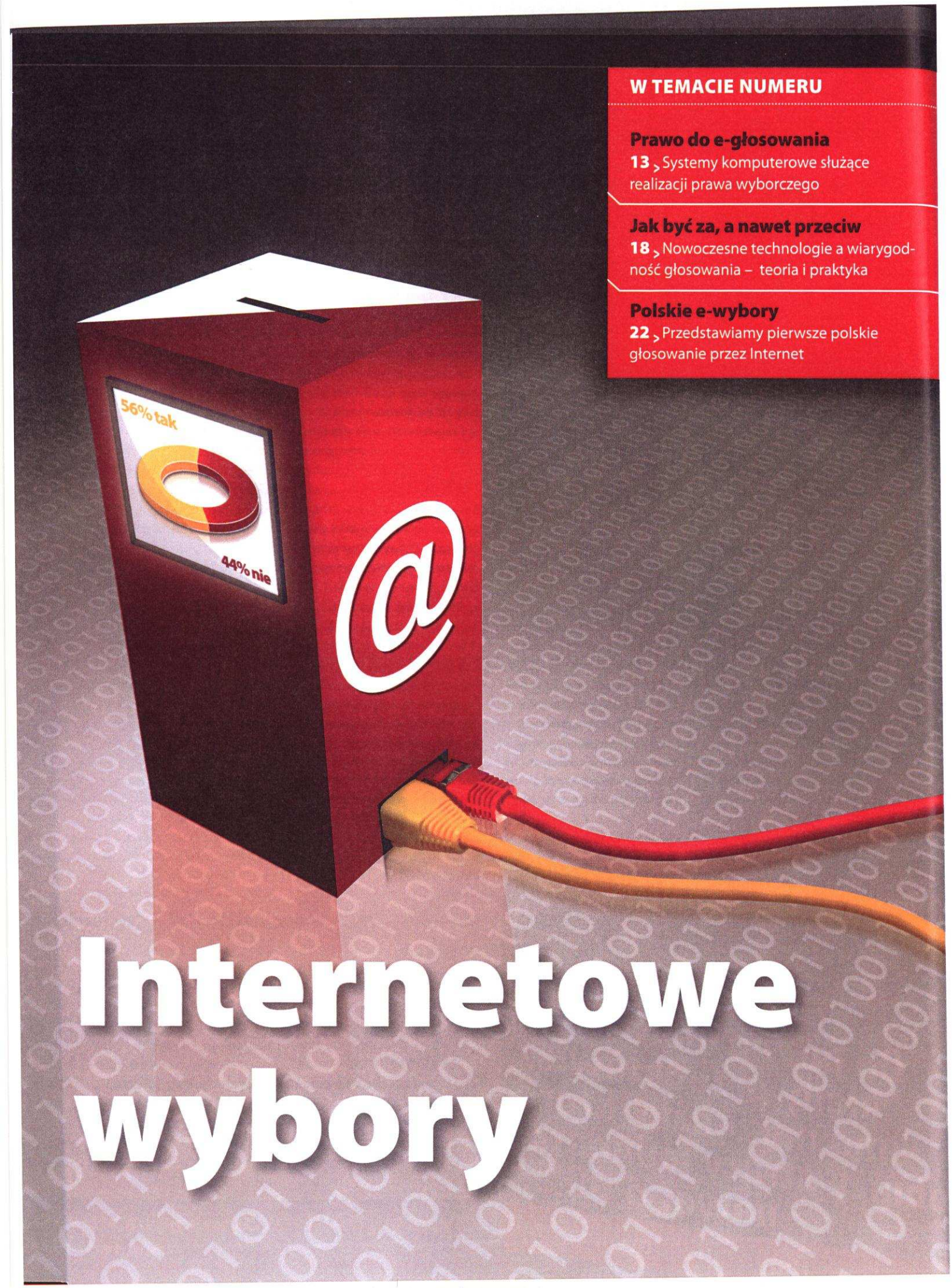


Internetowe wybory

W TEMACIE NUMERU

Jak być za, a nawet przeciw

BEZPIECZEŃSTWO | Nawet w najbardziej wolnych i demokratycznych wyborach zdarzają się historie podważające wiarygodność głosowania. Czy zastosowanie nowoczesnych technologii informatycznych pozwoli je wyeliminować?

Borys Sobiegraj, Kamil Kulesza

Cechą współczesnej cywilizacji jest stale rosnąca liczba innowacji służących społeczeństwu. Wśród osiągnięć, z których w ciągu ostatnich kilkudziesięciu lat czerpaliśmy wyjątkowo intensywnie, są komputery i Internet. Ale oznacza to też konfrontację starych idei z wyzwaniami i możliwościami, które dają nowe technologie. Skojarzenie starogreckiej idei demokracji z powszechną dostępnością technologii informatycznych praktycznie samoistnie zrodziło pomysł e-votingu, czyli elektronicznego głosowania. Słownikowa definicja tego pojęcia: „forma głosowania, w której wykorzystywane są środki komunikacji elektronicznej", kojarzona jest często – niestety niewłaściwie i w dużym uproszczeniu – z wykorzystaniem komputerów do zbierania i liczenia oddanych głosów. Koncepcja wydaje się nowa, jednak po bliższym przyjrzeniu okazuje się, że historii ludzkiej cywilizacji znane są różne próby wdrażania systemów głosowania przy użyciu maszyn. Choć, oczywiście, są i tacy, którzy twierdzą, że historyczne przykłady nijak nie odnoszą się do obecnej sytuacji, ze względu na fundamentalną zmianę, która zaszła wraz z pojawieniem się współczesnych technik informatycznych. Na podstawie badań, które przeprowadziliśmy w Polskiej Akademii Nauk, wykażemy, że jest to rozumowanie błędne, choć w pierwszej chwili teza ta – paradoksalnie – wydaje się prawdziwa.

(Nie)jawnie oddam głos

Oszustwa wyborcze są tak stare jak samo głosowanie. Nieodłączny każdej grupie społecznej konflikt interesów już od greckich czasów skłaniał do takiego przeprowadzenia wyborów, aby zwyciężyła „właściwa" strona.

Jednym z najstarszych modeli wyborów było głosowanie jawne, znane już w starożytności. Trzeba jednak pamiętać, że metoda ta pozwalała na wykorzystanie bogatego arsenału środków perswazji – począwszy od zastraszania przemocą fizyczną lub degradacją ekonomiczną, przez przekupstwo, kończąc na słownej manipulacji.

Konkurencyjny model – głosowanie niejawne – bardzo długo nie mógł się zakorzenić w demokratycznych ustrojach. Mimo że było wykorzystywane w Grecji i we Francji pod koniec XVIII wieku, formalnie zostało uznane dopiero w 1856 roku w czasie wyborów na Tasmanii. Z brytyjskiej kolonii nowinka trafiła do krajów zachodniej Europy. Głosowanie niejawne pozwalało wyeliminować pewne problemy, z drugiej jednak strony – generowało kłopoty na innym polu.

Jedną z metod głosowania maszynowego, która nie ustrzegła się nacisków ekonomicznych, było głosowanie przez naciśnięcie przycisku. Jeden z przycisków smarowano pastą do butów, dzięki czemu osoba podająca rękę wyborcom wychodzącym z lokalu otrzymywała informację, jak głosowali. Głosowania niejawnego dotyczyła też manipulacja przez dorzucanie głosów, anulowanie głosów „za oponentem" (np. przez dostawianie krzyżyka na arkuszu, w przypadku gdy dozwolony był wybór jednego kandydata), manipulacja komisjami wyborczymi i kombinacje tych metod. Bardziej finezyjnym sposobem było przesuwanie granic okręgów mandatowych. Spośród metod legislacyjnych warto wspomnieć o stosowanym w wielu krajach po dziś dzień ograniczaniu praw wyborczych wybranym grupom społecznym.

Głosowanie niemal doskonałe

Przykładem systemu głosowania niejawnego, który na przestrzeni wieków ciągle się poprawiał, jest wybór papieża podczas konklawe. Obecnie jest on sformalizowany w każdym szczególe, według wskazówek opisanych w konstytucji apostolskiej „Universi dominici gregis", pochodzącej z 1996 roku. Doskonałą nieformalną analizę konklawe z punktu widzenia bezpieczeństwa przeprowadził Bruce Scheier w artykule „Hacking the Papal Election".

Konklawe, choć tajne, odbywa się na oczach wszystkich obecnych. Jest to mała

Letnie praktyki badawcze

Opisywane badania przeprowadzone zostały w ramach letnich praktyk badawczych (**www.praktyki.ibspan.waw.pl**) Polskiej Akademii Nauk. Projekty, w których uczestniczą studenci, odbywają się na wzór brytyjskich study groups. Tematyka badań dotyczy głównie bieżących problemów przemysłowych i biznesowych, których rozwiązaniem może być podejście badawczo-naukowe. Obecnie praktyki są organizowane wspólnie przez Instytut Badań Systemowych PAN, Instytut Matematyczny PAN i Wyższą Szkołę Informatyki Stosowanej i Zarządzenia pod auspicjami PAN.

grupa dobrze znających się osób, umieszczona w odizolowanym od świata miejscu, co uniemożliwia infiltrację. Osoba licząca głosy ma teoretycznie możliwość dokonania manipulacji, ale ponieważ jest obserwowana przez innych, zdecydowanie utrudnia to oszustwo. Dodatkowo istotny staje się aspekt psychologiczny przysięgi składanej podczas oddawania głosu, która w etycznym środowisku, jakie z założenia stanowią uczestnicy konklawe, powinna odegrać ważną rolę. Niestety, systemu tego nie można wykorzystać w wyborach na szeroką skalę.

Jak jest gdzie indziej

Innowacje w głosowaniu wprowadziło już wiele społeczeństw na całym świecie. Przypadki te przeanalizowaliśmy podczas letnich praktyk badawczych (patrz: **ramka „Letnie praktyki badawcze"**) – przykładowe wyniki tych badań, w wersji skróconej, przedstawiamy poniżej.

W Stanach Zjednoczonych w Lockport, w stanie Nowy Jork, już w 1892 roku zastosowano tzw. dźwigniową maszynę. Jej popularność rosła nieustannie aż do 1930 roku, gdy do gry weszły urządzenia na karty perforowane. Mimo pewnych wad były one używane aż do przełomu wieków. Jednak gdy w wyborach prezydenckich w 2000 roku dziurki „w ciąży" (nie do końca wycięte otwory, uniemożliwiające automatyczne odczytanie karty) wykluczyły głosy 2 mln wyborców, zdecydowano o zmianie systemu. Dwa lata później Kongres uchwalił ustawę Help America Voting Act, która miała doprowadzić do wprowadzenia nowoczesnych technologii głosowania i poprawić stronę organizacyjną. W rezultacie wiele firm zaczęło przygotowywać systemy głosowania elektronicznego, twierdząc, że są one w pełni bezpieczne. Jednak praktycznie wszystkie raporty eksperckie oceniały negatywnie stosowane systemy e-votingu, wskazywały dużą liczbę luk w ich ochronie, co doprowadziło ostatecznie do wycofania ich certyfikatów bezpieczeństwa. Niestety dla Johna Kerry'ego – to właśnie te systemy zdecydowały o zwycięstwie George'a Busha w wyścigu do urzędu prezydenta w 2004 roku. Najgłośniej dyskutowano wtedy o następujących nieprawidłowościach:

- blisko połowa z 6 mln Amerykanów przebywających poza granicami kraju nie otrzymała kart do głosowania lub dostała je po czasie (winę za to ponosi m.in. Pentagon, który z nieznanych przyczyn zamknął stronę służącą rejestracji chętnych do otrzymania karty);
- w Nowym Meksyku o zwycięstwie decydowało 5988 głosów, a jednocześnie maszyny nie policzyły aż 20 000 oddanych głosów;
- maszyny uszkodziły ok. 1 mln kart z głosami (co stanowiło około 1% wszystkich użytych);
- w Ohio błędy w wypełnianiu formularzy wykluczyły co czwartego wyborcę; wśród osób, którym uniemożliwiono w ten sposób głosownie dominowali emigranci, osoby słabo wykształcone i ludzie starsi, czyli naturalny elektorat demokratów.

Słabe punkty głosowania za pomocą maszyn

- oprogramowanie
- sposób dostarczania i testowania urządzeń liczących
- dostęp poszczególnych osób do votomatów (maszyn głosujących) przed i po głosowaniu
- pochodzenie papieru i tuszy do drukarek
- zabezpieczenie samego skanera
- zabezpieczenie dokładnego przebiegu procedur po głosowaniu

Wszystkie te nieprzewidziane okoliczności zdecydowanie faworyzowały George'a Busha.

Pierwsze próby elektronicznego głosowania **w Wielkiej Brytanii** przeprowadzono w 2003 roku. Wybory na Wyspach zwyczajowo zaczynają się od wpisania się na listę wyborców – technologia pozwoliła więc na rejestrację przez Internet. Niestety, luką w systemie, której nie udało się wyeliminować, okazał się sposób poświadczenia adresu zamieszkania osoby głosującej, czyli rachunki (np. za prąd, telefon). Dokumenty te pozwalały na kilkakrotne głosowanie osobom posiadającym więcej niż jeden dom. Z drugiej jednak strony system cechował się dużą elastycznością – umożliwiał oddanie głosów na wiele sposobów, m.in. przez telefony komórkowe, to jednak mogło oznaczać perspektywę kłopotów z przepustowością sieci komórkowych w dniu wyborów. Inną wadą systemu była rozbieżność między liczbą głosów zarejestrowanych przez votomat a tą, którą wskazały osoby liczące. W istocie okazało się, że ilość zasobów ludzkich, potrzebnych do przeprowadzenia wyborów, w zasadzie nie zmalała. Zdarzało się, że głosy w lokalu wyborczym wydrukowano tuszem, którego później nie rozpoznawały skanery. Sam system okazał się więc kapryśny i wymagał w niektórych okręgach powrotu do starych metod głosowania.

W Holandii ramy prawne głosowania elektronicznego dało przegłosowanie w 1997 roku ustawy Regulation for approval of voting machines. W kwietniu 2006 roku odbyło się pierwsze lokalne głosowanie w nowym systemie. >>

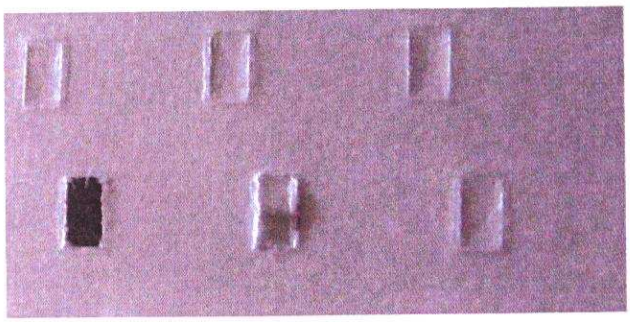
Dziś głosy wyborcze mieszkańców Stanów Zjednoczonych **liczone są za pomocą takich „votomatów"**.

FOT. PREMIER ELECTION SOLUTIONS

>> Doświadczenia z tych wyborów stały się inspiracją do działań dla grupy hakerskiej Wij vertrouwen stemcomputers niet (WVSN). Jeden z jej członków, Rop Gonggrijp, opowiadał później, że za dużo wiedział na temat komputerów, by zaufać czarnej skrzynce z Windows i dostępem do sieci bezprzewodowej, która nie daje możliwości weryfikacji oddanego głosu, aby móc dopuścić do dalszego używania tego systemu. Twierdzenia producenta, że przecież chodzi o maszyny głosujące, a nie komputery, a więc nie ma zagrożenia manipulacją, nie uspokoiło hakerów. Obojętność administracji na kampanię informacyjną WVSN w kwestii bezpieczeństwa sprowokowała grupę do dalszych działań. Po zdobyciu jednego z automatów do głosowania zabrali się do trwających miesiąc testów. Powstał raport z dokładnym opisem możliwości manipulowania wynikami głosowania. Jakie zastrzeżenia mieli hakerzy do nowego systemu? Stwierdzili brak odpowiedniego zabezpieczenia urządzeń przed otworzeniem przez osoby trzecie, prostotę manipulacji komponentami votomatów, możliwość łatwej zmiany oprogramowania po dostaniu się do środka. Poza tym urządzenia liczące emitowały łatwo wykrywalne nieekranowane fale radiowe, które pozwalały sprawdzić, na kogo jest oddawany głos, z odległości do 25 m. W rezultacie upublicznienia wyników badań i protestów opinii publicznej rok temu wycofano się w Holandii z przeprowadzania e-wyborów.

Elektroniczny system głosowania **w Rosji** nosi nazwę GAS Wybory i wykorzystuje techniczne zespoły automatyzacji (TAS), ustanowione w prawie wszystkich administracyjnych jednostkach podziału terytorialnego. TAS-y oparte są na lokalnej sieci komputerowej i mają do dyspozycji 2100 automatów. Do systemu została dołączona baza z danymi 112 mln obywateli.

Mimo dużego poparcia administracji dla nowego systemu kilka kwestii budzi wątpliwości. Najważniejsze z nich dotyczą wpływu systemów informatycznych na uczciwość wyborów oraz roli agencji rządowej FAPSI odpowiadającej od strony technicznej za przesłanie danych między TAS a Federalnym Centrum Informacji. FAPSI jest spadkobiercą zlikwidowanego KGB i od 1995 roku wszystkie systemy kryptograficzne używane w Federacji Rosyjskiej muszą być licencjonowane przez tę agencję. Wszyscy dostawcy Internetu w Rosji muszą zainstalować System Operatywnej Czynności Dochodzeniowej, umożliwiający zdalne sterowanie i filtrowanie ruchu sieciowego z centrali FAPSI. Krążą pogłoski, że wszystkie systemy licencjonowane przez FAPSI mają „tylne drzwi", umożliwiające agencji swobodny dostęp do zaszyfrowanych informacji.



Karty perforowane używano w Stanach Zjednoczonych do przełomu wieków. O zmianie sytemu zdecydowano, **gdy dziurki „w ciąży"** (nie do końca wycięte otwory) uniemożliwiły odczytanie kart dwóch mln wyborców.

Jednak zastrzeżenia można mieć nie tylko do systemu elektronicznego. Pojawiło się wiele nieprawidłowości związanych z tzw. czynnikiem ludzkim: sterty kart do głosowania wypełniono przed rozpoczęciem wyborów, urny opieczętowano już z samego rana, zanotowano próby przekupstwa i pozbycia się obserwatorów, a także nieznane dotąd metody liczenia głosów. Po kraju jeździły autobusy ze studentami mającymi zaświadczenia o prawie do głosowania poza miejscem zamieszkania, a do niektórych szpitali nie przyjmowano rodzących kobiet bez dokumentu o prawie głosu. Jak widać, trudno było nie wziąć udziału w wybieraniu władz, a jeśli już do tego doszło, nieobecność tylko ułatwiała komisji samodzielne wypełnienie karty wyborczej.

Estoński system zadebiutował w 2005 roku w wyborach władz lokalnych. Mimo iż przez Internet głosowało niecałe 2% uprawnionych obywateli, e-wybory zaprezentowano jako sukces. Od strony formalnej, by wziąć w nich udział, trzeba było jedynie wyposażyć się w kartę (będącą jednocześnie dowodem osobistym) wraz z czytnikiem i zalogować na stronie WWW. Głosowanie elektroniczne odbyło się kilka dni przed wyborami w lokalach. Jeśli obywatel głosował zarówno w jeden, jak i drugi sposób, ważny był głos pochodzący z lokalu wyborczego.

Dzięki wyborom parlamentarnym z 2007 roku Estonia stała się pierwszym krajem w świecie, któremu udało się wdrożyć głosowanie on-line na skalę narodową.

Było to możliwe dzięki spełnieniu kilku warunków, wśród których ważne były:

- odpowiednie zaplecze technologiczne – znakomita większość obywateli Estonii ma dowody osobiste z chipem. Znaczenie ma również fakt, że w kraju tym dynamicznie rozwija się e-administracja.
- polityczna wola rządu, który mimo przeszkód przeforsował zmiany prawne.
- atmosfera wzajemnego zaufania, która panowała pomiędzy politykami, mediami i wyborcami.

Warto jednak zwrócić uwagę, że system e-votingu był stosowany na stosunkowo niewielką skalę w małym kraju. Ponadto, opisane tu przykładowe warunki nie są łatwe do spełnienia w każdym przypadku. Analogicznie jak podczas konklawe – w „kontrolowanych warunkach laboratoryjnych" wszystko zdaje się przebiegać prawidłowo, w rzeczywistości – niekoniecznie.

Nieco teorii

Skoro wybory elektroniczne wiążą się z taką liczbą problemów praktycznych, warto zgłębić teoretyczne podstawy e-głosowania. W tym kontekście przybliżymy protokół dr. Davida Chauma oraz przykład z krajowego podwórka – protokół prof. Mirosława Kutyłowskiego.

Dr Chaum jest autorem nie tylko wielu artykułów z dziedziny kryptografii, ale i 17 patentów. Stworzył ślepy podpis (bezwarunkowo bezpieczny podpis protokołów przeprowadzania anonimowych transakcji cyfrowych), przyczynił się do powstania podwalin elektronicznych pieniędzy. Zorganizował grupę badań nad kryptografią w Centrum Matematyki i Informatyki w Amsterdamie, był również współzałożycielem

FOT. WWW.LS.UNIOVA.EDU/~JONES/CARDS/

International Association for Cryptologic Research (IACR).

Protokół Chauma jest próbą pogodzenia sprzeczności e-votingu, czyli zachowania tajności głosowania przy jednoczesnej możliwość sprawdzenia, czy głos został poprawnie policzony. Sprawdzenie, na kogo oddano głos, możliwe jest tylko „przy maszynie" w lokalu wyborczym, natomiast zliczenie głosów można przeprowadzić przez Internet. „Głos" składa się z dwóch rozdzielnych warstw, które nałożone na siebie odtwarzają go graficznie (jednej połówki pozbywamy się w lokalu, druga służy do weryfikacji przez Internet). W kryptografii taką technikę określa się mianem dzielenia sekretu za pomocą metod wizualnych. Dostęp do informacji o głosie ma grupa osób nieznających swoich tożsamości. Każda z nich dysponuje „kawałkiem układanki" w postaci algorytmu dekodującego. Wieloetapowe rozkodowywanie z pomocą tak podzielonego procesu dekodowania pozwala zachować anonimowość głosującym i utrudnia manipulację pulą głosów. Protokół Chauma jest jedną z najlepszych obecnie propozycji teoretycznych, natomiast stosunkowo niewiele wiadomo o jego praktycznym zastosowaniu, zwłaszcza na szerszą skalę.

Profesor Mirosław Kutyłowski pracuje Instytucie Matematyki i Informatyki Politechniki Wrocławskiej. W jego dorobku naukowym znajdują się prace o bezpieczeństwie komputerowym, kryptografii, e-votingu, prawnych problemach systemów teleinformatycznych, teorii algorytmów i złożoności obliczeniowej.

Protokół polskiego naukowca przewiduje wykorzystanie urządzeń powszechnie dostępnych (takich jak komputer, drukarka, skaner lub czytnik kodów kreskowych), co obniża koszt operacji. Dla bezpieczeństwa votomaty nie są podłączone do sieci, a kodami dostępu do puli głosów dysponuje grupa osób. Głosy oznaczone są sygnaturą urządzenia, w którym zostały wygenerowane. Głosowanie odbywa się kilkuetapowo. Najpierw generowana jest karta do głosowania, a na graficznej jej reprezentacji dokonuje się wyboru. Informacja o wyborze w pamięci komputera jest dwuczęściowa i jako taka „żyje" w systemie do czasu rozkodowania, co ogranicza możliwość manipulacji. Po głosowaniu otrzymuje się wydruk kontrolny. Oddany i wydrukowany głos składany jest w maszynie zliczającej, skąd po głosowaniu jest przesyłany ustalonym łańcuchem serwerów w sieci. Podczas tej drogi następuje ponowne scalanie głosu i rozkodowywanie, a ostatnia komisja otrzymuje i publikuje odszyfrowaną wersję. O wykorzystaniu protokołu w e-wyborach przeprowadzonych 8–10 czerwca przez naukowców Politechniki Wrocławskiej piszemy więcej na str. 22.

Niebezpieczne związki

Po przeanalizowaniu obu protokołów stwierdziliśmy, że cechą wspólną jest duży nacisk na ich kryptograficzną stronę, co jest zrozumiałe, gdyż były one projektowane przez kryptografów. Jednak obszar ten jest przecież tylko jedną ze składowych e-votingu. Pozostałe, niemniej ważne elementy systemów elektronicznego głosowania, na które w naszych badaniach zwróciliśmy uwagę, przedstawiamy **w ramce „Słabe punkty głosowania za pomocą maszyn"**.

Analiza doświadczeń e-głosowania zebranych przez inne kraje, a także podstaw teoretycznych wskazuje, że na ten system można spojrzeć podobnie jak na starsze metody głosowania. Jednym z paradoksów jest to, że współczesne techniki informacyjne nie usprawniły samego procesu, raczej go skomplikowały i „zaciemniły". Jak widać, sposoby nadużywania i oszukiwania systemu głosowania są te same od stuleci, a zmienia się tylko sposób jego wdrażania, ściśle związany z technologią dostępną w danym czasie. Tylko maksymalnie przejrzyste procedury są w stanie zapewnić w miarę pewne i skuteczne działanie systemu.

Praktyka elektronicznego głosowania wybranych państw pokazuje, jak niebezpieczne mogą być próby wprowadzenia nowego systemu, pozbawionego odpowiedniego przygotowania i dopuszczenia do użycia maszyn do głosowania bez odpowiednich zabezpieczeń. Te ostatnie mogą okazać się luką często większą od uchybień w samym protokole głosowania. Tymczasem błędy te nie są wcale rzadkością, nawet przy zachowaniu odpowiedniej staranności przez projektanta systemu.

Warto zdać sobie sprawę, że nadużycia przy wyborach związane z wykorzystaniem luk w votomatach mają raczej znaczenie drugorzędne. O wiele „skuteczniejsze" są bowiem bardziej typowe metody – zastraszanie czy przekupywanie głosujących, przymuszanie ludzi do głosowania, aresztowania liderów opozycji, zastraszanie wyborców i inne tego rodzaju środki, kojarzone zazwyczaj z krajami Trzeciego Świata. To metody nadzwyczaj efektywne i rzadko kiedy powodujące protesty, w przeciwieństwie do fałszerstw wyborów na masową skalę, takich jakie miało miejsce np. w Kenii. Trzeba też dodać, że tego rodzaju oszustwa nie są tylko kłopotem krajów rozwijających się. Wręcz przeciwnie – przekupstwu wyborców sprzyja bogactwo i demokracja państw, w których wyborcy decydują o redystrybucji dochodu narodowego. Kwestią, którą powinni raczej zająć się etycy i politolodzy, jest to, czy można mówić w tym przypadku o fałszerstwie wyborów, czy raczej tylko o wypełnianiu zobowiązań wyborczych. Ostatecznie, przykład Florydy, której opinia publiczna dowiedziała się o mataczeniu przy urządzeniach wspierających głosowanie w wyborach prezydenckich w 2000 roku, pokazał, że skala takiego ataku wcale nie musi być większa niż skutki bardziej „standardowych" metod manipulacji wynikami (np. nieprawidłowości przy tworzeniu list wyborczych).

Romans demokracji z nowoczesnymi technologiami nie miał najlepszego początku. Jeszcze nie wiadomo, czy podobnie jak głosowanie niejawne wyprzedziło jawne, e-voting również stanie się kolejnym ogniwem ewolucji. Problemy, które wiążą się z tym systemem, nie wróżą mu świetlanej przyszłości. Niemniej, rozpalająca wyobraźnię perspektywa powodzenia staje się paliwem potrzebnym rządom, prywatnym firmom i licznym zespołom naukowców do rozwiązania tego problemu.

Borys Sobiegraj jest studentem ostatniego roku Wydziału Fizyki Uniwersytetu Warszawskiego. Był uczestnikiem letnich praktyk badawczych 2008, podczas których pracował m.in. przy projekcie dotyczącym głosowania z wykorzystaniem maszyn.

Kamil Kulesza jest adiunktem w Instytucie Badań Systemowych PAN, związany jest również z University of Cambridge. W swojej pracy badawczej zajmuje się zagadnieniami związanymi z informatyką i zastosowaniami matematyki, ze szczególnym uwzględnieniem bezpieczeństwa informacji. Jest też zaangażowany w letnie praktyki badawcze PAN od momentu ich powstania.