



Stanowisko Stowarzyszenia Internet Society Poland w sprawie głosowania elektronicznego w wyborach powszechnych

styczeń 2007

streszczenie:

W mediach pojawiają się ostatnio informacje o inicjatywach wprowadzenia powszechnych elektronicznych form głosowania (w tym "przez internet"). Stowarzyszenie Internet Society Poland¹ analizuje je w świetle wymogów przejrzystości procedury wyborczej oraz nadziei na poprawę frekwencji wyborczej. Przedstawiono wybrane doniesienia o przypadkach manipulowania wynikami wyborczymi oraz kompromitacji elektronicznych maszyn wyborczych. Wskazano też na przykłady nasilającego się lobbingu producentów rozwiązań wspierających elektroniczne głosowania. Na ich tle zdaniem ISOC postulaty modyfikacji procedury wyborczej w kierunku dopuszczenia głosowania przez internet niosą ryzyko zagrożenia dla demokracji oraz wyeliminowania wyborców z procesu wyborczego.

1. Wstęp

Głosowanie elektroniczne uzależnia uczciwość procesu demokratycznego od skomplikowanych systemów komputerowych, w który wgląd ma tylko wąska grupa osób. Tym samym głosowanie elektroniczne znacząco zmniejsza przejrzystość procedury wyborczej w porównaniu z wyborami tradycyjnymi. Przykłady innych państw pokazują, że takie głosowanie nie wpływa w znaczący sposób na zwiększenie frekwencji.

Wybory są jedną z najważniejszych instytucji w demokracji. Sposób ich przeprowadzenia musi w oczach każdego obywatela gwarantować ich uczciwość, która jest podstawą prawidłowego funkcjonowania demokratycznego państwa.

System wyborczy jest osią demokracji i nawet najdrobniejsze jego zmiany trzeba analizować z najwyższą uwagą. Nasze stanowisko opieramy na doświadczeniu zawodowym członków stowarzyszenia oraz doświadczeniach międzynarodowych.

1. Internet Society (ISOC) propaguje rozwój Internetu i społeczeństwa informacyjnego. Do ISOC należy większość światowych pionierów Internetu. Oddziały ISOC działają w 150 krajach. W ramach Internet Society działają Internet Engineering Task Force (IETF) i Internet Architecture Board (IAB), które od zarania określają podstawowe standardy techniczne Internetu. Oddziały ISOC działają w 150 krajach i regionach świata. Serwis internetowy polskiego oddziału Stowarzyszenia: Internet Society Poland, znajduje się pod adresem <http://www.isoc.org.pl>

Konstytucja Rzeczypospolitej Polskiej gwarantuje, że wybory do Sejmu, Senatu oraz prezydenckie są powszechne, bezpośrednie i odbywają się w głosowaniu tajnym (art. 96, 97 i 127). Od strony technicznej wymienia się następujące warunki, jakie powinny gwarantować procedury wyborcze: anonimowość i tajność wyborów, brak możliwości sprzedaży głosu, prawidłowość wyników i weryfikowalność wyników przez wyborcę².

Wybory elektroniczne to pojęcie obejmujące szeroki zakres zastosowań technik informatycznych w referendach oraz wyborach powszechnych.

1. **Elektroniczna wizualizacja wyników wyborów** – systemy komputerowe pełnią rolę pomocniczą przy prezentacji i wizualizacji wyników wyborów przeprowadzonych tradycyjnie.

2. **Głosowanie wspomagane elektronicznie** – systemy komputerowe są głównym narzędziem służącym do przyjmowania i zliczania głosów. Głosy są oddawane przez wyborców osobiście w lokalach wyborczych na dedykowanych komputerach wyborczych (tzw. „voting machines”).

3. **Głosowanie przez internet** – głosy są oddawane zdalnie z dowolnej lokalizacji za pomocą Internetu, a ich przyjmowaniem i zliczaniem zajmuje się centralny komputerowy system wyborczy.

Polskie Krajowe Biuro Wyborcze od kilku lat stosuje wizualizację wyników wyborów oraz komputerowe wspomaganie przekazywania wyników z jednostek terenowych do centrali krajowej. Systemy informatyczne nie są jednak jedynym ani głównym mechanizmem składania i zliczania głosów – są nim komisje wyborcze. Wiążącymi wynikami wyborów są wyniki opublikowane przez Krajowe Biuro Wyborcze na podstawie ręcznego liczenia głosów przez każdą z komisji (przykładowo dla wyborów do Sejmu i Senatu RP: art. 70, ust. 1 ustawy Ordynacja Wyborcza do Sejmu Rzeczypospolitej Polskiej i do Senatu Rzeczypospolitej Polskiej³), zaś sieć komputerowa służy jedynie do ich przesyłania (art. 41, ust. 1 ustawy⁴).

Część krajów europejskich jak i USA wdrożyły różne formy głosowania wspomaganego elektronicznie lub głosowania przez Internet. Większość wdrożyła jedynie głosowanie wspomagane elektronicznie czyli głosowanie przy pomocy komputerów z ekranem dotykowym, ustawionym w lokalu wyborczym (USA, Brazylia, Belgia). Jedynie nieliczne (Estonia) wdrożyły głosowanie przez Internet.

2. Przejrzystość procedury wyborczej

Doświadczenia z czasów PRL („3 razy tak”), fałszerstwa wyborcze na Ukrainie w 2004 roku⁵, w niektórych republikach Federacji Rosyjskiej (Czeczenia⁶) oraz liczne problemy wyborcze w USA⁷ pokazują, że krytyczny dla uczciwości wyborów jest niezależny audyt prac komisji wyborczych.

2. Por. Tabela „Porównanie procedur wyborczych w wybranych krajach, z uwzględnieniem zastosowania elektronicznych metod głosowania”, 2 stycznia 2006, <http://www.computerworld.pl/artykuly/50398.html>; W tabeli uwzględniono takie parametry jak: Model zaufania, Weryfikacja, Możliwość dorzucenia głosów, Możliwość unieważnienia głosu, Możliwość usunięcia głosu, Poziom anonimowości, Sprzedawanie głosów, Podatność na atak DOS/DDOS, Zagrożenie wirusowe.

3. Dziennik Ustaw z 2001 roku Nr 46, poz. 499 z późn. zm.

4. *ibidem*

5. Według oficjalnych wyników Ukraińskiej Centralnej Komisji Wyborczej, pierwszą turę wyborów, która odbyła się 31 października 2004 wygrał Wiktor Juszczenko zdobywając 39,87% głosów, Wiktor Janukowycz zdobył wówczas 39,32% głosów. Janukowycz wygrał drugą turę wyborów z 49,42% głosów (Juszczenko 46,7%) i został prezydentem-elektem Ukrainy. Wyniki te jednak dalece odbiegały od wyników *exit polls* i nie zostały uznane przez opozycję ani przez międzynarodowych obserwatorów z OBWE.

6. 27 listopada 2005 roku odbyły się wybory do dwuizbowego parlamentu Czeczenii, które - według Kremla - były ostatnim etapem formowania legalnych władz republiki. Zgodnie ze wstępnymi wynikami wygrała je Wspólna Rosja, zdobywając ponad 60% głosów. Wyborów nie uznali czeczeńscy separatyści, nazywając je farsą. Por. "Czeczenia: wybory pod dyktando Ramzana Kadyrowa", Ośrodek Studiów Wschodnich, 1 grudnia 2005, <http://osw.waw.pl/pub/koment/2005/12/051201a.htm>

7. Omówienie wybranych przypadków w dalszej części opracowania.

W polskim systemie wyborczym audyt procesu wyborczego jest gwarantowany przez instytucje mężów zaufania, których uprawnienia umożliwiają weryfikowanie prac komisji wyborczej. Instytucja męża zaufania ma zapewniać niezależny audyt i przejrzystość prac komisji w celu zapobieżenia nadużyciom. Prawo do wystawienia swojego męża zaufania przez każdą zainteresowaną stronę (partia polityczna, kandydat) i umieszczenia go w każdej komisji gwarantuje, że zmiana wyników wyborów na poziomie komisji wyborczych jest znacznie utrudniona⁸.

Przy tradycyjnych wyborach z wykorzystaniem kart do głosowania, urn oraz ręcznego zliczania głosów mężowie zaufania mają pełny wgląd w prace komisji. Każdy mąż zaufania, niezależnie od wykształcenia i doświadczenia, może sprawdzić urnę, karty do głosowania i wynikowe protokoły oraz obserwować prace komisji. Dzięki łatwości wykonania procedury weryfikacji możliwe jest wydelegowanie dostatecznej liczby mężów zaufania, by skontrolować każdą komisję wyborczą. Dzięki tym cechom, w tradycyjnych wyborach proces głosowania jest więc niemal całkowicie przejrzysty.

Przy wyborach wspomaganych elektronicznie lub prowadzonych przez internet, czyli tam gdzie przyjmowaniem i zliczaniem głosów zajmują się systemy informatyczne, przejrzystość procesu głosowania dla mężów zaufania jest niemal zerowa. Nie mogą oni samodzielnie monitorować procesu zbierania i liczenia głosów, ponieważ odbywa się on w „czarnych skrzynkach” jakimi z ich punktu widzenia są komputery wyborcze. Oczywiście, przeanalizowanie działania takiego systemu jest teoretycznie możliwe – ale jest czynnością dostępną tylko wąskiej grupie wykwalifikowanych specjalistów, niezwykle czasochłonną, kosztowną i zawsze pozostawiającą pewien margines niepewności.

Przykłady nieprawidłowości w wyborach elektronicznych pokazują, że procedura ta kosztuje zwykle znacznie więcej niż zakładano, a mimo to ma poważne luki (przypadek irlandzki, przypadek Cyber Inc - omówione niżej). Ponadto niezwykle trudne jest przeprowadzenie weryfikacji przebiegu wyborów bez pogwałcenia tajności głosowania. W związku z tym głosowanie elektroniczne oznacza znaczące ograniczenie jawności procesu wyborczego w porównaniu z głosowaniem tradycyjnym, a co za tym idzie - znaczne ryzyko dla uczciwości głosowania⁹.

3. Głosowanie internetowe a frekwencja

Jednym z głównych argumentów wysuwanych na rzecz wyborów elektronicznych jest nadzieja na radykalną poprawę frekwencji wyborczej dzięki łatwiejszej dostępności narzędzi do głosowania, zwiększeniu atrakcyjności aktu wyborczego oraz zainteresowania obywateli jego formą. Głosowanie „przez internet” jako swoista recepta na zwiększenie frekwencji wyborczej postulowane jest m.in. przez Instytut Spraw Publicznych¹⁰, wprowadzenie takiej formy głosowania publicznie postuluje również senator Dariusz

8. Znacznie trudniej też zmanipulować wybory w licznych komisjach wyborczych w porównaniu ze scentralizowanym, elektronicznym systemem zbierania głosów.

9. W dostępnych opracowaniach brak na razie analiz wpływu tzw. „retencji danych telekomunikacyjnych” na swobodne wykonywanie prawa wyborczego w ew. wyborach przeprowadzonych „przez internet”; Retencja danych telekomunikacyjnych wynika m.in. z polskiej ustawy Prawo telekomunikacyjne, która stanowi w art. 165 ust. 1, iż: „operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać przez okres 2 lat...”. Ministerstwo Sprawiedliwości postulowało wcześniej wprowadzenie 15 letniego okresu retencji danych telekomunikacyjnych, co jednak spotkało się z krytyką opozycji w Sejmie. Warto też nadmienić, że w Unii Europejskiej przyjęto 15 marca 2006 kontrowersyjną Dyrektywę 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE. Informacje na temat retencji danych telekomunikacyjnych gromadzone są m.in. pod adresem: http://prawo.vagla.pl/retencja_danych

10. D. Uhlig, Internet i centra handlowe zwiększą frekwencję? 28 października 2005, <http://serwisy.gazeta.pl/wyborcza/1,34513,2989687.html>; tam m.in. na temat głosowania korespondencyjnego i „przez internet”: „według Kazimierza Czaplickiego to nie utopia - koszt przygotowania elektronicznego rejestru wyborców potrzebnego do wprowadzenia głosowania elektronicznego ocenił na 1,6 mln zł.”; por. również A.

Bachalski z Platformy Obywatelskiej¹¹, a także Stowarzyszenie Polska Młodych, które rozpoczęło kampanię na rzecz zebrania 100 tys podpisów pod obywatelskim projektem nowelizacji Ordynacji Wyborczej, w celu wprowadzenia przepisów umożliwiających głosowanie „przez internet”¹².

Jedynym krajem europejskim, który wprowadził głosowanie przez internet, jest Estonia. Jej doświadczenia pokazują, że mimo ogromnego kosztu dostępność głosowania elektronicznego tylko w minimalnym stopniu zwiększyła frekwencję – elektronicznie oddano 1,84% głosów (9 tys. głosów elektronicznych z 500 tys. głosów w wyborach samorządowych w 2005 roku przy frekwencji 47%¹³).

Przyczyną tak nikłego zainteresowania były prawdopodobnie bardzo wysokie wymagania wobec komputerów i osób chcących głosować elektronicznie. Te wysokie wymagania pomija się w większości publikacji powołujących się na „estoński sukces”. Potwierdzenie tożsamości głosującego musiało odbywać się za pomocą karty kryptograficznej, a ta wymagała specjalnego czytnika oraz dodatkowego oprogramowania.

Wymagania te znacznie przewyższają standard, do którego przyzwyczajeni są użytkownicy internetu, na przykład w bankowości internetowej. Zapewne z tego powodu w Estonii elektronicznie głosowało niecałe 2% wyborców, choć ogólne poparcie dla tego pomysłu deklarowało ponad 85% ankietowanych.

Z drugiej strony nie można obniżyć wymagań wobec uwierzytelnienia wyborców, jeśli głosowanie ma być bezpieczne. Nadużycia w systemach e-bankowych (np. *phishing*¹⁴) są zjawiskiem powszechnym (tylko w 2004 roku w USA skradziono w ten sposób 80 mln dolarów¹⁵) i straty te są pokrywane z ubezpieczeń budowanych na podstawie analizy ryzyka¹⁶. W przypadku nadużyć w systemie wyborczym

Stankiewicz, e-wybory czyli głosowanie przez Internet, Rzeczpospolita, 28 października 2005; autor tekstu pisze m.in., że „już np. Brytyjczycy, Belgowie, Szwajcarzy, Amerykanie i Estończycy głosują przez internet”, co jest - naszym zdaniem - stwierdzeniem dalece nieprecyzyjnym.

11. Komputer jak długopis w wyborach. Życie Warszawy. 29 sierpnia 2006. W artykule cytowany jest również dr Robert Sobiech, socjolog, który wskazuje na badania, zgodnie z którymi przyczyny absencji wyborczej nie wynikają jedynie z niemożności dotarcia do komisji wyborczych. W artykule omówiony jest też pomysł stowarzyszenia Collegium Cogitantium (por. dalej)
12. Stowarzyszenie Polska Młodych w swoich materiałach związanych z kampanią dotyczącą e-votingu w Polsce (umieszczonych pod adresem <http://www.polskamlodych.pl/>) pisze: "*Internautów uprawnionych do głosowania jest w Polsce 7 565 006. Ponad 2/3 z nich deklaruje, że korzysta z tego prawa. Skoro wirtualna rzeczywistość jest tak popularnym medium to dlaczego nie wykorzystać jej w życiu publicznym?*". W innym miejscu zaś: "*Rozwiązania, które proponujemy oparte są na technologiach wykorzystywanych przez – bardzo popularną w Polsce - bankowość internetową. Według ekspertów są one w pełni bezpieczne*". W dalszej części opracowania wykażemy, iż głosowanie elektroniczne opiera się na innych zasadach niż e-banking, a także to, iż bankowość elektroniczna nie jest pozbawiona zagrożeń, a więc nie jest tak bezpieczna, jak chcieliby to widzieć przedstawiciele stowarzyszenia. Stowarzyszenie Polska Młodych związane jest z występującym we wcześniej cytowanym w materiałach stowarzyszeniem Collegium Cogitantium.
13. Municipal elections 2005, Report on Internet Voting (raport dostępny na stronach estońskiej Państwowej Komisji Wyborczej, <http://www.vvk.ee/engindex.html>)
14. kradzież tożsamości, oszukańcze pozyskanie poufnej informacji osobistej, jak hasła czy szczegóły karty kredytowej, np. przez udawanie osoby godnej zaufania.
15. P. Krawczyk, Ukradli 3 mln zł przez internet, 1 marca 2006, <http://www.idg.pl/news/89746.html>; w artykule mowa jest również o kradzieży 3 milionów złotych z jednego z polskich banków. W tej sprawie oskarżono dwudziestu mieszkańców Szczecina.
16. Odpowiedzialność użytkownika i banku za nieautoryzowane transakcje, m.in. dokonane za pośrednictwem internetu, reguluje ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych. Jeżeli z powodu niewystarczających zabezpieczeń technicznych komuś udało się dokonać elektronicznego "fraudu", klienci banków mogą żądać od banku zwrotu skradzionych pieniędzy. Tylko w tygodniu poprzedzającym wydanie tego stanowiska w mediach informowano o licznych błędach w polskich serwisach bankowości elektronicznej: M. Bednarek, PKO BP też mógł mieć problem z hakerami, Gazeta Prawna Nr 7 (1877) 2007-01-10: "*...bank poinformował, że opisywany przypadek nie dotyczy bankowości elektronicznej PKO Inteligo, tylko serwisu informacyjnego na portalu internetowym banku*"; M. Bednarek, Bank Millennium: nasz system jest bezpieczny, Gazeta Prawna Nr 6 (1876) 2007-01-09: "*...zdaniem serwisu iHACK.pl – pozwala na wykradzenie informacji na temat klienta banku aktualnie korzystającego z bankowości on-line*"; Wcześniej zaś w serwisie Hacking.pl publikowano doniesienia o lukach w systemie bankowości elektronicznej mBanku: Bezpieczeństwo klientów

konsekwencje są trwałe i nieodwracalne. Trudno je również wycenić dla potrzeb ewentualnej rekompensaty finansowej¹⁷.

4. Głosowanie zdalne a sprzedaż głosów

W każdym przypadku głosowania zdalnego – czy to listownego czy internetowego – zagrożona jest tajność głosu i niezawisłość wyborcy, ale pojawia się również problem z uwierzytelnieniem, czyli potwierdzeniem tożsamości wyborcy, które zawsze wykonywane jest w tradycyjnym lokalu wyborczym poprzez sprawdzenie dokumentu tożsamości. Doświadczenia światowe pokazują, że w przypadku głosowania listownego takie nadużycia mogą mieć miejsce – np. podczas wyborów w Birmingham¹⁸ domokrażcy skupowali karty do głosowania pocztowego w cenie 1 funta.

Internet daje tutaj większe możliwości zabezpieczenia dzięki zastosowaniu silnych i osadzonych w systemie prawnym mechanizmów kwalifikowanego podpisu elektronicznego. Niemniej ich zastosowanie generuje dodatkowe, wymierne koszty po stronie klienta (komputer, oprogramowanie, karta kryptograficzna, czytnik i sam certyfikat) oraz tworzy kolejną barierę technologiczną przy realizowaniu praw obywatelskich.

Wspomniana wyżej praktyka estońska pokazuje, że jest to bariera, która praktycznie niweluje sens głosowania internetowego jako narzędzia zwiększającego dostępność wyborów. W Estonii dowody osobiste z certyfikatem kwalifikowanym posiada prawie połowa z 1,3 mln populacji (dla porównania – w Polsce na 38 mln obywateli wydano ok. 20 tys. certyfikatów¹⁹). Koszty poniesione na stworzenie równoległego z tradycyjnym systemem głosowania internetowego wydają się zatem niewspółmierne do osiągniętego rezultatu czyli mniej niż 2% oddanych za pośrednictwem internetu głosów.

5. Nieprawidłowości w głosowaniach elektronicznych

Zarzuty odnośnie sfalszowania wyborów lub możliwych nieprawidłowości w głosowaniu elektronicznym podnoszono wielokrotnie w Stanach Zjednoczonych a także w innych krajach, gdzie prowadzi się wybory wspomagane przez komputery wyborcze (Holandia, Irlandia, Włochy).

Wymienione poniżej przykłady nieprawidłowości towarzyszące wyborom przeprowadzanym elektronicznie wskazują, że brak pewności co do dokładności zliczanych głosów, podejrzenia o manipulację wynikami wyborów i nieprzejrzystość procedur wyborczych są jak na razie raczej standardem niż wyjątkiem. W przypadku pojawienia się wątpliwości niemożliwe lub znacząco utrudnione jest też zweryfikowanie wyników wyborów (powtórne liczenie).

Przypadek Clintona Curtisa

W 2000 roku amerykański programista Clinton Curtis²⁰ miał napisać na zlecenie firmy Yang Enterprises będącej producentem maszyn do głosowania oprogramowanie o charakterze konia trojańskiego, służące do niezauważalnego fałszowania wyników zebranych przez daną maszynę. Curtis opublikował oświadczenie w tej sprawie w grudniu 2004 roku.

mBanku zagrożone!, 3 stycznia 2007, <http://hacking.pl/6351>; mBank zareagował na te doniesienia oświadczeniem, zgodnie z którym "przy wystąpieniu szczególnych okoliczności istniało prawdopodobieństwo wykorzystania przez oszustów internetowych pewnego pola do nadużyć, polegającego na umożliwieniu przeglądania danych klientów".

17. Por. również Raport Zespołu Bezpieczeństwa PCSS pt. „Bezpieczna” E-Bankowość, 20 lutego 2006, http://security.psnc.pl/reports/e-banking_polska_ssl_report.pdf

18. B. Mason, Voting scandal mars UK election, 5 kwietnia 2005 r., http://news.bbc.co.uk/2/hi/uk_news/4410743.stm

19. por. Stanowisko ISOC Polska w sprawie barier podpisu elektronicznego w Polsce z 18 maja 2006 r., http://www.isoc.org.pl/bariery_podpisu_elektronicznego

20. Clint Curtis, hasło w Wikipedii, Wolnej Encyklopedii: http://en.wikipedia.org/wiki/Clint_Curtis

Promieniowanie z nieba?

W maju 2003 roku podczas głosowania z użyciem komputerów wyborczych DigiVote w Belgii jedna z kandydatek otrzymała nadmiarowe 4 tys. głosów nie oddanych przez żadnego wyborcę. Oficjalnie fenomen ten wyjaśniono „przypadkowym i spontanicznym przestawieniem się bitu” w liczniku znajdującym się w pamięci komputera z niewyjaśnionych powodów – później tłumaczono to m.in. działaniem promieniowania kosmicznego²¹.

Raport naukowców w sprawie urządzeń Diebold

We wrześniu 2003 roku powołana przez stan Maryland komisja SAIC²² opublikowała raport wskazujący na liczne problemy z bezpieczeństwem urządzeń DIEBOLD²³.

Dziennikarze i źródła

W 2003 roku dziennikarka Bev Harris znalazła na stronach firmy DIEBOLD kod źródłowy komputerów wyborczych AccuVote TS 4. Latem 2003 roku grupa naukowców (m.in. znany kryptolog Avi Rubin) po przeanalizowaniu ujawnionego kodu opublikowała obszerny raport, w którym ujawniła poważne luki w bezpieczeństwie wyborów oraz prywatności wyborców²⁴.

Generator liczb losowych

Przeprowadzony w 2004 roku niezależny audyt kodu źródłowego belgijskiego oprogramowania DigiVote ujawnił szereg błędów programistycznych m.in. błędy w generatorze liczb losowych mogące naruszyć prywatność wyborcy²⁵.

Belgijskie raporty

W 2004 roku dwa stowarzyszenia belgijskie – Pour EVA oraz Université Libre de Bruxelles opublikowały oświadczenia w sprawie wyborów wspomaganych elektronicznie w Belgii. Pierwsze z nich skrytykowało uzależnienie demokratycznych wyborów od uczciwości jednej, prywatnej firmy. Drugie wskazało na wciąż zdarzające się błędy w komputerach wyborczych są możliwe, wbrew deklaracjom producentów składanym przed wyborami²⁶.

-
21. Electronic Voting Random Spontaneous Bit Inversion Explained, <http://wiki.ael.be/index.php/ElectronicVotingRandomSpontaneousBitInversionExplained>, por. również RAPPORT CONCERNANT LES ÉLECTIONS DU 18 MAI 2003, <http://www.poureva.be/IMG/pdf/RapportExpert20030605.pdf> oraz Le Ministre DEWAELE reconnaît la faillibilité du vote électronique grâce à un rayon cosmique complice! Zoé GENOT (Ecolo) nous communique sa question orale au Parlement, http://www.poureva.be/article.php?id_article=36
 22. Science Applications International Corporation, <http://www.saic.com>
 23. Risk Assessment Report Diebold AccuVote-TS Voting System and Processes, September 2, 2003, <http://www.verifiedvoting.org/downloads/votingsystemreportfinal.pdf>
 24. T. Kohno, A. Stubblefield, A. D. Rubin, D. S. Wallach, Analysis of an Electronic Voting System, February 27, 2004; Raport opublikowany w ramach IEEE Symposium on Security and Privacy 2004 oraz pod adresem: <http://avirubin.com/vote.pdf>
 25. Raport "Both 2003 and 2004 versions of DigiVote contain major errors that compromise the anonymity of the voting procedure", <http://www.afront.be/lib/vote.html>
 26. BE: E-elections 2004: Belgium's e-voting operations considered successful, eGovernment News – 16 June 2004 – Belgium – eDemocracy & eInclusion; materiały opublikowane w europejskim serwisie grupy IDABC pod adresem <http://ec.europa.eu/idabc/en/document/2634/358>

Zgubiono 4,4 tys. głosów

W 2004 roku w hrabstwie Carteret w Północnej Karolinie doszło do bezpowrotnego zgubienie 4,4 tys. głosów przez komputery wyborcze UniLect Patriot ze świeżo zaktualizowanym oprogramowaniem producenta²⁷.

Kontrowersyjne wybory prezydenckie w USA

Wybory prezydenckie w USA w 2004 roku wzbudziły wiele kontrowersji w związku z zgłoszonymi i rzekomymi nieprawidłowościami w działaniu elektronicznych systemów wyborczych²⁸.

System za 52 miliony euro nie daje gwarancji

W 2004 roku irlandzkie władze przygotowując się do wyborów do Parlamentu Europejskiego zakupiły za 52 mln euro komputery wyborcze NEDAP. Później, pod naciskami organizacji pozarządowych i opozycji powołano Commission on Electronic Voting (CEV²⁹), której zadaniem była ocena wybranego rozwiązania. Komisja oceniła że system nie daje gwarancji tajności i dokładności wyborów, wymaganych przez ordynację wyborczą w związku z czym zrezygnowano z jego użycia w wyborach. Od tej pory na roczne utrzymanie bezużytecznego sprzętu wydawane jest ok. 800 tys euro rocznie³⁰.

Demonstracja fałszerstwa

W czerwcu 2005 roku Jon Sancho, mąż zaufania w hrabstwie Leon na Florydzie, wraz ze specjalistą Harrym Hursti zademonstrowali w praktyce fałszerstwo wyborcze na komputerach wyborczych DIEBOLD, dokonane przy pomocy odpowiednio spreparowanych kart wyborczych. Według producenta takie fałszerstwo miało być niemożliwe³¹.

Wielka Brytania porzuca plany wprowadzenie e-votingu

We wrześniu 2005 rząd Wielkiej Brytanii ogłosił, że porzuca plany wprowadzenia głosowania zdalnego przez Internet i SMS, uzasadniając to większymi kosztami i większym ryzykiem nadużyć niż w przypadku głosowania tradycyjnego a nawet przez pocztę³².

Nie pokażemy źródeł

W grudniu 2005 roku firm DIEBOLD odmówiła przekazania kodu źródłowego swoich komputerów wyborczych komisji powołanej przez stan Północna Karolina w celu dokonania niezależnego audytu³³.

-
27. Response to Jim Dickson's Recent Statements to Authorities, <http://www.votersunite.org/info/responsetodickson.asp>; Jim Dickson pełnił wówczas funkcję wiceprezesa Governmental Affairs of the American Association of People with Disabilities (AAPD, <http://www.aapd-dc.org>).
28. 2004 United States presidential election controversy, voting machines, hasło w Wikipedii, Wolnej encyklopedii: http://en.wikipedia.org/wiki/2004_United_States_presidential_election_controversy%2C_voting_machines
29. Commission on Electronic Voting, <http://www.cev.ie>
30. Electronic voting in Ireland, hasło w Wikipedii, Wolnej encyklopedii: http://en.wikipedia.org/wiki/Electronic_voting_in_Ireland
31. Zbiór pism wysłanych przez przedsiębiorstwo Diebold do Iona Sancho dostępny jest pod adresem: <http://www.bbvfforums.org/forums/messages/2197/10535.html>
32. P. Waglowski, Rząd brytyjski porzuca plany zdalnych wyborów - jeszcze nie czas na e-voting, 8 września 2005, <http://prawo.vagla.pl/node/5474>; por. również dział poświęcony wyborom serwisu VaGla.pl Prawo i Internet: <http://prawo.vagla.pl/wybory>
33. P. Krawczyk, Diebold nie odda źródeł, 1 grudnia 2005, <http://security.computerworld.pl/news/85762.html>

Polska nauka a e-voting

W czerwcu 2006 we Freiburgu zespół prof. dr hab. Mirosława Kutyłowskiego³⁴ zademonstrował metody zarażania oprogramowania służącego do składania głosów przez Internet, tak aby w sposób niezauważalny dla głosującego, bez generowania dodatkowej komunikacji informacje o przesłanym głosie były dostępne dla atakującego. Atak dotyczył znanych i uważanych za bezpieczne protokołów kryptograficznych³⁵.

Procedury testowania a uprawnienia certyfikacyjne

Latem 2006 amerykańska komisja Election Assistance Commission odebrała uprawnienia certyfikacyjne firmie Cyber Inc., która zajmowała się m.in. testowaniem bezpieczeństwa amerykańskich systemów wyborczych. Przyczyną odebrania uprawnień były zaniedbania w procedurach testowych, gwarantujących uczciwość głosowań. Decyzja o odebraniu uprawnień została upubliczniona jednak dopiero w styczniu 2007 roku³⁶.

Nieautoryzowane oprogramowanie

W sierpniu 2006 stowarzyszenie Open Voting Foundation³⁷ ujawniło, że komputery wyborcze DIEBOLD umożliwiają trywialne załadowanie nieautoryzowanego oprogramowania³⁸.

Naukowcy kręcą filmy pokazujące kompromitację maszyn wyborczych

We wrześniu 2006 grupa prof. Eda Felten z Uniwersytetu Princeton opublikowała obszerny raport na temat bezpieczeństwa komputerów wyborczych DIEBOLD AccuVote-TS, przeprowadzony na podstawie analizy produkcyjnego egzemplarza urządzenia, bez dostępu do kodu źródłowego. Zespół wskazał na szereg błędów w zabezpieczeniach, umożliwiających m.in. zainstalowanie w nich nieautoryzowanego oprogramowania modyfikującego wyniki głosowania³⁹.

Anonimowe źródła dostarczają dyskietki

W październiku 2006 zatrudniona w Fundacji Freemana aktywistka Cheryl C. Kagan (wcześniej związana z administracją prezydenta Clintona) otrzymała z anonimowego źródła kod źródłowy oprogramowania komputerów wyborczych DIEBOLD BallotStation oraz GEMS, wraz z notatką krytykującą bezpieczeństwo tych systemów oraz politykę producenta. Przesłanie dyskietki do fundacji doprowadziło do wszczęcia śledztwa FBI⁴⁰.

34. Dokumentacja związana z pracami wrocławskich naukowców dostępna jest w dedykowanym serwisie Instytutu Matematyki i Informatyki Politechniki Wrocławskiej: <http://e-voting.im.pwr.wroc.pl/>

35. M. Gogolewski, M. Klonowski, P. Kubiak, M. Kutyłowski, A. Lauks, F. Zagórski, Kleptographic Attacks on E-Voting Schemes, czerwiec 2006, http://zagorski.im.pwr.wroc.pl/felippo/papers/Kleptographic_Attacks_on_E-Voting_Schemes.pdf

36. C. Drew, U.S. Bars Lab From Testing Electronic Voting, The New York Times, January 4, 2007: <http://www.nytimes.com/2007/01/04/washington/04voting.html>

37. Open Voting Foundation, <http://openvotingfoundation.org/>

38. A. Dechert, Worst ever security flaw found in Diebold TS Voting machine, 6 sierpnia 2006, http://openvotingfoundation.org/tiki-read_article.php?articleId=1

39. A. J. Feldman, J. A. Halderman, E. W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine; <http://itpolicy.princeton.edu/voting/>, Integralną częścią opracowanego raportu jest film video, obrazujący możliwości manipulacji maszynami wyborczymi.

40. L. H. Lamone, At the Center of the Election Maelstrom. State Elections Chief Draws Array of Critics, Washington Post, 22 września 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/21/AR2006092101594.html>; P. Wagłowski, Kody źródłowe maszyn wyborczych Diebolda w rękach demokratów, 23 października 2006, <http://prawo.vagla.pl/node/6761>

Instalacja nieautoryzowanego oprogramowania w telewizji

W październiku 2006 holenderskie stowarzyszenie WWSN⁴¹ zademonstrowało w programie telewizyjnym instalację nieautoryzowanego oprogramowania i fałszowanie wyników głosowania w komputerach wyborczych firmy NEDAP⁴².

Jakie państwo kontroluje proces wyborczy?

W listopadzie 2006 gazeta Washington Post opublikowała artykuł wskazujący na to, że właścicielem firmy Smartmatic produkującej popularne komputery wyborcze Sequoia jest wenezuelska grupa Bizta, w której z kolei 30% udziałów ma rząd Wenezueli. Wzbudziło to obawy odnośnie potencjalnych manipulacji wynikami wyborów, jakich tą drogą mógłby dokonywać otwarcie wrogi wobec USA rząd Wenezueli⁴³.

Proces sądowy po ostatnich wyborach do Kongresu USA

29 grudnia 2006 amerykański sąd odmówił Christiane Jennings prawa do wglądu w kod źródłowy maszyn obsługujących głosowanie elektroniczne w ostatnich wyborach do Kongresu w niektórych hrabstwach stanu Floryda, tłumacząc to koniecznością ochrony tajemnicy handlowej producenta. Christiane Jennings uzasadniała swoją prośbę niezwykle wysoką liczbą pustych głosów, co jej zdaniem sugeruje, że maszyny "zgubiły" część głosów. W wyborach tych kandydat Republikanów, Vern Buchanan, wygrał przewagą jedynie 369 głosów. Przedmiotem sporu są maszyny z ekranami dotykowymi, które obsługiwały wybory w hrabstwie Sarasota. W hrabstwie tym odnotowano 18000 pustych głosów (prawie 15%), zdecydowanie więcej niż w równoległych wyborach do Senatu i na stanowisko gubernatora stanu⁴⁴.

Organizacje dokumentują

Powyżej wymieniono tylko wybrane przypadki, w rzeczywistości było ich znacznie więcej:

Stowarzyszenie Campaign for Verifiable Voting in Maryland udokumentowało setki przypadków zgubienia lub niezgodności w wynikach głosowań oraz tysiące przypadków zawieszenia, zresetowania lub niemożności uruchomienia komputerów do głosowania w USA w latach 2002-2006. W ich wyniku stracono tysiące godzin pracy lokali wyborczych⁴⁵.

Stowarzyszenie Voters Unite udokumentowało liczne przypadki utraty głosów i innych błędów w komputerach wyborczych dziewięciu producentów stosowanych w USA – ES&S, Diebold, Sequoia, MicroVote, AVS/WINvote, Hart Intercivic, Unilect, Danaher, VTI. Niemal wszystkie posiadały wymagane prawem certyfikaty bezpieczeństwa⁴⁶.

41. WWSN to skrót od nazwy grupy, której pełna nazwa brzmi: "Wij vertrouwen stemcomputers niet" (nie ufamy komputerom do głosowania); <http://www.wijvertrouwenstemcomputersniet.nl>.

42. P. Krawczyk, Dziura w komputerach do głosowania NEDAP, 9 października 2006, <http://security.computerworld.pl/news/100729.html>; NEDAP voting machines hacked, 5 października 2006, <http://connect.educase.edu/taxonomy/term/2801>; Reportaże telewizyjne oraz inne materiały video poświęcone działaniom WWSN dostępne są m.in. w serwisie YouTube, por. AT5 item about SDU newvote voting computer back to use, <http://youtube.com/watch?v=DNkdIOKItgk>

43. Z. A. Goldfarb, Voting Machine Firm Denies Chavez Ties. Smartmatic Asked for Federal Review; The Washington Post, 31 października 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/30/AR2006103001224.html>

44. Judge rules against Jennings, Democrats to seat Buchanan, 29 grudnia 2006, <http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061229/BREAKING/61229007>; por. również: P. Waglowski, Po wyborach w USA walka o źródła oprogramowania iVotronic, 31 grudnia 2006, <http://prawo.vagla.pl/node/6922>

45. State Board of Election's Documents Detailing Diebold's Questionable Ability to Count Every Vote, <http://truevotemd.org/content/view/430/61/>

46. Malfunctions and Miscounts, Sorted by Vendor, <http://www.votersunite.org/info/messupsbyvendor.asp>

Z aferami podsłuchowymi w tle

Na zakończenie tej części należy też zwrócić uwagę na głośne skandale związane z poufnością komunikacji elektronicznej, które nie ominęły nawet takich rządów, jak rząd Grecji, kolebki demokracji. Dzięki interfejsom podsłuchowym umieszczonym w centralach telefonicznych Ericssona nieznanymi sprawcy podsłuchiwali rozmowy prowadzone przez telefony komórkowe greckiego premiera Kostas Karamanlisa, wielu członków jego gabinetu, polityków opozycji i licznych przedsiębiorców. Podsłuchiowano rozmowy szefa greckiego MSZ Petrosa Moliwiatisa, a na liście kontrolowanych numerów znalazł się również jeden należący do ambasady USA w Atenach. Podsłuchiowano ponad 100 osób przez rok. Sprawców nie wykryto. Przywołany przykład wskazuje na to, że w elektronicznym świecie niezwykle trudno uzyskać naprawdę poufny kanał zdalnej komunikacji elektronicznej⁴⁷.

6. Lobbying producentów maszyn do głosowania w Polsce

Rynek komputerów wyborczych jest obecnie rynkiem takim jak każdy inny i silna konkurencja wymusza na producentach intensywną walkę o rynki zbytu. Jednak interes tych firm nie stanowi uzasadnienia dla ingerowania w tak ważną instytucję demokratycznego państwa jaką są powszechne wybory. Dotyczy to zwłaszcza organów stanowiących w Polsce prawo, które są i będą poddawane nasilonemu lobbyingowi mającemu na celu pokazanie faktycznych lub rzekomych zalet głosowania elektronicznego, przy pominięciu jego wad.

Prareferendum europejskiego w Głucholazach

W 2003 roku podczas prareferendum europejskiego w Głucholazach firmy SAS Institute, Diebold Polska, Ośrodek Badań Wyborczych, Polska Grupa Badawcza oraz poseł PO Tadeusz Jarmuziewicz zaprezentowali maszynę do głosowania Diebold AccuVote-TS. Marcin Palada z OBW: „Polska ordynacja wyborcza jest przestarzała i nie dopuszcza głosowania elektronicznego. Nasz system wyborczy wymaga gruntownej przebudowy - jest to jeszcze dziedzictwo poprzedniej epoki. Nie chodzi tylko o nowinki technologiczne, system jest niewydolny w sensie sprawności maszyny. Duże nadzieje wiąże ze zмирzającą do władzy koalicją. Być może uda się wprowadzić elektroniczne wybory już za cztery lata”⁴⁸.

Propozycja integracji w ramach e-PUAP

W 2004 roku konsorcjum firm McKinsey i Inforvide zaproponowało wprowadzenie głosowania przez portal internetowy (PUB.O.17) w ramach projektu e-PUAP. Według wyliczeń McKinsey administracja miałaby zaoszczędzić 5,9 mln zł, a wyborcy – 23,9 mln zł, jednak wyliczenie to wydaje się nierzetelne ponieważ całkowicie pominięto w nim koszt budowy i utrzymania elektronicznego systemu wyborczego oraz koszt uwierzytelnienia ze strony wyborców – np. podpis kwalifikowany⁴⁹.

Pokażmy kandydatom na prezydenta maszyny w ich lokalach

W październiku 2005 w dwóch lokalach wyborczych w Warszawie i Sopocie zaprezentowano komputery wyborcze iPOS produkcji firm Wincor Nixdorf z oprogramowaniem firmy Suport. Inicjatorem eksperymentu była firma Polska Grupa Badawcza. Prawdopodobnie nie przez przypadek wybrano dwie komisje wyborcze, w których swój głos w wyborach prezydenckich mieli oddać dwaj kandydaci na ten urząd: Lech Kaczyński i Donald Tusk⁵⁰.

47. por. P. Wagłowski, Jak podsłuchiowano polityków w Grecji, 16 marca 2006, <http://prawo.vagla.pl/node/6072>; na temat podobnej afery podsłuchowej we Włoszech czytaj m.in.: P. Wagłowski, Tapnięcie podsłuchowe we Włoszech, 29 września 2006, <http://prawo.vagla.pl/node/6684>

48. A. Maciejewski, Jak to się robi w Głucholazach, 16 września 2005, <http://www.computerworld.pl/news/83131.html>

49. A. Maciejewski, Kiedy zagłosujemy przez internet?, 16 września 2005, <http://www.computerworld.pl/news/83119.html>

50. A. Maciejewski, Warszawa i Sopot głosowały elektronicznie, 24 października 2005,

Skąd głosowanie przez internetowy portal w notatce z obrad Rady Ministrów?

W notatce omawiającej obrady Rada Ministrów, które odbyły się w dniu 1 sierpnia, kiedy to Rada Ministrów przyjęła rozporządzenie w sprawie Planu Informatyzacji Państwa na rok 2006, wymieniono „głosowanie przez portal internetowy”, chociaż sam Plan Informatyzacji Państwa na rok 2006 nie wspomina o takim głosowaniu⁵¹.

Komentarz do wyborów w Brazylii

W październiku 2005 przy okazji komentowania wyborów w Brazylii swoje komputery wyborcze zaprezentował Unisys Polska⁵².

Prezentacje konferencyjne

W lutym 2006 na konferencji Computerworld „Państwo w mikro i makroskali” zaprezentowano holenderskie maszyny do głosowania NEDAP⁵³.

Potestujmy w Częstochowie

W kwietniu 2006 roku Częstochowski Urząd Miasta przeprowadził testowe głosowanie przy pomocy maszyn NEDAP⁵⁴.

7. Wnioski

Biorąc pod uwagę powyższe Stowarzyszenie Internet Society Poland uważa, że:

W interesie polskiej demokracji jest pozostanie przy dotychczasowym systemie wyborów bezpośrednich i prowadzonych w lokalach wyborczych, bez wprowadzania eksperymentów z głosowaniem „przez internet”.

Zastosowanie systemów informatycznych w procesie wyborczym powinno ograniczać się do funkcji pomocniczych, takich jak wizualizacja wyborów, co leży w interesie przejrzystości procesu wyborczego.

Zastosowanie komputerów wyborczych stanowi nieuzasadniony wydatek oraz poważne zagrożenie dla przejrzystości oraz uczciwości procesu wyborczego.

Środki inwestycyjne należy przeznaczyć przede wszystkim na usprawnienie procedur elektronicznej wizualizacji wyników, dodatkowych mechanizmów weryfikacji uczciwości tradycyjnych procedur wyborczych przy pomocy technik kryptograficznych (np. Punchscan⁵⁵) i procedur umożliwiających weryfikację oddanego głosu przez wyborcę.

Nienaruszalnymi, koniecznymi warunkami obowiązującymi przy jakichkolwiek przyszłych zmianach w procedurach wyborczych powinny być: anonimowość, tajność, niemożność sprzedaży głosu, prawidłowość wyników oraz weryfikowalność wyników przez wyborcę. Postulaty wprowadzenie

<http://www.computerworld.pl/news/84427.html>; P. Wąglowski, Elektroniczne testowanie kandydatów na Prezydenta, 24 października 2005, <http://prawo.vagla.pl/node/5659>

51. komunikat Kancelarii Prezesa Rady Ministrów z dnia 01.08.2006: http://www.kprm.gov.pl/441_18118.htm

52. A. Maciejewski, Brazylija pionierem e-votingu? 16 września 2005, <http://www.computerworld.pl/news/83134.html>

53. P. Gamczyk, Powyborczy e-horyzont, 27 stycznia 2005, <http://www.computerworld.pl/news/74883.html>

54. A. Gontarz, Częstochowa głosowała elektronicznie, 5 kwietnia 2006, <http://www.computerworld.pl/news/91529.html>

55. por. <http://punchscan.org/>

elektronicznego głosowania w powszechnych wyborach, w tym głosowania „przez internet”, nie mogą ignorować aktualnego stanu wiedzy i zagrożeń sygnalizowanych przez naukowców⁵⁶.

Znane są nam przykłady grup złożonych z osób o wysokich kwalifikacjach technicznych, które opracowały skuteczne i bezpieczne procedury głosowania internetowego we własnym gronie - najbardziej znanym przykładem jest społeczność twórców systemu Debian. Sądzymy, że z czasem doświadczenie zebrane przez takie społeczności i idące w ślad za tym rozszerzanie grona osób rozumiejących wszystkie praktyczne wymagania proceduralne związane z takim głosowaniem, doprowadzą do powstania ogólnie uznanych i sprawdzonych zasad demokracji opartej na głosowaniu „przez internet” w wyborach powszechnych. Będzie to jednak proces powolny, obejmujący równoległe edukację wyborców oraz organizatorów i administratorów procesu wyborczego.

Internet Society Poland deklaruje chęć współpracy ze wszystkimi zainteresowanymi rozwojem społeczeństwa obywatelskiego z wykorzystaniem internetu. Internet może być bardzo wygodnym narzędziem prowadzenia debaty publicznej, w tym prowadzenia konsultacji społecznych, a także być wykorzystywany do udostępniania informacji publicznej.

Chociaż jesteśmy pasjonatami internetu uważamy, że jeszcze nie nadszedł czas na wybory organizowane elektronicznie, a także „przez internet”.

Stanowisko to zostało zredagowane przez grupę członków Internet Society Poland: Marcina Cieślaka, Józefa Halbersztadta, Krzysztofa Kowalczyka, Pawła Krawczyka, Jarosława Lipszyca, Władysława Majewskiego i Piotra Wąglowskiego jako podsumowanie trwającej przez kilka ostatnich miesięcy środowiskowej dyskusji.

Kontakt dla mediów:

Marcin Cieślak, Prezes Zarządu ISOC Polska

saper@isoc.org.pl

Paweł Krawczyk, Członek Zarządu ISOC Polska

kravietz@post.pl

<http://www.isoc.org.pl>

56. por. International Association for Voting Systems Sciences - IAVOSS, <http://www.iavoss.org/>; por. Również M. Kutylowski, F. Zagórski, „Szansa czy zagrożenie – wybory elektroniczne”, Computerworld, 2 stycznia 2006, <http://www.computerworld.pl/artykuly/50392.html>