ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2016
Seria: ORGANIZACJA I ZARZĄDZANIE z. 96 Nr kol. 1963

Marcin SOBOTA
Politechnika Śląska
Wydział Matematyki Stosowanej
marcin.sobota@polsl.pl

WYBRANE ASPEKTY GŁOSOWANIA ELEKTRONICZNEGO

Streszczenie. Głosowanie elektroniczne jest formą głosowania, w którym wykorzystuje się środki komunikacji elektronicznej. Głosowanie takie może być wspomagane przez wizualizację wyników, wspierane elektronicznie lub prowadzone w pełni elektronicznie z zastosowaniem sieci Internet. W ramach niniejszego artykułu zostaną przedstawione wybrane aspekty głosowania realizowanego w pełni drogą elektroniczną. Opisano w nim główne zagrożenia i problemy związane z wykorzystaniem elektronicznych kart do głosowania, nadawaniem uprawnień głosującym oraz elementów silnej kryptografii.

Słowa kluczowe: e-voting, głosowanie elektroniczne, wybory elektroniczne, bezpieczeństwo, kryptografia.

SELECTED ASPECTS OF ELECTRONIC VOTING

Summary. Electronic voting is a form of voting which uses electronic tools of communication. This form of voting may be aided by the visualization of results, supported by electronic or fully carried out electronically via the Internet. This paper present selected aspects of voting carried out fully electronically.

Keywords: e-voting, electronic voting, electronic elections, security, cryptography.

1. Wprowadzenie

Głosowanie elektroniczne jest formą głosowania, w której wykorzystuje się środki komunikacji elektronicznej. Głosowanie takie może być wspierane elektronicznie na trzech poziomach:

- wizualizacja wyników, w której systemy komputerowe wykorzystywane są do zbierania oraz prezentacji wyników wyborów. Poza tą częścią głosowanie odbywa się drogą tradycyjną – lokale wyborcze, papierowe karty do głosowania itd.;
- głosowanie wspomagane elektronicznie – systemy komputerowe odpowiedzialne za zbieranie i prezentację wyników dodatkowo rozbudowane są o elektroniczne urządzenia, za pośrednictwem których głosujący oddają swoje głosy. Elementem tradycyjnym pozostaje fakt, że urządzenia te są dostępne wyłącznie w lokalach wyborczych specjalnie przygotowanych na czas wyborów;
- głosowanie w pełni elektroniczne – drogą komunikacji jest sieć rozległa Internet, a głosujący mogą oddać swój głos z dowolnego miejsca i dowolnego urządzenia wyposażonego w odpowiednią aplikację.

Niniejsze opracowanie będzie dotyczyć aspektów związanych z głosowaniem w pełni elektronicznym, w którym zweryfikowana osoba uprawniona do głosowania może oddać swój głos z dowolnego miejsca i w dowolnym czasie (ograniczonym przez termin początkowy i końcowy głosowania).

2. Uprawienia do głosowania

Jednym z podstawowych elementów związanych z głosowaniem elektronicznym jest nadanie uprawnień do głosowania. W przypadku głosowania metodami tradycyjnymi sprawdzenie uprawnień odbywa się przez weryfikację danych osoby głosującej przez komisję wyborczą na podstawie dokumentu tożsamości. Każda osoba uprawniona znajduje się na liście osób uprawnionych, tworzonych na podstawie miejsca zameldowania. O ile proces weryfikacji nie jest kłopotliwy, o tyle dużym ograniczeniem jest sama lista osób uprawnionych. Drukuje się ją dla komisji wyborczej pracującej w wybranym lokalu wyborczym zgodnie z miejscem zameldowania osoby uprawnionej. Oznacza to, że głosujący może oddać swój głos tylko w miejscu, gdzie może zostać zweryfikowany, tzn. wyłącznie w jednym, określonym lokalu wyborczym (jeśli zgłosi ten fakt odpowiednio wcześniej, może to być inny lokal wyborczy niż wynikający z jego miejsca zameldowania).

Ciekawe jest, jak zostanie rozwiązany ten problem w momencie, kiedy zostanie zniesiony obowiązek meldunkowy (ma to nastąpić 1 stycznia 2018 roku[1]).

Zastosowanie metod głosowania wspieranego elektronicznie nie znosi tego ograniczenia, ponieważ weryfikacja następuje dokładnie w taki sam sposób. Różnica sprowadza się jedynie do tego, że głosujący zamiast papierowej karty do głosowania otrzymuje urządzenie elektroniczne, za pomocą którego może oddać swój głos.

[1] http://prawo.gazetaprawna.pl/artykuly/890858,wiemy-kiedy-zniknie-obowiazek-meldunkowy-prezydent-podpisal-ustawe.html.

Głosowanie w pełni elektroniczne pozwala na oddanie głosu z dowolnego miejsca przy wykorzystaniu dowolnego urządzenia, dla którego stworzono odpowiednią aplikację. W przypadku takiego sposobu głosowania pojawia się jednak duży problem związany z nadaniem uprawnień. Osoba chcąca oddać głos za pośrednictwem sieci Internet, musi zostać wstępnie zweryfikowana w celu nadania jej uprawnień, np. w postaci użytkownika i hasła. Wystarczy więc, że taka osoba uda się do odpowiedniej instytucji w celu dokonania weryfikacji swojej tożsamości oraz nadania uprawnień. Problem polega jednak na tym, że instytucja, weryfikując obywatela oraz nadając mu uprawnienia, gromadzi informacje pozwalające na jego późniejszą identyfikację, a tym samym zostaje zachwiana zasada tajności głosowania (głosujący, podając nazwę użytkownika i hasło, zostaje zidentyfikowany, a tym samym możliwe jest późniejsze powiązanie go z oddanym głosem).

Można zastosować model, w którym głosujący po weryfikacji danych otrzymuje (wybiera) dane pozwalające na jego późniejszą identyfikację jako uprawnionego, przy czym komisja posiadałaby jedynie informację, że dane logowania pozwalają na oddanie głosu, ale nie byłaby w stanie powiązać tych danych z konkretną osobą. Pojawia się tu jednak pewien zasadniczy problem. Co w sytuacji, kiedy osoba uprawniona zgłosiłaby fakt zgubienia danych do logowania? Ponieważ do osoby nie zostały te dane przypisane, więc nie wiadomo, który identyfikator należy wykluczyć z puli uprawnionych. Ponieważ danych nie można wykluczyć, mogą zostać one wykorzystane podczas głosowania (zgłaszający się po nowe uprawnienia może kłamać w kwestii zgubienia danych logowania w celu zdobycia dodatkowej możliwości oddania głosu lub dane te mogą zostać przejęte przez inną osobę, która je wykorzysta w dniu wyborów).

Jak widać, pojawia się konflikt między koniecznością gromadzenia informacji nt. nadanych uprawnień do głosowania a możliwością powiązania głosującego z jego głosem, co łamie zasadę tajności wyborów. Problem ten jest przez Autora opracowywany i zostanie opisany w odrębnej publikacji.

Częściowo (nie określono, co w sytuacji utraty danych uprawniających do logowania w systemie głosowania) rozwiązanie podaje zespół Prof. Kutyłowskiego[2]. W przedstawionym modelu osoba uprawniona zgłasza chęć oddania głosu przez Internet, co skutkuje wysłaniem pod jej adres zameldowania kuriera z zamkniętą kopertą zawierającą uprawnienia do oddania głosu (podobny mechanizm wykorzystywany jest np. w procesie zdalnego otwierania kont bankowych; w kopercie umieszczone są dane do logowania). Kurier ma określoną liczbę kopert (koperty są nierozróżnialne), z których adresat wybiera w sposób losowy jedną. Takie podejście powoduje, że wyborca otrzymuje uprawnienia, natomiast nadający uprawnienia (Komisja Uprawnień) gubi informację o tym, kto posługuje się jakimi danymi. Koperty są oczywiście drukami ścisłego zarachowania, tak by nie następował „wyciek" uprawnień.

[2] http://www.computerworld.pl/news/322273/E.voting.za.czy.przeciw.html.

W obecnych systemach wyborów realizowanych przez Internet wyborcy posługują się np. dowodami z podpisami kwalifikowanymi, co oczywiście ich jednoznacznie identyfikuje. W takim systemie pozostaje jedynie mieć nadzieję, że dwie oddzielne komisje, tzn. Komisja Wyborcza odpowiedzialna za zbieranie i zliczanie głosów oraz Komisja Uprawnień odpowiedzialna za nadawanie uprawnień wyborcom, nigdy nie wymienią się danymi w celu powiązania wyborcy z oddanym głosem.

Oczywiście istnieje jeszcze możliwość rezygnacji z tajności wyborów, co definitywnie rozwiązałoby ten problem. Wymagałoby to zmiany nastawienia wyborców oraz zmian w prawie.

3. Karty do głosowania

Karty do głosowania są jednym z najważniejszych elementów związanych z głosowaniem. To za ich pośrednictwem głosujący wybiera swojego kandydata bądź kandydatów. Zarówno w przypadku głosowania tradycyjnego, jak i wspomaganego elektronicznie sprawa wygląda tak samo: głosujący wskazuje swój wybór i go zatwierdza, wrzucając kartę do urny lub zapisując dane w aplikacji. Tu jednak zaczynają się pojawiać zasadnicze różnice.

W przypadku głosowania tradycyjnego komisja wyborcza weryfikuje i zlicza oddane głosy. Poprawność procesu zliczania głosów stanowi element zaufania względem komisji wyborczej. Głosujący nie ma żadnej możliwości weryfikacji, czy jego głos został zliczony poprawnie, a nawet czy w ogóle został zliczony. Zaufanie odnosi się nie tylko do celowych działań komisji wpływających na zmianę oddanych głosów (podmienione karty, głosy oddane jako nieważne itp.), lecz także do zdarzających się błędów ludzkich.

Głosowanie wspierane elektronicznie ma postawiony za jeden z celów możliwość weryfikacji oddanego głosu. Wyborca ma mieć możliwość śledzenia swojego głosu od momentu oddania go do momentu, kiedy głosy zostaną zliczone, a wyniki wyborów ogłoszone. W przypadku głosowania elektronicznego o błędzie ludzkim nie ma mowy. Mogą się za to pojawić błędy sprzętowe, błędy aplikacji czy celowe manipulacje głosami.

Karty do głosowania są ważnym elementem z punktu widzenia komitetów wyborczych z jeszcze jednej przyczyny. Powszechnie wiadomo, że każdy z komitetów wyborczych chce zajmować na listach wyborczych jak najwyższą pozycję, a każdy kandydat chce znajdować się na jak najwyższej pozycji w ramach danego komitetu wyborczego. Wynika to z bardzo prostej przyczyny. Wyborcy, którzy nie mają do końca zdefiniowanych preferencji, wybierają tych kandydatów, którzy na listach znajdują się najwyżej. Oznacza to, że największe szanse w wyborach mają ci kandydaci, którzy zajmują najwyższe pozycje na listach wyborczych.

Oczywiście w modelu w pełni elektronicznym można by zachować układ jednej karty do głosowania. Jednak z punktu widzenia bezpieczeństwa zdecydowanie lepszym rozwiązaniem jest tworzenie wielu kart do głosowania. Przyjęcie modelu, w którym kandydaci rozstawieni są na wielu kartach do głosowania, powoduje, że osoba zainteresowana fałszowaniem wyborów musiałaby się dowiedzieć nie tylko, jaki głos został oddany, lecz także która z kart została wykorzystana. Przykład: w wyborach startuje 100 kandydatów, tworzy się 100 kart do głosowania, a każdy z kandydatów zajmuje każdą z pozycji (kandydat X na karcie nr 1 jest na pozycji 5, na karcie nr 2 jest na pozycji 13, na karcie nr 3 jest na pozycji 27, itd., wypełniając wszystkie możliwe pozycje w ramach wszystkich kart). Oznacza to, że oddanie głosu na kandydata 16, nie niesie ze sobą żadnej informacji dla kogoś, kto nie wie, jaka karta do głosowania została wykorzystana. Układ kart można modyfikować, tworząc np. macierz, co skracałoby długość listy w przypadku dużej liczby kandydatów.

Tabela1

Przykład macierzy zawierającej nazwiska kandydatów

	A	B	C	D	E
1	K1	K11	K9	K8	K14
2	K1	K2	K7	K5	K20
3	K19	K12	K16	K15	K13
4	K4	K17	K3	K6	K18

Źródło: Opracowanie własne.

Wyborca oddawałby głos w postaci D3, co oznaczałoby wskazanie kandydata K15.

Kolejnym elementem zwiększającym bezpieczeństwo mogłoby być wstawianie tzw. ślepych kandydatów (pustych miejsc w ramach tworzonej macierzy – rozwiązanie, które jest niemożliwe w przypadku list tradycyjnych).

Tabela 2

Przykład macierzy zawierającej „ślepych kandydatów”

	A	B	C	D	E
1	K1		K9	K8	K14
2	K1	K2			
3	K19		K16	K15	K13
4		K17	K3		K18

Źródło: Opracowanie własne.

Gdyby dla tak przygotowanej karty komisja otrzymała głos wyborcy w postaci np. C2, byłoby pewne, że głos został zmodyfikowany na drodze wyborca-komisja.

Elektroniczne karty do głosowania mają jeszcze jedną zaletę – można dla nich ustawić parametry obowiązujące w ramach danych wyborów, np. dokonujemy wyboru jednego kandydata. Wyborca nie miałby możliwości oddania głosu nieważnego z powodu nieodpowiedniej liczby wybranych kandydatów, a jak pokazują wyniki np. z wyborów samorządowych w 2014 roku liczba głosów nieważnych wyniosła ponad 5 milionów na 14,5 miliona oddanych wszystkich głosów[3].

Wracając do kwestii kolejności kandydatów na kartach do głosowania, można, co oczywiście nie stanowi od strony programowej żadnego problemu, zastosować podejście dwuwarstwowe – warstwa wewnętrzna wykorzystywałaby opisane powyżej mechanizmy, warstwa zewnętrzna, widok dla wyborcy, byłaby przetworzeniem karty w taki sposób, aby zawsze wyglądała tak samo.

4. Bezpieczeństwo głosowania

Bezpieczeństwo wyborów realizowanych w pełni drogą elektroniczną jest jednym z podstawowych, o ile nie najważniejszym problemem do rozwiązania. To od poziomu bezpieczeństwa w dużej mierze wyborcy uzależniają chęć oddania głosu przez Internet. Pozytywnym sygnałem jest fakt stałego wzrostu zainteresowania obywateli e-usługami, w tym zakupami i płatnościami realizowanymi przez Internet[4]. Oznacza to, że wzrasta poziom zaufania do usług realizowanych drogą elektroniczną, maleją obawy przed nieuczciwymi sprzedawcami oraz obawy przed możliwością utraty pieniędzy na skutek oszustw czy kradzieży. Można więc przypuszczać, że wiele osób postawiłoby na e-wybory ze względu na wygodę, przyjmując tę formę za bezpieczną i bardziej przejrzystą (możliwość weryfikacji własnego głosu). Można jeszcze dodać, że w ankiecie przeprowadzonej przez bank ING wśród klientów bankowości elektronicznej na grupie ponad 37 tysięcy osób prawie 80% zadeklarowało chęć oddania swojego głosu w wyborach przez Internet[5].

Bezpieczeństwo komunikacji zapewniają metody kryptograficzne[6;7;8;9;10]. Wykorzystuje się metody klucza symetrycznego, klucza asymetrycznego oraz systemy certyfikacji. Każda

[3] http://wiadomosci.onet.pl/kraj/pkw-publikuje-statystyki-z-wyborow-samorzadowych-inny-odsetek-glosow-niewaznych/ghw3jz.
[4] Sobota M.: Społeczno-ekonomiczne aspekty głosowania elektronicznego. Zeszyty Naukowe Politechniki Śląskiej, seria: Organizacja i Zarządzanie, z. 86, Gliwice 2015, s. 519-526.
[5] http://media.ingbank.pl/pr/96284/ankieta-ing-wielkie-tak-ze-strony-klientow-ing-dla-wyborow-przez-internet.
[6] Stinson D.: Kryptografia. Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
[7] Pipkin D.: Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
[8] Anderson R.: Inżynieria zabezpieczeń. Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
[9] Sobota M., op. cit., s. 519-526.
[10] Sobota M.: E-voting cards based on SARG04 protocol. Internet in The Information Society, 2016. 11th International Conference Proceedings, Dąbrowa Górnicza 2016.

komunikacja jest realizowana przy wykorzystaniu klucza sesji, podobnie jak podczas komunikacji szyfrowanej w Internecie[11].

Autor proponuje rozwiązanie[12] wykorzystujące zmodyfikowany kwantowy protokół SARG04. Protokół ten opiera się na dwóch alfabetach: prostym i ukośnym. Nadawca (Komisja Wyborcza), kodując kolejno klasyczne 0 i 1 za pomocą polaryzacji światła, wysyła do odbiorcy (wyborca) identyfikator karty do głosowania. Wykorzystując protokół SARG04, strony uzgadniają, która z kart do głosowania zostanie wykorzystana i po tym uzgodnieniu wyborca oddaje swój głos. Silną stroną tej metody jest fakt, że każda próba podsłuchania, jaki identyfikator jest uzgadniany, wprowadza do komunikacji błędy pozwalające stwierdzić aktywność niepożądanej strony komunikacji (wynika to z praw mechaniki kwantowej). Jeżeli okazuje się, że identyfikator karty zostaje uzgodniony bez wystąpienia podsłuchu, to oznacza to, że oddany głos nie może zostać zidentyfikowany przez osobę trzecią (mechanizm został opisany w rozdziale 3). Pełen opis wykorzystania protokołu można znaleźć w pracy [7].

5. Podsumowanie

Głosowanie elektroniczne to przyszłość. Budowa wiarygodnego systemu spełniającego wysokie standardy bezpieczeństwa zgodnego z normami prawnymi oraz wygodnego dla użytkownika pozwoliłaby na sprawne przeprowadzanie wszelkiego rodzaju wyborów oraz np. referendów. Dzisiaj wybory czy referendum przeprowadzane tradycyjnymi metodami to olbrzymie i kosztowne przedsięwzięcie. Dobrze zbudowany system zapewniłby dużą elastyczność i skalowalność, mógłby być wykorzystywany wielokrotnie i do różnych celów, a w ostateczności znacznie obniżyłby koszt realizacji przedsięwzięć tego typu (początkowo koszt byłby wysoki, ale docelowo zniknęłyby lokalne komisje wyborcze i ich diety, lokale, czynsze za wynajem, druk kart do głosowania itd.). W zasadzie całkowity koszt sprowadzałby się do utworzenia i utrzymania centralnego systemu głosowania (zbieranie, zliczanie głosów, prezentacja wyników, udostępnianie aplikacji itp.), natomiast całą resztę stanowiłaby infrastruktura już istniejąca (sieci komputerowe rozległe oraz końcowe urządzenia wyborców, takie jak komputery stacjonarne, laptopy, tablety, smartfony itp.).

Istotnym elementem jest też możliwość znacznego ograniczenia – praktycznie do zera – możliwości oddania głosu nieważnego. Jeżeli we wspomnianych wcześniej wyborach samorządowych w 2014 roku głosy nieważne stanowiły ogromny odsetek (na ok. 14,5

[11] http://klub.platforma.org/files/raport.pdf.
[12] Sobota M.: E-voting cards based on SARG04 protocol. Internet in The Information Society, 2016. 11th International Conference Proceedings, Dąbrowa Górnicza 2016.

miliona oddanych głosów ponad 5 milionów to głosy nieważne)[13], to uniemożliwienie oddania głosu nieważnego mogłoby znacznie wpłynąć na wyniki wyborów.

Przeciwnicy wyborów realizowanych przez Internet zwracają głównie uwagę na możliwość fałszowania wyników wyborów, jednak z punktu widzenia modelu tradycyjnego wykorzystywanego dziś fałszowanie jest również możliwe, i to na każdym etapie wyborów – rozpoczynając od lokalnej komisji wyborczej, przez system zbierania i podliczania głosów po Główną Komisję Wyborczą. Należy zauważyć, że za każdym systemem stoi człowiek i to głownie od niego zależy, jak każdy system będzie funkcjonował.

Bibliografia

1. Anderson R.: Inżynieria zabezpieczeń. Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
2. Pipkin D.: Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
3. Sobota M.: Społeczno-ekonomiczne aspekty głosowania elektronicznego. Zeszyty Naukowe Politechniki Śląskiej, seria: Organizacja i Zarządzanie, z. 86, Gliwice 2015, s. 519-526.
4. Sobota M.: E-voting cards based on SARG04 protocol. Internet in The Information Society 2016. 11th International Conference Proceedings, Dąbrowa Górnicza 2016.
5. Stinson D.: Kryptografia. Wydawnictwa Naukowo-Techniczne, Warszawa 2005.
6. http://media.ingbank.pl/pr/96284/ankieta-ing-wielkie-tak-ze-strony-klientow-ing-dla-wyborow-przez-internet.
7. http://prawo.gazetaprawna.pl/artykuly/890858,wiemy-kiedy-zniknie-obowiazek-meldunkowy-prezydent-podpisal-ustawe.html.
8. http://www.computerworld.pl/news/322273/E.voting.za.czy.przeciw.html.
9. http://wiadomosci.onet.pl/kraj/pkw-publikuje-statystyki-z-wyborow-samorzadowych-inny-odsetek-glosow-niewaznych/ghw3jzhttp://klub.platforma.org/files/raport.pdf.
10. http://klub.platforma.org/files/raport.pdf.
11. http://wiarygodnewybory2014.blog.pl/?p=183.

Abstract

Electronic voting is the future. Construction of a reliable system that meets the high safety standards in accordance with legal norms and comfortable for the user would allow to conduct all kinds of elections and for example referenda. Nowadays, elections or referendum, carried

[13] http://wiarygodnewybory2014.blog.pl/?p=1836.

out by traditional methods is enormous and costly undertaking. Well-built system would provide flexibility and scalability, it could be used many times and for different purposes and ultimately could considerably decrease the cost of implementation of projects of this type (initial cost would be high but eventually there would be no local electoral commissions and their salaries, premises, rents for rent, printing voting cards etc.). In fact, the total cost would be limited to the creation and maintenance of a central voting system (collecting, counting of votes, presentation of results, sharing application etc.). The whole rest constitutes the infrastructure already existing (computer networks, extensive and terminal equipment of voters, such as desktops, laptops, tablets, smartphones, etc.).