Portál pre odborné publikovanie ISSN 1338-0087

Využitie informačných a komunikačných technológií pri hlasovaní vo voľbách

Ralbovský Andrej · Humanitné vedy, Študentské práce

01.03.2013

Práca sa zaoberá možnosťami využitia IKT pri skvalitňovaní demokratického politického systému zavedením alternatívnych spôsobov hlasovania vo voľbách. Voľby ako prostriedok pokojnej zmeny moci sú už po stáročia vykonávané spôsobom, ktorý obsahuje množstvo nedostatkov. Technický pokrok však prináša nové metódy hlasovania, ktoré môžu vyriešiť mnohé zo súčasných problémov demokracie a ktoré otvárajú doteraz nevídané možnosti participácie občanov na politickej moci a posilňovania občianskej spoločnosti.

Aj na Slovensku pozorujeme snahy o zavedenie hlasovania vo voľbách prostredníctvom internetu. V tejto práci opisujeme aktuálny stav využitia informačných a komunikačných technológií, obzvlášť internetu pri hlasovaní vo voľbách v rôznych krajinách sveta, analyzujeme výhody a riziká, ktoré z toho vyplývajú a navrhujeme opatrenia, prostredníctvom ktorých by bolo možné čo najviac skvalitniť demokraciu na Slovensku.

1. Úvod

Voľby sú základným prvkom každého demokratického politického systému. Podľa Klokočku medzi ich hlavné úlohy patrí predovšetkým [1]:

1. Legitimácia politickej moci (a vládnucej strany alebo vládnucich strán) na základe reprezentácie názorov a záujmov voličov a prenesením ich dôvery na politické strany a osoby.
2. Výber politickej elity cestou formácie politickej reprezentácie, vychádzajúci z diferenciácie politických smerov, avšak určené ústavou ku hľadaniu konsenzu na základe možnej integrácie, resp. harmonizácie záujmov.
3. Pokojné riešenie politických konfliktov v spoločnosti, ktorá pomocou procesných pravidiel a prostredníctvom „sčítania vôlí“ umožňuje previesť konkurenčný boj o politickú moc na zápas v rámci určitých pravidiel „politickej hry“.
4. Kontroly, overovanie politickej moci, ktorý (tiež svojou pravidelnosťou) aktualizuje možnosť uskutočniť mocenské zmeny v štáte (vláda na čas).
5. Aktivizácia voličov v prospech určitých hodnôt, cieľov a programov a tým ako nástroj posilňovania občianskeho vedomia a participácie občanov na politickom živote. [2]

Kým tieto úlohy sa v čase nemenia, počas storočí trvania demokracie v rôznych

krajinách sa výrazne zmenil spôsob, akým občania odovzdávajú svoje hlasy. V starom Grécku sa na to používali kamene a črepiny, ktoré sa vhadzovali do rôznych nádob, neskôr ich vystriedali papiere, obálky a zapečatené urny.

V dôsledku technického pokroku došlo k výraznému posunu v kvalite života ľudí. Nástup informačných a komunikačných technológií (IKT) začal meniť mnohé oblasti ľudskej spoločnosti. V súčasnej dobe sa čoraz viac začínajú presadzovať spôsoby hlasovania, ktoré tento pokrok reflektujú a pri ktorých sa využívajú práve informačné a komunikačné technológie. V ďalších kapitolách pojednávame jednak o aktuálnom stave využívania IKT pri hlasovaní vo voľbách v rôznych krajinách sveta, ako USA, Estónsko či Nórsko, analyzujeme výhody aj nevýhody takéhoto prístupu a tiež navrhujeme možné riešenie pre podmienky Slovenskej republiky.

2. Analýza súčasného stavu

Vždy existovali snahy, aby bolo hlasovanie vykonávané takým spôsobom, ktorý by bol jednak dostatočne pohodlný pre voliča, ale tiež by umožňoval jednoduché sčítavanie hlasov volebnou komisiou a nedovoľoval konanie volebných podvodov. Zlomovým bol rok 1858, keď sa v USA začali používať predtlačené volebné lístky [4]. Neskôr, koncom 19. storočia sa začali využívať mechanické volebné stroje, pri ktorých volič odovzdal svoj hlas stlačením páky. Príklad takéhoto volebného stroja je na obrázku Obr. 1.

Obr. 1 Mechanický volebný stroj požívaný v USA v 19. storočí [3]

V 20. storočí ich postupne nahradili dierne štítky a nakoniec plne elektronické zariadenia. Ich predpokladaný prínos spočíval iba v zjednodušení sčítavania hlasov a odstránení nutnosti manipulácie s volebnými obálkami a hlasovacími lístkami. Náklady sú však enormne vysoké v porovnaní s klasickým spôsobom volieb[1] a ešte ich zvyšuje nutnosť drahých certifikačných procedúr. Istá výhoda sa ukazuje v znížení administratívy pri práci s voličskými zoznamami, nakoľko táto môže byť vykonávaná plne elektronicky. Tieto zariadenia boli rôzneho druhu, niektoré iba opticky rozpoznávali papierové hlasovacie lístky, teda len nahrádzali ručné sčítavanie hlasov. Pre voliča sa spôsob odovzdania hlasu nemenil.

Druhý typ týchto zariadení vyžadoval, aby volič realizoval hlasovanie priamo

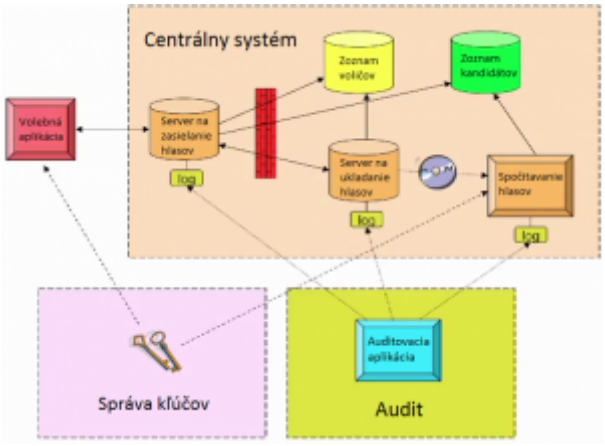
prostredníctvom neho, najčastejšie stlačením tlačidiel alebo prostredníctvom dotykovej obrazovky. Bol však veľký problém so zaistením dôvery voličov, pretože takýto spôsob hlasovania kombinuje nevýhody internetových volebných systémov (problém s efektívnou kontrolou, možnosť zlyhania techniky) a klasického hlasovania (nutnosť vydržiavať volebnú komisiu), pričom okrem rýchlosti a presnosti sčítania hlasov neprináša v podstate nijaké výhody.

Všetky tieto technológie boli charakteristické tým, že volič sa musel osobne dostaviť do volebnej miestnosti. Koncom 20. storočia sa s rozvojom internetu ako celosvetovej verejnej počítačovej siete začali objavovať snahy o umožnenie odovzdávania hlasov bez nutnosti návštevy volebnej miestnosti. Hlasovanie prostredníctvom internetu je v súčasnosti v rôznej miere možné vo viacerých štátoch sveta. Po prvý krát boli použité v USA, neskôr ich zaviedli aj iné štáty, okrem iného Švajčiarsko (cez internet umožňujú voliť tri kantóny (Geneva, Neuchâtel, Zürich) [5]), Kanada [6][7], či Nórsko (v roku 2011 boli internetové voľby v 10 územnosprávnych jednotkách). No asi najvýznamnejším je prípad Estónska, ktoré je známe rozsiahlym zavádzaním riešení e-demokracie do života.

2.1 Estónsko – prvý naozaj úspešný celoštátny projekt

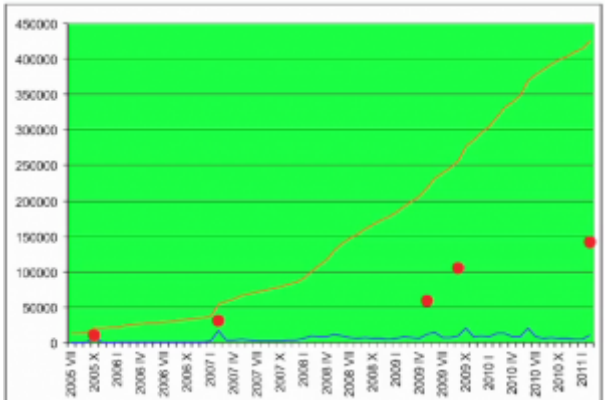
Estónsko, napriek tomu, že je to postkomunistická krajina, bývalá republika Sovietskeho zväzu, je priekopníkom v oblasti e-demokracie. Prístup na internet je v tejto krajine vyhlásený za základné ľudské právo [8] a internet tam každodenne používa 63% populácie. Takého prostredie vytvára vhodné podmienky pre využitie IKT aj v demokratickom procese. V októbri 2005 sa v Estónsku konali prvé celonárodné voľby s možnosťou internetového hlasovania, ktorých výsledky boli záväzné. Celkovo tam prostredníctvom internetu bolo možné voliť v piatich voľbách [9]. Estónsky systém, podobne ako mnohé iné, je založený na asymetrickej kryptografii. Jeho základná schéma je na obrázku Obr. 2.

Na začiatku je vygenerovaný kľúčový pár ústrednej volebnej komisie. Nakoľko však táto komisia je kolegiátny orgán, tak pomocou vhodnej matematickej schémy je súkromný kľúč rozdelený medzi jej členov, a to takým spôsobom, že je potrebné poskladať určitý minimálny (vopred ustanovený) počet častí držaných jednotlivými členmi na rekonštrukciu súkromného kľúča komisii. Niektoré takéto schémy sú opísané napríklad v [10] alebo [11]. V Estónsku sa občianske preukazy vo forme čipových kariet vydávajú od roku 2002 [9] a v roku 2006 ich počet dosiahol milión. Je teda prirodzené, že sa využívajú aj na autentifikáciu. Čip, ktorý v nich je, pre svoju funkčnosť vyžaduje dva PIN kódy. Prvý z nich, označovaný ako PIN1 sa používa na autentifikáciu, teda overenie totožnosti. Druhý (PIN2) slúži na digitálne podpísanie a na rozdiel od PIN1 spôsobuje právne následky.



Obr. 2 Estónsky systém [12]

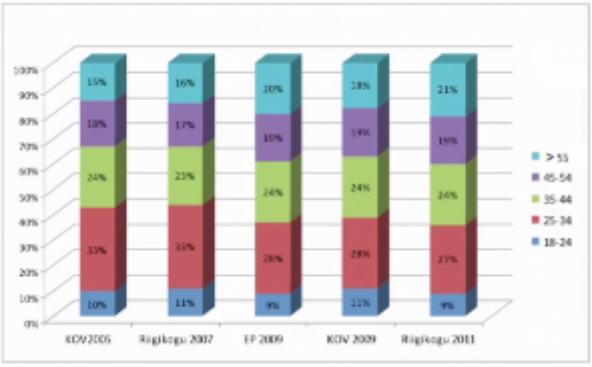
Keď užívateľ plánuje uskutočniť voľbu, musí po stiahnutí volebnej aplikácie zadať svoj osobný PIN1 kód, čím sa autentifikuje. Od systému obdrží verejný kľúč volebnej komisie a zoznam kandidujúcich strán a osôb, z ktorých si vyberie tie, za ktoré má v úmysle hlasovať. Po vybratí svojich kandidátov zadá PIN2. Týmto sa jeho elektronický hlasovací lístok digitálne podpíše. Voľbu môže viackrát zopakovať a v prípade, že zahlasuje vo volebnej miestnosti, nebude sa na jeho elektronický hlas prihliadať. Možnosť hlasovania cez internet je v súčasnosti prístupná v období sedem dní pred dňom, keď sa volí papierovo. [9]



Obr. 3 Počet elektronických hlasov v závislosti od počtu vydaných občianskych preukazov s čipom [9]

Ako vidieť z grafu na obrázku Obr. 3, spočiatku bol limitujúcim faktorom počet vydaných občianskych preukazov obsahujúcich čip (počet občianskych preukazov znázorňuje červená krivka, červené body naznačujú počty voličov pri jednotlivých druhoch volieb). V súčasnosti je však už taký veľký, že počet hlasujúcich prakticky neovplyvňuje. Na Obr. 4 je veková štruktúra voličov. Najväčšou skupinou, ktorá volí prostredníctvom internetu, sú mladí ľudia do 35 rokov. Podiel starších ako 55 rokov sa v priebehu rokov mierne zvýšil o 6 percentuálnych bodov na 21%

Zaistenie dôvery je kľúčové, preto okrem toho, že je kompletná dokumentácia spoločne s celým popisom systému zverejnená, všetky procedúry sú dokumentované na video a jednotlivé technické prostriedky zapečatené, aby sa predišlo neoprávnenej manipulácií. Do priestorov, kde sa nachádzajú technické zariadenia, majú prístup iba poverené osoby[2] [13].



Obr. 4 Veková štruktúra estónskych voličov hlasujúcich cez internet [9]

2.2 Nórsko – pokročilý systém založený na estónskych skúsenostiach

Nórsky systém sa začal pripravovať v auguste 2008, pričom sa vychádzalo najmä zo skúseností z Estónska. Je o niečo zložitejší oproti estónskemu systému a na rozdiel od neho umožňuje aj individuálnu a univerzálnu overiteľnosť [14]. Na autentifikáciu v Nórsku sa používa systém MinID [15], ktorý slúži aj na každodennú komunikáciu so štátnymi inštitúciami. Podobne ako pri internet-bankingu, používa sa v ňom prihlasovacie meno a heslo spoločne s autentifikačným kódom odoslaným v SMS správe.

Nórsky systém hlasovania sa vyznačuje tým, že v ňom nie je nutné dôverovať počítaču voliča, takže ak aj je na tomto nejaký druh škodlivého softvéru, nemalo by byť možné zmariť odovzdanie hlasu ani ho pozmeniť. Slúži na to ďalší komunikačný kanál, ktorým je SMS správa odoslaná na mobilný telefón voliča, v ktorej je uvedený kód volenej strany. Niekoľko dní vopred je voličovi odoslaná poštová zásielka, prostredníctvom ktorej obdrží volebnú kartu, kde sú uvedené jednotlivé politické strany a k nim prislúchajúce kódy. Tieto kódy sú pre každého voliča iné a po prijatí SMS správy volič porovná, či obdržaný kód zodpovedá volenej strane. Odoslané SMS správy sa pre potreby kontroly zaznamenávajú a tento záznam sa pri počítaní hlasov porovnáva s odovzdanými hlasmi. Akákoľvek nezrovnalosť v prijatom kóde by mohla indikovať pokus o manipulovanie volieb.

Obr. 5 Schéma nórskeho systému [16]

V nórskom systéme je vo veľkej miere zavedený princíp oddelenia úloh (separation of duties). Je rozdelený na niekoľko nezávislých, ale vzájomne spolupracujúcich častí pod správou rôznych inštitúcií, ktoré sú geograficky vzdialené stovky kilometrov. Niektoré časti sú fyzicky oddelené od všetkých verejných sietí, aby sa zaistilo, že v nijakom prípade nebudú napadnuté útočníkmi zvonku. Entitu RCG (Random Code Generator),

ktorá má na starosti generovanie a odosielanie kontrolných kódov cez SMS spravuje Riaditeľstvo civilnej ochrany a krízového plánovania patriace pod Ministerstvo spravodlivosti nachádzajúce sa v meste Tønsberg.

VCS (Vote Collector Service), podsystém na zber šifrovaných hlasov od voličov je spravovaný organizáciou patriacou pod Ministerstvo obchodu a priemyslu a nachádza sa v meste Brønnøysund. Fyzicky oddelené komponenty (najmä tie na generovanie šifrovacích kľúčov a počítanie hlasov) sa nachádzajú v Osle a obsluhujú ich zamestnanci Ministerstva pre miestnu samosprávu a regionálny rozvoj. Samotný súkromný kľúč volebnej komisie až do okamihu sčítavania hlasov fyzicky nikde neexistuje, pretože sa skladá z dvoch kľúčov, ktoré sú samostatne vygenerované a rozdelené medzi členov volebnej komisie [17].

Zatiaľ jediné voľby v Nórsku, ktoré boli realizované elektronicky boli voľby do orgánov územnej samosprávy v roku 2011. Celkovo aj prostredníctvom internetu mohli hlasovať občania 10 územných celkov, čo tvorilo spolu 4,5% celkového počtu obyvateľov [16].

3. Požiadavky kladené na internetové volebné systémy

Ak je hlasovanie vykonávané prostredníctvom Internetu, okrem základných princípov volebného práva musí byť kladený dôraz na to, aby vyhovovali dodatočným požiadavkám, ktoré sú pri papierových voľbách splnené implicitne:

1. „Oprávnenosť – len registrovaní voliči môžu voliť, voľba musí byť jedinečná
2. Súkromie – nie je možné vytvoriť spojenie medzi jednotlivou voľbou a voličom
3. 3. Overiteľnosť – možnosť overiť, či bol hlas zaznamenaný a započítaný do výsledku volieb je dvojaká, vzťahuje sa jednak na voliča a tiež na systém ako taký:
   - individuálna – samotný volič vie overiť, či bol jeho hlas započítaný
   - univerzálna – ktokoľvek môže overiť, či hlasy boli spočítané správne
4. Nespochybniteľnosť – schéma by mala poskytovať mechanizmy na vyriešenie nezrovnalostí v každej fáze
5. Správnosť – hlasy musia byť správne zaznamenané a započítané
6. Spravodlivosť – nikto by nemal byť schopný vypočítať čiastočné výsledky, pokiaľ prebiehajú voľby
7. Robustnosť – schéma je maximálne robustná, ak je potrebná spolupráca všetkých autorít na volebný podvod resp. chybu
8. Bezdokladovosť – volič nie je schopný poskytnúť dôkaz o svojej voľbe niekomu inému
9. Nedonútiteľnosť – nikto by nemal byť schopný prinútiť voliča k určitej voľbe“ [18][19]

4. Výhody internetových volieb

Hlasovanie prostredníctvom internetu ponúka oproti klasickému papierovému hlasovaniu niekoľko výhod. Okrem väčšieho pohodlia pre voličov a s tým súvisiacej vyššej volebnej účasti je to predovšetkým možná úspora nákladov, rýchlejšie a presnejšie výsledky a v prípade správnej implementácie aj vyššia bezpečnosť.

4.1 Volebná účasť

Jedným z hlavných prínosov hlasovania prostredníctvom internetu je možnosť voliť zo

zahraničia, resp. z ktoréhokoľvek miesta, kde je dostupné pripojenie na internet. Nie všetci občania majú možnosť dostaviť sa v deň volieb do miesta svojho trvalého bydliska. Ide najmä o vojakov v zahraničných misiách, ľudí dlhodobo žijúcich v zahraničí, ale napríklad aj o astronautov [20]. V prípade hlasovania cez internet by bolo hlasovanie pre voliča omnoho dostupnejšie. To by sa následne malo prejaviť aj na vyššej volebnej účasti.

4.2 Zlepšenie prístupnosti pre hendikepovaných

Hendikepovaní, aj keď formálne majú rovnaké právo zúčastňovať sa na výbere politickej reprezentácie, je pre nich často veľmi ťažké uplatniť si ho. Takýto osobám zvykne spoločnosť vychádzať v ústrety jednak tým, že sa im umožňuje, aby im pri volebnom akte pomohla iná osoba [21] (pričom to nemôže byť člen volebnej komisie) a tiež tým, že sa im poskytuje možnosť hlasovania mimo volebnej miestnosti, obálku v takomto prípade volič vhodí do prenosnej volebnej urny. Pri internetovom hlasovaní by však znevýhodnení občania dostali ďalšiu možnosť hlasovať a to aj bez pomoci iných osôb. Mnoho ľudí s postihnutím, najmä nevidiacich, je navyknutých pracovať s počítačom, pričom pri tejto činnosti obvykle vyžívajú špeciálne programové prostriedky. Ak by teda mali možnosť hlasovať cez internet prostredníctvom svojho počítača, značne by im to zlepšilo kvalitu života [22].

4.3 Sčítavanie hlasov

Sčítavanie hlasov je v prípade hlasovania realizovaného prostredníctvom IKT výrazne rýchlejšie a presnejšie, pretože sa eliminuje priamy kontakt volebných komisárov s hlasovacími lístkami, čo vedie k odstráneniu ľudských chýb vznikajúcich pri ručnom sčítavaní hlasovacích lístkov a písaní zápisníc. Taktiež sa znižuje počet osôb, ktoré majú možnosť výsledky ovplyvniť volebným podvodom.

4.4 Úspora nákladov

Otázka úspory nákladov je sporná. Na jednej strane kritici poukazujú na omnoho vyššie počiatočné náklady pri nasadení systému, zástancovia argumentujú výhodnosťou pri dlhodobom používaní. Priestor na úsporu by bol predovšetkým v prípade, že by sa zrušila možnosť súbežného papierového hlasovania. Pokým však internetové voľby slúžia ako doplnok k tým papierovým, celkové náklady na voľby budú vždy vyššie, pretože náklady sa papierové zostanú v rovnakej výške (stále bude treba zabezpečiť rovnaký počet obálok a hlasovacích lístkov, pre každého občana a zaplatiť rovnaký počet volebných komisárov), ale pribudnú výdavky na elektronický systém. Ak by však podstatná časť populácie začala využívať elektronické spôsoby hlasovania, mohlo by sa pristúpiť k redukcii počtu volebných okrskov a volebných komisárov.

5. Potenciálne riziká

S novými spôsobmi hlasovania sa vynárajú aj riziká, s ktorými sa pri papierových voľbách nemuselo uvažovať. Najvýznamnejšími sú menšia možnosť kontroly a jej vyššia zložitosť, riziko hackerských útokov, možnosť pomerne jednoduchého vyradenia systému z prevádzky a tým znemožnenia uskutočniť voľbu či jednoduchšie kupovanie hlasov.

5.1 Zložitejšia kontrola

Kontrola regulárnosti a férovosti volieb je podstatnou súčasťou každého volebného systému bez ohľadu na spôsob, akým sa odovzdávajú hlasy [23]. Kým pri papierových voľbách je táto kontrola viac-menej priamočiara a pomerne jednoduchá aj pre ľudí bez predchádzajúcich skúseností v tejto problematike, v prípade elektronického hlasovania sa stáva omnoho menej zjavnou a častokrát vyžaduje špeciálne znalosti, ktorými väčšina ľudí nedisponuje. To má za následok, okrem zvýšených nákladov, tiež zníženú dôveru ľudí vo volebné výsledky. Avšak na rozdiel od papierových volieb, elektronické volebné systémy umožňujú individuálnu a v niektorých prípadoch [16] aj univerzálnu overiteľnosť [24]. Dalo by sa teda povedať, že ponúkajú ešte vyššiu mieru dôveryhodnosti a možnosť lepšej kontroly, ale za cenu potreby rozsiahlych znalostí v danej problematike, čo môže u niektorých občanov vyvolať nedôveru.

5.2 Kybernetické útoky

Riziko kybernetických útokov je skutočne vážna hrozba, ktorá u papierových volieb nemá ekvivalent[3]. Tomuto riziku sú vystavené okrem centrálneho systému, u ktorého je však možné dosiahnuť pomerne vysokú úroveň zabezpečenia, aj osobné počítače voličov, z ktorých uskutočňujú svoju voľbu. Zabezpečeniu centrálneho systému sa musí venovať veľká pozornosť, pretože prípadný hackerský útok by mohol mať za následok podstatné ovplyvnenie volebných výsledkov a v krajnom prípade aj narušenie ústavného zriadenia.

Preto musí byť zaistená úplná auditovateľnosť, kde každá činnosť je zaznamenaná a neskôr je možné spätne zrekonštruovať všetky operácie, samozrejme pri súčasnom zachovaní tajnosti hlasovania. Určité skúsenosti s aktuálnymi možnosťami zabezpečenia počítačových systémov môže poskytnúť internet-banking [25]. Pri jeho zavedení sa tiež poukazovalo na veľké bezpečnostné riziká, ale za roky používania sa ukázalo, že najväčšie hrozby pochádzajú nie z útokov na banku (ktorých úspešnosť je mimoriadne nízka), ale sú to práve problémy na strane užívateľov, obzvlášť ich neskúsenosť a neschopnosť odhaliť mnohokrát veľmi sofistikované pokusy o vydanie hesla alebo uskutočnenie operácie v prospech útočníka.

5.3 Obmedzená dostupnosť

Pomerne častým argumentom odporcov je aj skutočnosť, že dostupnosť serverov v internete môže byť obmedzená použitím tzv. DDoS útokov [26], ktorých princíp spočíva v preťažení systému početnými požiadavkami, ktoré navonok vyzerajú akoby pochádzali od legitímnych používateľov, ale ich jediným účelom je, aby došlo k využitiu všetkých systémových prostriedkov a nebolo možné obsluhovať ostatných používateľov. Pokým sa ale možnosť internetových volieb chápe iba ako doplnková k papierovým a bez záruky, nie je toto riziko až také významné.

5.4 Problém so zaistením tajnosti v dlhodobom časovom horizonte

Určitým problémom, ktorý dodnes nebol uspokojivo vyriešený, môže byť aj skutočnosť, že súčasná kryptografia je založená na nemožnosti vyriešiť matematický problém pri aktuálnych technických možnostiach počítačov. Avšak postupom času sa výpočtový výkon zvyšuje a v horizonte niekoľkých desiatok rokov, v závislosti od technickej

implementácie, bude možné takto chránené údaje dešifrovať [14]. To predstavuje potenciálny problém pre súkromie voliča a môže narušiť princíp tajného hlasovania. Aj keď by sa dalo namietať, že po takom dlhom čase už tajnosť nemá význam, pri papierových voľbách toto nehrozí.

5.5 Jednoduchšie kupovanie hlasov

Kupovanie hlasov [27] je fenomén, ktorý sa vyskytuje v mnohých štátoch sveta bez ohľadu na spôsob voľby. Kritici však tvrdia, že zavedením možnosti hlasovania prostredníctvom internetu by sa kupovanie hlasov výrazne zjednodušilo [28]. Argumentujú tým, že kým vo volebnej miestnosti je volebná komisia, ktorá dohliada na priebeh volieb, čim je zaručená aspoň minimálna úroveň kontroly, v prípade hlasovania cez internet by bolo možné omnoho jednoduchšie jednak ovplyvniť voliča a tiež aj skontrolovať, či skutočne odovzdal hlas žiadanej strane. Je pravda, že v prípade, ak by bol systém volieb cez internet navrhnutý nesprávne, kupovanie hlasov by bolo výrazne jednoduchšie. Avšak vo väčšine týchto systémov sú implementované minimálne dva mechanizmy, ktorých účelom je kupovaniu hlasov zabrániť, alebo ho aspoň výrazne sťažiť do takej miery, ako je to pri klasických papierových voľbách.

Prvým z nich je možnosť opakovať voľbu prostredníctvom internetu, pričom sa počíta iba posledný odovzdaný hlas [9]. V prípade, že bol na voliča vyvíjaný nátlak, môže odovzdať nový hlas, hneď ako hrozba nátlaku pominie. Druhý spôsob ako kupovaniu hlasov zabrániť, je využitie skutočnosti, že internetové voľby sú alternatívou k papierovým. Keď sa volič rozhodne odovzdať hlas vo volebnej miestnosti, má tento jeho úkon za následok zrušenie akéhokoľvek hlasu odovzdaného elektronicky [9]. Týmto sa obtiažnosť kupovania hlasov dostáva na takú úroveň, aká by bola bez možnosti voliť cez internet. Problém kupovania hlasov ale spočíva skôr v myslení ľudí, než v spôsobe hlasovania. V podstate neexistuje spôsob, ako mu úplne zabrániť, snahou štátu by však malo byť čo najviac ho sťažiť, aby sa nikomu takéto praktiky neoplatili.

6. Spôsoby zaistenia bezpečnosti a dôveryhodnosti volieb prostredníctvom elektronických zariadení

Dôvera občanov je pri každých voľbách kľúčová, no pri elektronickom hlasovaní je jej zaistenie výrazne zložitejšie. Kým pri hlasovaní prostredníctvom papierových hlasovacích lístkov má každý občan možnosť bezprostrednej a priamočiarej kontroly, keďže pozná princíp a možné spôsoby zneužitia (ktoré môže po kontrole viac-menej jednoznačne potvrdiť alebo vylúčiť), pri hlasovaní prostredníctvom zložitých elektronických zariadení, navyše keď sa údaje často prenášajú cez internet alebo iný komunikačný kanál do centrály vzdialenej stovky či tisícky kilometrov od miesta odovzdania hlasu, sa funkčnosť zdá omnoho menej zjavnou a kontrola bez hlbokých znalostí kryptografie a technických aspektov fungovania takéhoto systému je v podstate vylúčená.

Väčšina občanov nemá inú možnosť, než spoliehať sa na expertov, ktorí však nemusia byť vždy nezávislí a ich hodnotenia môžu byť viac či menej skreslené. Preto otvorenosť takýchto systémov a dokumentácia dostupná včas a v celom rozsahu, sú nevyhnutnými predpokladmi na bezproblémový priebeh volieb, ako aj následnú akceptáciu výsledkov občanmi. Dôvera musí byť posudzovaná v dvoch rovinách – jednak na úrovni vlády ako

zákazníka a tiež na úrovni verejnosti ako používateľa. Verejnosť môže byť ďalej rozdelená na dve časti a to technických expertov, ktorí môžu prezentovať kvalifikované názory na bezpečnosť systému a občanov bez náležitých znalostí, ktorí sa musia spoliehať na týchto expertov. V prípade, že značná časť občanov nebude o dôveryhodnosti systému presvedčená, môže sa stať, že voľby prostredníctvom internetu budú odignorované a všetky vynaložené prostriedky vyjdú nazmar. V horšom prípade sa môže stať, že občania odmietnu uznať legitimitu takto zvolených zástupcov [29].

Problematika bezpečnosti je pri hlasovaní cez internet kľúčová a býva najčastejším argumentom odporcov. Je nutné poznamenať, že kým bude internetové hlasovanie iba doplnkovou možnosťou pri voľbách a paralelne sa budú konať aj papierové voľby, bezpečnosť nemôže vzrásť, potenciálne však môžu pribudnúť slabiny nového systému [30]. Pri riešení problematiky bezpečnosti je v zásade potrebné zaistiť zabezpečenie všetkých troch základných komponentov volebného systému:

- centrálnej infraštruktúry (táto môže byť realizovaná aj ako distribuovaná, teda pozostávajúca z viacerých vzájomne spolupracujúcich častí, pričom každú časť môže mať v správe iný subjekt)
- zariadenia, prostredníctvom ktorého volič realizuje svoju voľbu (najčastejšie to býva počítač, ale sú popísané aj riešenia, kde je možné voliť s použitím mobilného telefónu [31], či digitálnej televízie [32])
- komunikačného kanálu – obvykle internetovej linky medzi zariadením voliča a centrálnym systémom, ale v závislosti od implementácie to môže byť aj iný kanál

Centrálna infraštruktúra je miesto, ktoré bude v najväčšej miere pod drobnohľadom verejnosti a kde sa najviac sústredí úsilie osôb snažiacich sa narušiť priebeh volieb. Musí byť zabezpečená maximálna ochrana pred útokmi tak zvonku, ako aj zvnútra. V ideálnom prípade by mala byť rozdelená medzi čo najviac entít pod správou nezávislých subjektov, pričom na to, aby bola narušená bezpečnosť by museli všetky spolupracovať. V praxi býva rozdelenie minimálne na dve časti – jedna je pripojená do internetu a slúži na zber hlasov od voličov (ekvivalent volebnej urny), pričom však tieto sú zašifrované a druhá časť je fyzicky oddelená od verejných sietí a jej účelom je dešifrovať a spočítať hlasy [17].

Údaje sú medzi nimi prenášané na pamäťovom médiu (najčastejšie DVD) [9]. Veľkú pozornosť je nutné venovať už počiatočným fázam prípravy technických prostriedkov, aby sa úplne vylúčila možnosť neoprávnenej manipulácie. Všetky procedúry musia byť zdokumentované a do priestorov, v ktorých sa nachádzajú technické zariadenia používané na zaznamenávanie a počítanie hlasov môžu mať prístup iba oprávnené osoby.

Zaistenie dôveryhodnosti počítača (ako aj akéhokoľvek iného zariadenia použitého na odovzdanie hlasu) voliča je rovnako dôležité ako zabezpečenie ostatných častí systému. Problémom je, že kým pri volebných serveroch spravovaných štátnymi orgánmi sú na problematiku bezpečnosti vyčlenené značné finančné prostriedky a personálne kapacity, v prípade domácich používateľov je bezpečnosť často podceňovaná [33][34]. Mnohokrát sa stáva, že používateľ ani nevie, či je jeho počítač bezpečný a do akej miery mu môže dôverovať.

Pri nesprávne implementovanej volebnej schéme by sa mohlo stať, že hlas niektorého voliča v skutočnosti buď nebude vôbec započítaný, alebo bude pozmenený a volič sa o tom ani nedozvie. Veľkou hrozbou sú najmä rôzne druhy škodlivého softvéru inštalované na počítač bez vedomia jeho používateľa. Viac informácií k tejto problematike je možné nájsť v [35]. Preto sa v snahe o splnenie požiadavky overiteľnosti aj v prípadoch, keď počítač voliča nie je dôveryhodný, zvykne využívať druhý kanál na prenos informácií, nezávislý od (potenciálne nedôveryhodného) počítača [29]. Vhodnou voľbou je zaslanie SMS správy na mobilný telefón voliča, ktorá obsahuje informácie o prijatí hlasu. Je však nevyhnutné súčasne rešpektovať požiadavky súkromia a bezdokladovosti. Táto metóda sa využíva napríklad v nórskom systéme a podrobnejšie je popísaná v ďalších kapitolách.

7. Technická realizácia hlasovania prostredníctvom internetu

Elektronické volebné systémy sú obvykle postavené na použití asymetrickej kryptografie. Jej princíp tkvie v tom, že na rozdiel od symetrickej, kde sa používa ten istý šifrovací kľúč[4] na zašifrovanie aj dešifrovanie, tu je použitý pár šifrovacích kľúčov, ktoré sú matematicky prepojené, avšak z jedného nie je možné odvodiť druhý. Ak je nejaká operácia vykonaná jedným z nich, jej opak je možné urobiť druhým. Jeden z týchto kľúčov sa obvykle zverejní, kým druhý sa ponechá v tajnosti. Potom môže ktokoľvek zašifrovať údaje týmto verejným kľúčom, ale dešifrovať ich môže iba držiteľ súkromného.

Asymetrická kryptografia umožňuje aj schému, ktorú nazývame digitálny podpis. Držiteľ súkromného kľúča digitálne podpíše správu tak, že ju „zašifruje“ prostredníctvom tohto súkromného kľúča. „Dešifrovať“ ju môže ktokoľvek, kto má k dispozícii verejný kľúč. Ak sa mu to podarí, nadobudne istotu, že správa pochádza od držiteľa súkromného kľúča. Viac tejto problematike venujú práce [36] alebo [37]. Princíp asymetrickej kryptografie je znázornený na Obr. 6.

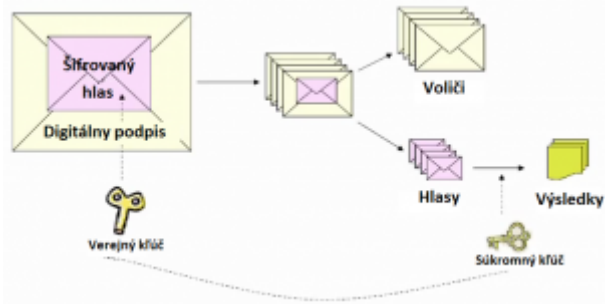
Obr. 6 Princíp asymetrickej kryptografie [38]

Pri úkone odovzdania hlasu cez internet je prvým a základným krokom autentifikácia, teda overenie totožnosti voliča. Je ekvivalentom predloženia občianskeho preukazu komisii vo volebnej miestnosti. Môže mať rôzne formy, od zadania prihlasovacieho mena a hesla (eventuálne v kombinácii so zadaním kontrolného kódu zaslaného SMS správou, ako je to bežné pri internet-bankingu), cez rôzne formy jednorazových či premenlivých hesiel [39] až po použitie čipových kariet [40], v ktorých sa používa asymetrická kryptografia.

Princíp elektronického hlasovania je veľmi podobný hlasovaniu prostredníctvom pošty,

ktoré je upravené v [21]. Základná schéma elektronického volebného systému je na Obr. 7. Po tom ako je volič pokúšajúci sa hlasovať prostredníctvom internetu autentifikovaný, je mu zobrazený zoznam strán a kandidátov. Keď si z nich vyberie, je jeho elektronický „hlasovací lístok“ zašifrovaný verejným kľúčom volebnej komisie (krok analogický s vložením do obálky) a digitálne podpísaný svojím súkromným kľúčom[5] (analógia s vložením do návratnej obálky). Takýto blok údajov je zabezpečeným kanálom prostredníctvom internetu poslaný do centrálneho systému, kde je bezpečne uložený.

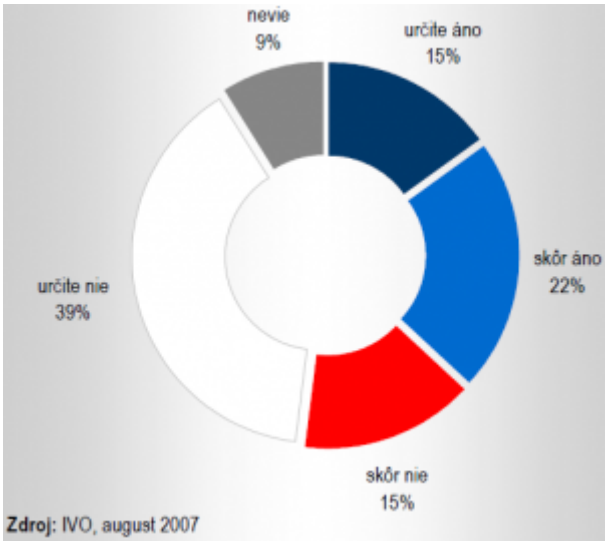
To ako volič hlasoval zatiaľ nemôže nikto zistiť, pretože by na to potreboval súkromný kľúč volebnej komisie. Aby sa zamedzilo kupovaniu hlasov a nátlaku medzi členmi spoločnej domácnosti, môže obvykle volič svoje hlasovanie viackrát zopakovať, pričom sa počíta iba jeho posledný odovzdaný hlas. V prípade, že sa rozhodne neskôr voliť vo volebnej miestnosti, hlas odovzdaný cez internet sa neberie do úvahy. Toto je možné vďaka tomu, že v úložisku je spojenie medzi identitou voliča a jeho zašifrovaným hlasom. Po ukončení internetového hlasovania je táto väzba odstránená a na systém spočítavania hlasov sú prenesené iba zašifrované hlasy bez informácie o identite voliča. Hneď na to sa zíde ústredná volebná komisia a použije svoj súkromný kľúč na dešifrovanie hlasov. Tie sú následne spočítané a vyhlásia sa výsledky.



Obr. 7 Základná schéma elektronického volebného systému [12]

8. Možnosti využitia internetu pri voľbách v podmienkach Slovenskej republiky

Slovenská republika je krajinou s pomerne rozšíreným používaním IKT svojimi obyvateľmi. Je teda možné uvažovať o zefektívnení demokratického procesu s vuyžitím nových spôsobom hlasovania.



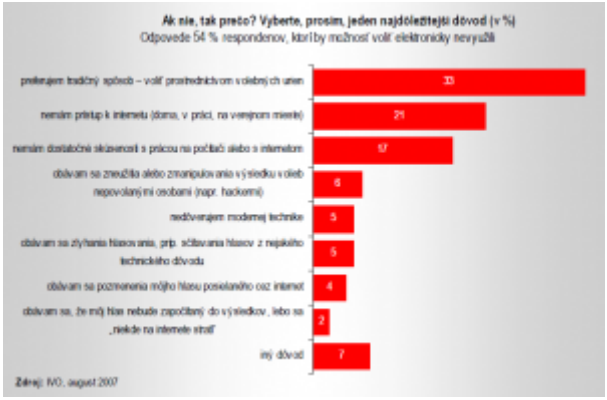
Obr. 8 Odpoveď na otázku: “Ak by bola možnosť voliť v najbližších parlamentných,

prezidentských ci komunálnych voľbách elektronicky – prostredníctvom internetu – využili by ste túto možnosť?"

Nutným predpokladom pre zavedenie elektronického hlasovania vo voľbách je však, okrem politickej vôle, aj postoj občanov k tejto otázke. Ak by bola veľká väčšina ľudí v štáte proti, mohlo by sa stať, že by takto vykonané voľby neboli všeobecne rešpektované (podrobnejšie sa tomu venujeme v kapitole 6). Prieskum Inštitútu pre verejné otázky na tému e-demokracie, kde bola načrtnutá aj problematika elektronických volieb, ktorý sa konal v roku 2007, ukázal, že ľudia stále preferujú tradičnú formu hlasovania. Ak by bola možnosť voliť v najbližších voľbách elektronicky, určite alebo skôr áno by ju využilo 37% opýtaných, určite alebo skôr nie až 54%. Nevedelo odpovedať 9% opýtaných.

Ako najčastejšie dôvody udávali preferovanie tradičného spôsobu (33%), absenciu prístupu na internet (21%), nedostatočné skúsenosti s prácou s počítačom (17%), obavy o bezpečnosť (12%), či nedôveru technike alebo obavy zo zlyhania (10%). Zaujímavou skutočnosťou je, že opýtaní nevyjadrili obavu o prípadné vyzradenie ich voľby (porušenie zásady tajnosti hlasovania). Skutočnosť, že by sa niekto nezúčastnil elektronického hlasovania však nutne neznamená, že je proti nemu. Zvlášť v prípade, ak udáva dôvody ako absencia prístupu na internet alebo nedostatočné skúsenosti s prácou na počítači. Na základe výsledkov referenda z roku 2010 [41], možno badať istý posun vo verejnej mienke.

Aj keď účasť na tomto referende bola iba 22,84% oprávnených voličov, čo môže naznačovať nezáujem ľudí tak o verejné dianie všeobecne, ako aj otázky, ktoré boli položené. Na druhej strane ale mohla veľká časť týchto občanov takýmto spôsobom vyjadriť svoj nesúhlas so všetkými šiestimi otázkami, keďže neplatnosť referenda má rovnaké účinky ako explicitné hlasovanie proti. Môžeme však predpokladať, že veľká väčšina z tých, ktorí sa referenda nezúčastnili nemá jednoznačný postoj. Z tých, ktorí sa zúčastnili, na otázku číslo 5 „Súhlasíte s tým, aby Národná rada Slovenskej republiky ustanovila možnosť voliť poslancov Národnej rady Slovenskej republiky a poslancov Európskeho parlamentu prostredníctvom internetu?" odpovedalo kladne 70,46%, záporne 22,22% a neplatných hlasov bolo 7,3%.



Obr. 9 Najčastejšie dôvody odmietania hlasovania prostredníctvom internetu [42]

Ďalším dôležitým faktorom pre možnosť hlasovania prostredníctvom internetu je problematika autentifikácie voliča. Najlepším variantom sa ukazujú byť čipové karty, no keby sa mali vydávať osobitné volebné preukazy pre každého občana, ktorý by o to

požiadal, bolo by to jednak ekonomicky neúnosné a tiež by to mnohých voličov odradilo od elektronického hlasovania. Najvýhodnejšie by teda bolo integrovať čip do občianskych preukazov. Na Slovensku sa vydávanie občianskych preukazov s čipom schválilo v roku 2012 [43][44]. Potrvá však istý čas (rádovo niekoľko rokov), kým sa občianske preukazy s čipom rozšíria natoľko, že ich bude mať väčšina občanov. Ďalšie kroky, okrem prijatia potrebných zákonov, sú najmä technického charakteru.

Bolo by potrebné, po predchádzajúcej verejnej diskusii technicky zrealizovať systém, ktorý by umožňoval hlasovanie prostredníctvom internetu a spĺňal by všetky kritériá na zaistenie spravodlivých volieb [45]. Tu sa však môžu využiť skúsenosti z iných krajín, ktoré už podobným procesom prešli. Dôležitým aspektom je, aby existovalo rozdelenie kometencií Vhodným riešením je zverenie kľúčových komponentov volebného systému Štatistickému úradu SR, nakoľko tento by mal byť politicky nezávislý. Ďalšími inštitúciami vhodnými na správu niektorých subsystémov sú ministerstvá vnútra, spravodlivosti, či financií.

9. Záver

V práci sme pojednávali o problematike využitia informačných a komunikačných technológií pri hlasovaní vo voľbách. Aj keď funkcie volieb zostávajú rovnaké a ich podstata sa nemení, spôsob ich prevedenia sa vyvíja v súlade s technickým pokrokom. Venovali sme sa predovšetkým absenčným spôsobom hlasovania, teda možnostiam uskutočnenia voľby z miesta mimo volebnej miestnosti. Podľa niektorých názorov otázka nestojí, či by malo byť internetové hlasovanie umožnené, ale kedy [45]. Popísali sme požiadavky kladené na takéto systémy, ich výhody a nevýhody, rozsah používania v niektorých štátoch sveta, ako aj možnosti ich zavedenia s prihliadnutím na podmienky Slovenskej republiky.

Pre uskutočnenie voľby na diaľku nemusí byť nutné použiť počítač, ale je možné tento úkon realizovať aj s využitím iných zariadení ako sú mobilné telefóny, tablety, či zariadenia na sledovanie digitálnej televízie [32]. Zistili sme, že je to veľmi perspektívny spôsob posilnenia demokracie a po vyriešení prvotných problémov by mohol zjednodušiť hlasovanie najmä ľuďom žijúcim v zahraničí a hendikepovaným, v dlhodobom časovom horizonte znížiť celkové náklady, ako aj zrýchliť sčítavanie hlasov a odstrániť ľudské chyby pri ich sčítavaní. Najväčšie ťažkosti pri nasadzovaní sú najmä politického a sociálneho charakteru, pretože príklad krajín ako Estónsko či Nórsko nám dokazuje, že technickú realizáciu je možné zvládnuť bez väčších problémov.

10. Zoznam použitej literatúry

1. HORVÁTH, P. Voľby a volebné systémy, In: Slovenská politologická revue, 4/2004, s. 2-3.
2. KLOKOČKA, V. Ústavní systémy evropských státu. Praha: Linde Praha, a.s., 1996. 304-305 s. ISBN 80-7201-606-7
3. Smithsonian Gear-and-Lever Voting Machine [online]. : National Museum of American , 2004 [cit 2012-04-17], Dostupné na internete: http://americanhistory.si.edu/vote/resources_gearlever.html
4. RETEROVÁ, S. Způsoby hlasování ve volbách a jejich historický vývoj: hlasovací technika jako stěžejní proměnná volebního procesu [online]. Brno: Středoevropské

politické studie, 2007 [cit 2012-04-17], Dostupné na internete: http://www.cepsr.com/clanek.php?ID=306
5. RNIB Digital Accessibility Team. Countries with e-voting projects [online]. London: Royal National Institute of Blind People, 2009 [cit 2012-04-17], Dostupné na internete: http://www.tiresias.org/research/guidelines/evoting_projects.htm
6. CBC News. Halifax prepares for online voting [online]. Toronto: CBC News, 2008 [cit 2012-04-17], Dostupné na internete: http://www.cbc.ca/news/canada/nova-scotia/story/2008/09/25/halifax-electronic-voting.html
7. SIBLEY, K. Markham voters go from in line to online [online]. Ontario: ITbusiness.ca, 2003 [cit 2012-04-17], Dostupné na internete: http://www.itbusiness.ca/it/client/en/Home/News.asp?id=5272
8. WOODARD, C. Estonia, where being wired is a human right [online]. Boston: The Christian Science Monitor, 2003 [cit 2012-04-17], Dostupné na internete: http://www.csmonitor.com/2003/0701/p07s01-woeu.html
9. MARTENS, T. Internet voting in Estonia. In: eVoting International Conference. Bratislava: IT Asociácia Slovenska, 2011
10. BLAKLEY, G. R. "Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference. Baltimore: ICSCA, 1979
11. SHAMIR, A. How to share a secret. In: Communications of the ACM. New York: ACM, 1979
12. MARTENS, T. E-Voting System: General Overview [online]. Tallinn: Estonian National Electoral Committee, 2010 [cit 2012-04-17], Dostupné na internete: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf
13. ANSPER, A. – BULDAS, A. – JÜRGENSON, A. – ORUAAS, M. – PRIISALU, J. – RAIEND, K. – VELDRE, A. – WILLEMSON, J. – VIRUNURM, K. E-voting concept security: analysis and measures [online]. Tallinn: National Electoral Committee, 2010 [cit 2012-04-17], Dostupné na internete: http://www.vvk.ee/public/dok/E-voting_concept_security_analysis_and_measures_2010.pdf
14. KRIPP, M. Interview. In: eVoting International COnference. Bratislava: IT Asociácia slovenska, 2011
15. Agency for Public Management and eGovernment MinID: Your public ID [online]. Oslo: Norwegian e-goverment portal, 2012 [cit 2012-04-17], Dostupné na internete: http://minid.difi.no/minid/minid.php?lang=en
16. NORE, H. Internet voting in Norway 2011. In: eVoting International Conference. Bratislava: IT Asociácia Slovenska, 2011
17. SPYCHER, O. – VOLKAMER, M. – KOENIG, R. Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting. In: VoteID'11, 3rd International Conference on E-Voting and Identity. Talinn: International Association for Voting System Sciences, 2011
18. FRANKOVIČ, R. Elektronické voľby: bakalárska práca. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2009. 40 s.
19. RJASKOVA, Z. Electronic voting schemes. Bratislava: Comenius university, 2002. 63 s.
20. JAMES, K. Astronauts Cast Vote From Space Thanks to 1997 Texas Law [online]. Galveston: Gather, 2012 [cit 2012-04-17], Dostupné na internete: http://news.gather.com/viewArticle.action?articleId=281474978657286
21. Zákon č. 333/2004 Z.z. o voľbách do Národnej rady Slovenskej republiky

22. NORDEN, L. The Machinery of Democracy: Voting System Security, Usability, and Cost, In: Voting Rights & Elections Project, 2006, s. 175.
23. Benátska komisia. Odporúčania č. 190/2002 (Code of Good Practice in Electoral Matters). Rada Európy, 2003
24. KRNÁČ, K. Interview. In: eVoting International Conference. Bratislava: IT Asociácia Slovenska, 2011
25. MISTRÍK, R. Interview. In: eVonting International Conference. Bratislava: IT Asociácia Slovenska, 2011
26. kol. Encyclopaedia Of Information Technology. New Delhi: Atlantic Publishers & Distributors, 2007. 397 s. ISBN 81-269-0752-5
27. DEKEL, E. – JACKSON, M. – WOLINSKY, A. Vote Buying, In: Journal of Political Economy, 2008, s. 30.
28. DRGONEC, J. Elektronické voľby: problém práva alebo demokracie?. In: eVoting International Conference. Bratislava: IT Asociácia Slovenska, 2011
29. ANSPER, A. – HEIBERG, S. – LIPMAA, H. – VERLAND, T. A. LAENEN, F. Security and Trust for the Norwegian E-votingPilot Project E-valg 2011. In: NordSec ’09 Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age. Oslo: University Graduate Centre, 2009
30. GAŽI, P. Elektronické voľby: utópia alebo realita? [online]. Bratislava: FMFI UK, 2011 [cit 2012-04-17], Dostupné na internete: www.dcs.fmph.uniba.sk/~gazi/uib/materialy/volby.pdf
31. NÁDASKÝ, Ľ. Ako voliť mobilným telefónom. In: eVoting International Conference. Bratislava: IT Asociácia slovenska, 2011
32. CALDELLI, R. – BECARELLI, R. – FILIPPINI, F. – PICCHIONI, F. – GIORGETTI, R. Electronic Voting by Means of Digital Terrestrial Television: The Infrastructure, Security Issues and a Real Test-Bed. In: Software Services for e-Business and e-Society 9th IFIP WG 6.1 Conference on e-Business, e-Services and e-Society. Nancy: I3E, 2009
33. KAWAMOTO, D. Survey: Most home PC users lack security [online]. San Francisco: CNET News, 2005 [cit 2012-04-17], Dostupné na internete: http://news.cnet.com/Survey-Most-home-PC-users-lack-security/2100-1029_3-5986344.html
34. Ernst & Young. Risk at Home: privacy and security risks in telecommuting [online]. London: Ernst and Young: Center for Democracy and Technology, 2007 [cit 2012-0--17], Dostupné na internete: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/PrivacyResources/DownloadableDocuments/EYCDTRiskatHomePrivacyandSecurityinTelecommuting.pdf
35. NASH, T. An Undirected Attack Against Critical Infrastructure, In: Vulnerability & Risk Assessment Program (VRAP), 2005, s. 11.
36. FERGUSON, N. – SCHNEIER, B. Practical cryptography. New York: Wiley, 2003. 410 s. ISBN 0-471-22357-3
37. MENEZES, A. – VAN OORSCHOT, P. C. – VANSTONE, S. A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. 816 s. ISBN 0-8493-8523-7
38. KLOKOČOVÁ, L. Šifrovanie [online]. Bratislava: SOŠ Vranovská 4, 2009 [cit 2012-0--17], Dostupné na internete: http://www.sosvranovska.eu/KLOKOCOVA/CO%20V%20SKOLE/INF%20pom%C4%82%C2%B4cky/%C5%A0ifrovanie.pdf
39. M’RAIHI, D. – MACHANI, S. – PEI, M. – RYDELL, J. Time-based One-time Password

Algorithm, In: IETF Draft, , s. 14.
40. KÜMERLING, O. – KUHN, M. G. Design Principles for Tamper-Resistant SmartcardProcessors, In: Advanced digital security research, 2005, s. .
41. ŠÚ SR. Referendum 2010 [online]. Bratislava: Štatistický úrad Slovenskej republiky, 2010 [cit 2012-04-17], Dostupné na internete: http://app.statistics.sk/ref2010/menu/indexV.jsp?lang=sk
42. VELŠIC, M. e-Demokracia na Slovensku: Správa z výskumu. Bratislava: Inštitút pre verejné otázky, 2008. 29 s. ISBN 978-80-89345-02-1
43. Ministerstvo vnútra SR. Slovensko začne tento rok vydávať občianske preukazy s elektronickým čipom [online]. Bratislava: Tlačové správy MV SR, 2012 [cit 2012-0--17], Dostupné na internete: http://www.minv.sk/?25&sprava=slovensko-zacne-tento-rok-vydavat-obcianske-preukazy-s-elektronickym-cipom
44. Sita. Nové občianske preukazy budú mať čipy [online]. Bratislava: Denník SME, 2012 [cit 2012-04-17], Dostupné na internete: http://www.sme.sk/c/6240177/nove-obcianske-preukazy-budu-mat-cipy.html
45. TÓTH, Š. Cesta k elektronickým voľbám. In: eVoting International Conference. Bratislava: IT Asociácia slovenska, 2011

Spoluautorom článku je Mgr. Ing. Milan Potančok, PhD., Oddelenie ekonomiky a manažmentu podnikania. Študentská vedecká konferencia, Akademický rok 2011/2012

---

[1]Náklady závisia od toho, ako často sa voľby konajú. Čím sú častejšie, tým nižšie sú náklady, pretože na jedny voľby pripadá menšia suma

[2]Ide predovšetkým o pracovníkov inštitúcií spravujúcich systém, nezávislých pozorovateľov, kameramanov, atď.

[3]V prípade, že sa hlasy spočítavajú pomocou elektronických prostriedkov pripojených do verejných sietí, je táto hrozba aj tu. Minimálne je však možnosť opätovného prepočítania hlasov na základe archivovaných papierových materiálov (zápisníc a hlasovacích lístkov)

[4]Šifrovací kľúč je informácia, ktorá určuje priebeh kryptografického algoritmu. Pri šifrovaní, kľúč špecifikuje transformáciu správy do šifrovaného textu, pri dešifrovaní je tomu naopak

[5]V prípade využitia čipových kariet (ako je to v Estónsku) je tento kľúč uložený na čipovej karte. V iných prípadoch (napr. Nórsko) ho volič obdrží po autentifikácii.