СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАСПРОСТАНЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Казловский М. А.

Белорусский государственный университет, Минск, Беларусь,
e-mail: kazlovski@bsu.by

В настоящее время во всем мире активно проводится цифровизация различных сфер жизни общества. В Республике Беларусь, например, в ближайшее время будет проведена выдача идентификационных карт, которые позволят гражданам совершать юридически значимые действия через Интернет. Естественным образом возникает вопрос о создании системы электронного голосования, которая позволила бы избирателям выражать волеизъявление дистанционно. Использование такой системы имеет ряд неоспоримых плюсов: удешевление стоимости проведения выборов, увеличение процента явки, усложнение фальсификации результатов. Однако, у электронного голосования есть и ряд недостатков, связанных с формой его проведения: сложность удаленной авторизации избирателя, возможность стороннего вмешательства в ход голосования, необходимость в профессиональном аудите как используемых криптографических протоков, так и разработанных программных реализаций. В работе строится общая модель систем электронного голосования, вводятся требования к таким системам, а также изучается вопрос соответствия известных систем сформулированным требованиям.

Как правило, в модели электронного голосования выделяют следующих субъектов: избиратель, избирательная комиссия, кандидат и противник [1]. Избиратель, имеющие право голоса, отдает его за одного или нескольких из конкурирующих кандидатов. Избирательная комиссия – это государственный орган, ответственный за проведение выборов. Противник – злонамеренная сущность, которая пытается манипулировать голосованием и/или подсчетом голосов. Внешний противник может воздействовать на избирателя, пытаясь принудить или подкупить его, а также пытаться нарушить конфиденциальность и анонимность избирателей, используя недостатки протокола голосования. Внутренний противник дополнительно может пытаться изменить ход подсчета голосов, раскрыть промежуточные результаты голосования, а также нарушить функционирование избирательной комиссии.

Процесс электронного голосования обычно состоит из пяти этапов, при этом этапы 1 – 4 идут именно в такой последовательности, а этап 5 может выполнятся несколько раз (после каждого из этапов 2 – 4):

1. Анонс, во время которого объявляются используемые протоколы, формируется список избирателей, устанавливаются секретные параметры и назначаются члены избирательной комиссии.
2. Регистрация, во время которой личность избирателя проверяется и подтверждается избирательной комиссией.
3. Голосование, во время которого избиратель отдает свой голос.
4. Подсчет, во время которого избирательная комиссия проверяет валидность голосов и обрабатывает их для подведения итогов выборов.
5. Верификация, во время которой избиратели и сторонние наблюдатели проверяют отданные голоса.

В качестве свойств, которым должна соответствовать идеальная система электронного голосования, можно выделить:

1. Право голоса: в выборах могут принимать участие только избиратели, которые имеют право голосовать (то есть включенные в список избирателей), при этом избиратель не должен иметь возможность проголосовать больше раз, чем предусматривают правила голосования.
2. Приватность: невозможно определить, как проголосовал конкретный избиратель; предполагается что анонимность голоса может быть нарушена только при сговоре избирателя и избирательной комиссии.
3. Точность: все валидные голоса должны быть правильно записаны и подсчитаны, голоса недействительных избирателей не должны быть учтены.
4. Честность: чтобы провести беспристрастные выборы, никто не должен иметь возможность подсчитывать промежуточное количество голосов по ходу проведения выборов.
5. Проверяемость: личная – каждый избиратель имеет возможность убедиться, что его голос учтен корректно и универсальная – любой желающий имеет доступ к итогам голосования и может проверить, что учтены все действительные голоса и подсчет голосов был проведен корректно.
6. Защищённость: система должна корректно функционировать даже при активных и пассивных атаках избирателей и/или членов избирательной комиссии, а также при невыполнении или некорректном выполнении субъектом возложенных на него функций.
7. Недоказуемость: избиратель не имеет возможности получить или составить доказательство, подтверждающее содержание его голоса (как именно он проголосовал): это не позволит заставить избирателя проголосовать определенным образом.
8. Расширяемость: система голосования должна быть спроектирована таким образом, чтобы корректно функционировать при любом масштабе выборов.

В качестве криптографических механизмов, которые могут использоваться в системах электронного голосования можно выделить:

- Протокол, организующий защищенное соединение: используется для безопасной передачи информации между субъектами системы.
- Протокол, организующий анонимное соединение (Mixnets, DC-net): используется для анонимной отправки избирателем своего голоса.
- Доска объявлений: используется как публичный канал, доступный всем субъектам системы.
- Протокол слепой подписи: используется для анонимизации голоса.
- Протокол разделения секрета: используется для того, чтобы достичь защищенности путем распределения доверия между субъектами.
- Гомоморфное шифрование: используется для обеспечения приватности голосования.
- Протокол интерактивного или неинтерактивного доказательства с нулевым разглашением: используется для подтверждения действительности голоса и/или криптографической операции.

Все системы электронного голосования можно классифицировать, основываясь на том, как избиратели подают голоса в избирательную комиссию:

- Скрытый избиратель: избиратели подают голоса анонимно ([2], [3]).
- Скрытое голосование: избиратели открыто подают зашифрованные голоса ([4], [5]).
- Скрытый избиратель со скрытым голосованием: избиратели отправляют анонимно зашифрованные голоса ([6], [7], [8]).

Сравнительный анализ данных систем проведен в таблице 1.

Табл. 1. Сравнительный анализ популярных систем электронного голосования

Свойство / схема голосования	[2]	[3]	[4]	[5]	[6]	[7]	[8]
Право голоса	С	С	С	С	С	С	С
Приватность	С	С	С	С	С	С	С
Точность	С	УС	С	С	Н	Н	С
Честность	УС	УС	УС	УС	С	УС	УС
Проверяемость	С	ЛП/УП	С	С	ЛП	ЛП	С
Защищённость	Н	УС	УС	УС	Н	УС	УС
Недоказуемость	С	С	С	С	Н	С	С
Расширяемость	Н	С	УС	С	С	Н	УС
Легенда: С – соответствует, Н – не соответствует, УС – условно соответствует; ЛП – личная проверяемость, УП – универсальная проверяемость							

Таким образом, можно сделать вывод, что наиболее перспективными для дальнейшего исследования являются системы, в которых скрытый избиратель осуществляет скрытое голосование.

Литература

1. Sampigethaya K., Poovendran R. A framework and taxonomy for comparison of electronic voting schemes. In: Computers & Security 25(2); 2006. p. 137-153.
2. Sako K, Killian J. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In: Advances in cryptology – EUROCRYPT '95. LNCS, vol. 921. Springer-Verlag; 1995. p. 393–403.
3. Chaum D. Secret-ballot receipts: true voter-verifiable elections. IEEE Security & Privacy Magazine Feb 2004.
4. Baudron O, Foque PA, Pointcheval D, Poupard G, Stern J. Practical multi-candidate election system. In: Proceedings of the 20th ACM symposium on principles of distributed computing. ACM Press; 2001. p. 274–283.
5. Lee B, Kim K. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In: ICISC '02. LNCS, vol. 2587. Springer-Verlag; 2002. p. 389–406.
6. Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. In: Advances in cryptology – AUSCRYPT '92. LNCS, vol. 718. Springer-Verlag; 1993. p. 248–259.
7. Okamoto T. Receipt-free electronic voting schemes for large scale elections. In: Proceedings of the workshop on security protocols '97. LNCS, vol. 1361. Springer-Verlag; 1997. p. 25–35.
8. Kiayias Aggelos, Yung Moti. The vector-ballot e-voting approach. In: Financial cryptography. LNCS, vol. 3110. Springer-Verlag; 2004. p. 72–89.