комиссии (например, схема Шамира), тест на эквивалентность открытого текста (PET), который используется для реализации защиты от принуждения, а также протокол «забывчивой» передача (OT), который может быть использована для анонимного заполнения бюллетеня (например, протокол Чу-Цзена [4]).

Отдельно необходимо упомянуть механизмы, которые используются для обеспечения анонимности. На этапе регистрации применяются механизмы «слепой» подписи или «слепого» аккумулятора [5], которые позволяют избирателю анонимно зарегистрировать эфемерный открытый

ключ. На этапе голосования можно использовать связываемые кольцевые подписи, которые могут гарантировать, что подпись любого бюллетеня была выполнена одним из имеющих право голоса избирателей, причем каждый избиратель подписал не более одного бюллетеня. На этапе подсчета используют механизмы перемешивания, которое разрушает связь между зашифрованным и расшифрованным бюллетенем, и гомоморфного шифрования, которое позволяет расшифровать сумму всех голосов.

АТАКИ НА СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Можно выделить следующие атаки, которые возможно как на офлайн, так и на онлайн голосования: вброс (нарушение правила один избиратель – один учтенный бюллетень), подмена (замена поданного избирателем бюллетеня), «мертвые души» (включение в список избирателей посторонних лиц) и неправильный подсчет (некорректная обработка бюллетеней). В системах электронного голосования для защиты от вброса используется подпись бюллетеня и, быть может, доказательства с нулевым разглашением; для защиты от подмены возможно внедрение публичного хранилища бюллетеней, которое может быть основано, например, на технологии «блокчейн», для защиты от «мертвых душ» можно применять публичную аутентификацию избирателей, в рамках которой избиратель предъявляет свой сертификат открытого ключа; для защиты от неправильного подсчета требуется или публикация ключа расшифрования, или предъявление доказательства с нулевым разглашением корректности расшифрования.

Для электронного голосования можно выделить дополнительные направления атак: небезопасное приложение для голосования, недоверенная регистрационная комиссия, недоверенная избирательная комиссия, принуждение на этапе регистрации и нарушение анонимности с помощью сетевой информации. Программное обеспечение с открытым исходным кодом и поддержание индивидуальной проверяемости с помощью криптографических механизмов, публичная аутентификация избирателя, алгоритмы разделения секрета для личных ключей избирательной комиссии, аппаратный токен для регистрации избирателя, анонимный канала связи для подачи голоса (например, виртуальные частные сети) соответственно могут быть предложены в качестве механизмов защиты.

Библиографические ссылки

1. *Kho, Y. X., Heng, S. H., & Chin, J. J.* A Review of Cryptographic Electronic Voting // Symmetry. 2022. Vol. 14, issue 5, p. 858.

2. *Juels A., Catalano D., Jakobsson M.* Coercion-Resistant Electronic Elections // Towards Trustworthy Elections: New Directions in Electronic Voting. 2010. pp. 37–63.
3. *Chaum D., Pedersen T. P.* Wallet databases with observers // Annual international cryptology conference. 1992. pp. 89–105.
4. *Chu C. K. and Tzeng W. G.* Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. // PKC'05, 8th International Workshop on Theory and Practice in Public Key Cryptography. 2005. pp. 172–183.
5. *Agievich S.* Blind accumulators for e-voting // Proceedings of Central European Conference on Cryptology CECC '22. 2022. pp. 15–18.