UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2025 Daniel Pospíšil

Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Elektronický volební systém

Bakalářská práce

2025 Daniel Pospíšil

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Daniel Pospíšil**
Osobní číslo:	**I22131**
Studijní program:	**B0688A140009 Informační technologie**
Téma práce:	**Elektronický volební systém**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem této bakalářské práce je navrhnout elektronický volební systém, který by mohl být použit pro zajištění bezpečných, transparentních a efektivních voleb různých volebních schémat.
V teoretické části bakalářské práce budou zhodnoceny technické, právní a sociální aspekty implementace volebního systému a bude provedena rešerše dostupných řešení na trhu.
V aplikační části bakalářské práce bude navržen a vytvořen systém pro elektronické volby. Systém bude umožňovat více volebních schémat. Systém bude navržen tak, aby reflektoval potřebu vysoké míry zabezpečení volebního procesu. K vytvořenému systému budou zpracovány metodické pokyny pro administrátora systému, členy volební komise a další účastníky voleb.

Rozsah pracovní zprávy: **30 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná**

Seznam doporučené literatury:

FLANAGAN, David. JavaScript: the definitive guide. Seventh edition. Sebastopol: O´Reilly, 2020. ISBN 1491952024.
ŽÁRA, Ondřej. JavaScript: programátorské techniky a webové technologie. Brno: Computer Press, 2015. ISBN 9788025145739.
BEASLEY, Michael. Practical web analytics for user experience: how analytics can help you understand your users. Amsterdam: Morgan Kaufmann, an imprint of Elsevier, 2013.
ANISOVÁ, Hana a MÜLLER, Miroslav. UML srozumitelně. 2. aktualiz. vyd. Brno: Computer Press, 2007. ISBN 8025110834.
SOMMERVILLE, Ian. Softwarové inženýrství. Brno: Computer Press, 2013. ISBN 978-80-251-3826-7.
DUCKETT, Jon; STONE, Emme a ULLMAN, Chris. PHP & MySQL: server-side web development. Hoboken, New Jersey: Wiley, [2022]. ISBN 1119149223.

Vedoucí bakalářské práce: **Ing. Lukáš Čegan, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **15. prosince 2024**
Termín odevzdání bakalářské práce: **16. května 2025**

L.S.

prof. Ing. Petr Doležel, Ph.D. v.r.
děkan

Ing. Jan Panuš, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 28. února 2025

Prohlašuji:

Práci s názvem Elektronický volební systém jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 11. 5. 2025

Daniel Pospíšil v.r.

PODĚKOVÁNÍ

Tímto bych rád poděkoval svému vedoucímu práce, panu Ing. Lukáši Čeganovi, Ph.D., a to především za jeho cenné rady a připomínky, stejně jako za vřelý, avšak kritický přístup, který po celou dobu k mé práci zaujímal. Zvláště si cením času, který této práci osobně věnoval. Dále bych velmi rád poděkoval své rodině za její podporu a mnohdy i trpělivost nejen při vypracovávání této práce, ale i během celého studia, kdy mi byla pevnou oporou.

ANOTACE

Tato bakalářská práce se zabývá elektronickými volebními systémy. Cílem práce je navrhnout a implementovat funkční prototyp volební aplikace, která klade důraz na bezpečnost, anonymitu, dostupnost a jednoduchost použití. V teoretické části jsou popsány základní principy elektronického hlasování, přehled již existujících řešení a analýza funkčních a nefunkčních požadavků na systém. Experimentální část se věnuje návrhu systému a realizaci webové aplikace. Výsledný systém demonstruje možnosti moderních technologií při nahrazování tradičních volebních procesů.

KLÍČOVÁ SLOVA

Volby – korespondenční volby – elektronické volby – elektronické hlasování – volební právo – kybernetická bezpečnost – šifrovací algoritmus

TITLE

Electronic voting system

ANNOTATION

This bachelor's thesis deals with electronic voting systems. The aim of this thesis is to design and implement a functional prototype of a voting application with an emphasis on security, anonymity, accessibility, and ease of use. The theoretical part describes the basic principles of electronic voting, provides an overview of existing solutions, and analysis of functional and non-functional requirements for the system. The experimental part focuses on system design and the implementation of a web application. The final system demonstrates the potential of modern technologies in replacing traditional voting processes.

KEYWORDS

Elections – correspondence elections – electronic elections – electronic voting – suffrage – cyber security – crypting algorithm

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ČR – Česká republika

LZPS – Listina základních práv a svobod (definované v ústavním zákonu č. 2/1993 Sb. ve znění pozdějších předpisů)

COVID-19 – infekční onemocnění Sars-CoV-2, které koncem roku 2019 způsobilo celosvětovou pandemii

QR kód – Quick Response kód

USA – Spojené státy americké (angl. United States of America)

EVM – Electronic Voting Machines

ID – jednoznačný identifikátor

MFA – Multi-Factor Authentication

DDoS útok – Distributed Denial-of-service

AES-256 – Advanced Encryption Standard 256-bit

RSA – Rivest-Shamir-Adleman

HTTP – HyperText Transfer Protocol

FTP – File Transfer Protocol

HDD – pevný disk pro ukládání dat, obsahuje pohyblivé části (angl. Hard Disk Drive)

SSD – pevný disk pro ukládání dat, obsahuje NAND flash čipy (angl. Solid-State Drive)

PDF – univerzální formát souboru pro dokumenty (angl. Portable Document Format)

PDO – PHP Document Object

1:N – vazba relačních databází, jednomu záznamu je přiřazeno více záznamů z jiné tabulky

M:N – vazba relačních databází, více záznamům je přiřazeno více záznamů z jiné tabulky

ECC – Elyptic-curve cryptography (nikoli Error Code Correction)

TERMINOLOGIE

QR kód – jedná se o typ kódu, ve kterém mohou být uchovávána data a který je možné načíst příslušnou čtečkou QR kódů

EVM – elektronické hlasovací zařízení, založené buď na technologii optického skenu, nebo přímého záznamu

MFA – vícefázové ověření totožnosti na základě více na sobě nezávislých metod, například pomocí hesla a kódu v mobilním telefonu

DDoS útok – cílený kybernetický distribuční útok za účelem zahlcení a znepřístupnění určité služby ostatním uživatelům

AES-256 – standard šifrovacího algoritmu využívající 256bitový klíč

RSA – standard šifrovacího algoritmu na principu rozložení na prvočísla

HTTP – nezabezpečený protokol pro komunikaci s webovými servery

FTP – protokol pro vzdálené sdílení souborů

HDD – druh pevného disku pro ukládání dat, obsahuje v sobě pohyblivé části

SSD – druh pevného disku pro ukládání dat, na rozdíl od HDD neobsahuje pohyblivé části, ale NAND flash čipy

PDO – komponenta programovacího jazyka PHP pro práci s objekty nebo databází

Zdrojový kód – soubor napsaný v určitém programovacím jazyce, který má svoji logiku

Šifrovací algoritmus – logický postup určený k zakrytí komunikace tak, že komunikace nebude čitelná

Hardware – fyzické vybavení počítače

Software – programové vybavení počítače

Open-source software – software, který je k dispozici zdarma a má otevřený zdrojový kód, což znamená, že si jej každý může upravit podle sebe

Hash – náhodná směs čísel a písmen, která nedávají žádný význam

Časové razítko – časový údaj značený pomocí čísla, jehož hodnota odpovídá UNIX hodinám

Phishing – internetový podvod používaný k získání citlivých osobních údajů, jako je například číslo kreditní karty

GDPR – obecné nařízení o ochraně osobních údajů

Framework – softwarový rámec, který poskytuje sadu nástrojů, knihoven a předdefinovaných struktur pro usnadnění vývoje aplikací

Entitně relační diagram – typ diagramu běžně používaný mezi programátory v případě potřeby zobrazení algoritmu

MySQL – databázový systém vyvinutý firmou Oracle

SQLite – „odlehčená“ verze systému MySQL

Entita – v oboru databází označení pro tabulku

ECC – způsob asymetrického šifrování na základě výpočtů nad eliptickými křivkami

ÚVOD

Když se řekne termín „volby“, většina lidí si jej spojí především s volbami týkajícími se politiky, v nichž jsou voleni kandidáti do veřejně činných pozic. Není to však pouze politické prostředí, kde se volí. Může se jednat například o volby do akademické obce, školské rady nebo různých spolků. Jednu vlastnost však všechny tyto druhy voleb mají společnou, a tím je nutnost fyzické přítomnosti voliče. Je nutné si ale uvědomit, že výpočetní technologie se stále vyvíjejí směrem kupředu, a proto dříve nebo později nastane doba, kdy se i právě zmíněné volby budou vyřizovat primárně elektronicky. Lze však předpokládat, že tento přechod bude postupný a půjde ruku v ruce s digitalizací celého systému. V konečném důsledku se stačí pouze zamyslet nad tím, jaká byla úroveň digitalizace a komunikace ještě před pěti až deseti lety nejen v České republice, ale i ve světě. K výraznější potřebě a urychlení celkové digitalizace poskytovaných služeb přispěla z nemalé části rovněž pandemie onemocnění COVID-19. Teprve v té době se například hojně začaly používat dříve zřídkakdy používané QR kódy. Elektronické hlasování je tedy logický vývoj v kontextu dnešních technologií. Ať už se jedná o jakoukoli digitální alternativu ke stávajícímu stavu, má za úkol především zjednodušit a zrychlit celý proces. Dalším benefitem může být určité pohodlí pro uživatele. Oprávněné obavy však existují kvůli zabezpečení, transparentnosti nebo kvůli možnému neoprávněnému sledování uživatelů.

Cílem této bakalářské práce je tedy navrhnout vhodný elektronický systém hlasování, který bude mít kromě uživatelské přívětivosti především korektně vyřešené zabezpečení, díky němuž bude systém vhodný pro použití v reálném nasazení. V první části je práce zaměřena na teoretickou stránku. Zde se řeší především volby v teoretické rovině do větší hloubky. Dále jsou v této části popsané i dnešní způsoby a možnosti hlasování, včetně jejich výhod a nevýhod, a příklady implementací elektronických volebních systémů. Ve druhé části se práce zaměřuje na konkrétní implementaci elektronického volebního systému po praktické stránce. Zde se tedy nachází popis implementace navrhovaného řešení, které je doplněno nejen o část zdrojového kódu tohoto navrhovaného systému, ale i o snímky obrazovky, na nichž je znázorněna vizuální podoba celé implementace.

1. VOLBY A VOLEBNÍ SYSTÉMY

1.1. Historie a současnost voleb

Historie volebního práva je dlouhá a rozmanitá, odrážející změny v politických, ekonomických a sociálních systémech po celém světě. Vývoj volebního práva byl často spojen s bojem za rovnost, demokracii a spravedlnost.

Ve starověku měli hlasovací právo pouze svobodní muži, občané města, což představovalo malou část populace. Otroci, ženy a cizinci hlasovací právo neměli. V Římské říši bylo rozhodování omezeno jen na majetné občany. Přístup k volebnímu právu byl tedy spojen s majetkem a sociálním postavením.

Ve středověku volební právo v moderním smyslu neexistovalo. Politická moc byla koncentrována v rukou šlechty a duchovenstva. S nástupem osvícenství se začínají objevovat myšlenky politické rovnosti a lidských práv. Americká revoluce a Velká francouzská revoluce přinesly myšlenky všeobecného volebního práva. Zpočátku však bylo omezeno pouze na majetné muže. S průmyslovou revolucí a šířením liberalismu roste tlak na rozšíření volebního práva.

V 19. století byl Nový Zéland první zemí, která zavedla všeobecné volební právo pro ženy, a v Evropě pak Finsko, které povolilo ženám nejen volit, ale i kandidovat.

V Československu ženy získaly volební právo po vzniku republiky. V průběhu 20. století se postupně zavádí volební právo pro všechny dospělé osoby bez ohledu na majetek, rasu, pohlaví nebo náboženství. V roce 1920 byla v Československu přijata ústava zaručující všeobecné a rovné volební právo.

Až do roku 1971 neměly ženy ve Švýcarsku federální volební právo.[1]

V současnosti je volební právo považováno za základní lidské právo, ale v praxi existují jistá omezení. Některé skupiny (např. vězni, mentálně postižení nebo cizinci) jsou stále v mnoha zemích vyloučeny. Diskriminace na základě rasy, etnického původu nebo pohlaví byla ve většině zemí odstraněna, i když ne vždy zcela.

1.2. Význam voleb a jejich funkce

Volby jsou formální proces a mohou být jedním z mnoha druhů různých forem výběru rozhodování. Označují počin, při kterém je nabízen výběr minimálně mezi dvěma nebo více

možnostmi. Volby mohou být považovány i jako označení svobodného rozhodnutí jednotlivce nebo odpovědnosti za vlastní činy. Mohou také znamenat nabídku či možnost a jsou chápány jako tradiční mechanismy právoplatné účasti v novodobém uspořádání fungující společnosti.

1.3. Volební právo

Právo volit je zakotveno v Ústavě České republiky, podrobně upraveno volebními zákony. Toto právo upravuje Článek 21 LZPS a stanovuje základní pravidla.

- Občané mají právo podílet se na správě veřejných věcí přímo nebo svobodnou volbou svých zástupců.
- Volební zákon stanoví podmínky, za kterých je volební právo vykonáváno.
- Volební právo je všeobecné, rovné a koná se tajným hlasováním.
- Každý občan má za rovných podmínek přístup k voleným a jiným veřejným funkcím.

Jedná se tedy o základní demokratické právo občanů, které je rozděleno na dvě hlavní složky, a to aktivní volební právo a pasivní volební právo.

Aktivní volební právo má každý občan České republiky, který dosáhl věku 18 let nejpozději v den voleb. U některých voleb mohou hlasovat i občané Evropské unie s trvalým pobytem v ČR. Jde například o komunální volby nebo volby do Evropského parlamentu.

Pasivní volební právo neboli právo být volen je klíčovým prvkem demokratických společností a odvíjí se od druhu voleb. Jakékoli omezení tohoto práva musí být řádně odůvodněné a nesmí obsahovat jakýkoli diskriminační prvek. Takovéto důvody zahrnují například nedostatečná věková hranice pro kandidaturu nebo bezúhonnost. Například do Poslanecké sněmovny může kandidovat občan ČR, který dosáhl věku minimálně 21 let, na post senátora může být volen občan ČR, který dosáhl věku 40 let, do obecních zastupitelstev může kandidovat občan ČR nebo Evropské unie starší 18 let s trvalým pobytem v dané obci, krajským zastupitelem se může stát občan ČR starší 18 let s trvalým pobytem v ČR a na prezidenta republiky může kandidovat občan ČR starší 40 let a s podporou alespoň 50 000 občanů, 20 poslanců nebo 10 senátorů. Do jakékoli jiné volené funkce může kandidovat osoba splňující podmínky, které stanovil daný subjekt ke kandidatuře.[2]

1.3.1. Základní pravidla volebního práva

Tato pravidla vycházejí z demokratických principů a jsou zakotvena v ústavách, volebních zákonech většiny demokratických zemí. Definují podmínky, za kterých mají občané pravidlo volit, být voleni a zajišťují férový a svobodný průběh voleb.

Základní pravidla volebního procesu zahrnují:

- **Všeobecnost** – každý občan má právo volit, pokud splňuje zákonem stanovené podmínky (např. věk a občanství). Výjimku tvoří osoby s omezením ve svéprávnosti či odpykávající si trest odnětí svobody (záleží na zemi).
- **Rovnoprávnost** – každý hlas má stejnou váhu bez ohledu na sociální postavení, majetek, náboženství, pohlaví či jiné charakteristiky voliče.
- **Přímost** – volby jsou zpravidla přímé, což znamená, že občané hlasují přímo pro své zástupce bez prostředníků.
- **Svobodnost** – volby musí být organizovány tak, aby voliči mohli svobodně vyjádřit svou vůli bez nátlaku, zastrašování nebo manipulace.
- **Přístupnost** – hlasování musí být dostupné všem oprávněným voličům včetně těch s omezenou mobilitou, zdravotním postižením nebo pobytem v zahraničí.
- **Anonymita** – každý volič má právo hlasovat tajně, což zajišťuje svobodu volby a ochranu před případným nátlakem.
- **Pravidelnost** – volby se konají pravidelně v předem stanovených intervalech, což zaručuje kontinuitu demokratického procesu.
- **Transparentnost a spravedlnost** – průběh voleb musí být transparentní a spravedlivý, aby bylo zajištěno, že výsledky odpovídají vůli voličů.

1.3.2. Podmínky k výkonu volebního práva

Podmínky k výkonu volebního práva jsou pro každý jednotlivý druh voleb vymezeny ve volebních zákonech či stanovách spolků, sdružení atd. a řadou prováděcích předpisů. Volební zákony, kterých se toto týká, jsou následující:

- Zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky, ve znění pozdějších předpisů (pro Parlament České republiky)[3]
- Zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů, ve znění pozdějších předpisů (pro zastupitelstva krajů)[4]

- Zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí, ve znění pozdějších předpisů (pro zastupitelstva obcí)[5]
- Zákon č. 62/2003 Sb., o volbách do Evropského parlamentu, ve znění pozdějších předpisů (pro Evropský parlament)[6]
- Zákon č. 275/2012 Sb., o volbách prezidenta republiky, ve znění pozdějších předpisů (pro prezidenta republiky)[7]

1.4. Druhy voleb

Aniž bychom si to mnohdy uvědomili, volby se uskutečňují téměř každou chvíli. Ať už se jedná o politické funkce či volby z oblasti soutěží, hodnocení uměleckých děl, akademického prostředí, výběru zástupců organizací, komunit, zájmových skupin, rozhodnutím o prioritách nebo jiných formách kolektivního rozhodování. Druhů voleb je opravdu velké množství, a tedy seznam těch nejčastějších je následující:[8]

- Volby podle úrovně rozhodování v politickém spektru
    - Parlamentní volby – volby do zákonodárného sboru, jako jsou Poslanecká sněmovna a Senát v České republice
        - Poslanecká sněmovna – volí se 1x za 4 roky
        - Senát – volí se 1x za 2 roky, a to vždy 1/3 senátorů
    - Prezidentské volby – volby prezidenta republiky, od roku 2013 je v České republice zavedena přímá volba prezidenta ČR, volí se 1x za 5 let
    - Regionální volby – volby do krajských zastupitelstev nebo regionálních orgánů, volí se 1x za 4 roky
    - Komunální volby – volby do obecních zastupitelstev nebo městských rad, volí se 1x za 4 roky
    - Evropské volby – volby do Evropského parlamentu v zemích Evropské unie, volí se 1x za 5 let

- Volby v profesních organizacích
    - Volby v profesních komorách – například volby do lékařské, notářské, advokátní nebo jiné profesní komory
    - Volby ve svazech a asociacích – například volby do vedení odborových organizací, podnikatelských svazů nebo zájmových sdružení

- Volby ve školství (mateřské, základní a střední školy)
    - Volby do školské rady – pro zajištění spolupráce mezi školou, rodiči, učiteli a zřizovatelem
    - Volby do studentské rady – zastupování zájmů žáků a studentů vůči vedení školy
    - Volba třídního mluvčího – prostředník mezi učiteli, vedením školy a třídou
    - Hlasování o školních projektech a aktivitách – hlasování o volbě školního výletu, programu na školních akcích nebo jiných důležitých otázkách týkajících se školy

- Volby v akademickém prostředí vysokých škol
    - Volby do akademického senátu – hlasování studentů a akademiků o složení orgánů na univerzitách a jejich fakultách
    - Volby rektora nebo děkana – obvykle prováděné akademickými senáty, které vybírají vedení univerzit a jejich fakult

- Volby v občanských spolcích a komunitách
    - Volby ve spolcích – například volby do vedení sportovních, kulturních nebo jiných zájmových sdružení
    - Volby v komunitních organizacích – například výběr představitelů v místních komunitách a neformálních skupinách

- Volby v korporacích a firmách
    - Volby správní rady – akcionáři nebo členové korporací volí vedení společnosti, jako je představenstvo nebo správní rada
    - Volby zaměstnaneckých zástupců – například volby zástupců zaměstnanců do dozorčích rad nebo výborů

- Volby v církvích a náboženských organizacích
    - Volby duchovních představitelů – například volba biskupů, rabínů nebo jiných náboženských vůdců
    - Volby rad farností nebo jiných náboženských orgánů – hlasování členů náboženských komunit o jejich vedení
- Volby v mezinárodních organizacích

    - Volby do vedení těchto organizací – například volby generálních tajemníků, prezidentů nebo předsedů mezinárodních organizací, např. OSN, UNESCO, NATO apod.

- Volby v neformálních skupinách
    - Volby v komunitách nebo družstvech – například volby předsedů družstevních bytových domů nebo zahrádkářských kolonií
    - Volby v zájmových skupinách – například hlasování o organizátorech nebo vedoucích v neformálních skupinách

- Volby podle typu hlasování
    - Přímé volby – voliči přímo rozhodují o zvolených zástupcích, například prezidentské volby
    - Nepřímé volby – voliči volí zástupce, kteří pak rozhodnou o volbě, například některé formy prezidentských voleb v minulosti

- Volby podle povahy účelu
    - Řádné volby – probíhají v plánovaném čase podle volebního kalendáře
    - Předčasné volby – konají se dříve, než bylo původně plánováno, například po rozpuštění parlamentu
    - Doplňovací volby – slouží k obsazení uvolněného mandátu, například při odstoupení poslance
    - Referenda – přímé hlasování občanů o konkrétní otázce; toto není standardní volba, ale často jsou k ní referenda přirovnávána

- Volby podle volebního systému
    - Většinový systém – kandidát s nejvyšším počtem hlasů vítězí, například většinový systém v Senátu ČR
    - Poměrný systém – mandáty se rozdělují podle procenta získaných hlasů, například volby do Poslanecké sněmovny
    - Smíšený systém – kombinace prvků obou předchozích systémů[9]

- Volby podle povahy mandátů

- Volby do veřejných orgánů – volby politiků zastupujících občany (parlament, prezident, zastupitelstva)
- Profesní volby – volby do orgánů profesních komor nebo organizací
- Vnitrostranické volby – volby do vedení politických stran nebo hnutí

1.5. Hlasování ve volební místnosti

Hlasování ve volební místnosti je tradiční formou voleb, při kterém voliči osobně přicházejí do předem určených volebních místností, aby zde odevzdali svůj hlas. Tento proces je přímý, anonymní a dohlíží na něj volební komise, která zajišťuje správnost a transparentnost voleb. Volič se identifikuje platným dokladem totožnosti, jako je např. občanský průkaz nebo cestovní pas. Poté obdrží hlasovací lístek a prázdnou úřední obálku. Hlasovací lístek si rovněž může vzít z domu, pokud mu sada s těmito hlasy byla doručena poštou. Volič následně vstupuje za plentu, aby mohl svůj hlasovací lístek upravit v soukromí a takto upravený hlas vloží do úřední obálky. Nakonec vhodí úřední obálku do volební urny, kterou spravuje volební komise. Po odevzdání hlasu volič opouští volební místnost, čímž je jeho hlas započítán.

1.5.1. Výhody, nevýhody a rizika

Protože se jedná o nejčastější formu hlasování, je neustále zdokonalována tak, aby nedostatků při této formě hlasování bylo co nejméně a pozitiv co nejvíce. Nespornou výhodou tohoto způsobu je jednoduchost. Ať už jde volit prvovolič nebo člověk v důchodovém věku, je téměř jisté, že bude vědět, jak postupovat. V případě technických nebo organizačních otázek je k dispozici volební komise, která může pomoci a která zároveň slouží jako asistence v průběhu hlasování. S tímto souvisí i transparentnost. Volební proces je veřejný a dohlíží na něj volební komise, která je autoritou a dodává tak důvěru a jistotu správnosti výsledků voleb. Díky tomu, že volič hlasuje vždy za plentou, se minimalizuje riziko ovlivnění jinou osobou a zvyšuje tak soukromí. Volič se proto nemusí obávat, že by nějakým způsobem byla narušena tajnost hlasování. Navíc je u každého fyzicky přítomného voliče ověřena jeho totožnost, což dále zvyšuje bezpečnost a snižuje potenciální riziko zneužití hlasovacího práva.

Byť by se mohlo zdát, že tato forma hlasování nemá žádné nevýhody nebo rizika, opak je pravdou. Dokonce tato negativa přímo souvisí s pozitivy. Dříve zmíněná volební komise se sice stará o správnost výsledků voleb, nicméně i tak může způsobit chyby. Může se

jednat o chyby způsobené nedbalostí, nezkušeností, ale i úmyslem v nějaké formě úplatku. V takovém případě skutečně existuje riziko, že někteří členové volební komise mohou ovlivnit výsledky voleb. Ovlivněna však nemusí být jen volební komise (resp. její členové), ale i samotní voliči. V tomto případě se však nátlak na voliče nebo jeho ovlivňování může odehrávat například těsně před vstupem do volební místnosti. Opatření proti tomuto sice existují, ale nemusí tomu vždy zabránit. Další nevýhodou je časově omezená dostupnost volebních místností. Tradičně jsou volební místnosti otevřeny pouze v určitých hodinách. Pro většinu voličů to může být dostatečné, avšak vždy existují voliči, kteří se nemohou dostavit právě z důvodu časové tísně. Fyzická přítomnost voliče však není problém jen u této kategorie voličů. Týká se to i těch voličů, kteří právě prochází nějakou nemocí nebo mají omezenou mobilitu. V neposlední řadě je nevýhodou také logistika. Do organizace ve volebních místnostech musí být zapojeno nemalé množství nejen personálu, ale i financí a také vybavení. V případě politických voleb se navíc musí jejich výsledky převážet odpovědným orgánům.

1.6. Korespondenční volba

Korespondenční volba je způsob hlasování, při kterém voliči odevzdávají svůj hlas prostřednictvím pošty. Tato metoda umožňuje účast ve volbách i těm, kteří nemohou hlasovat osobně, například kvůli pobytu v zahraničí, zdravotnímu stavu nebo jiným překážkám.

V České republice byla korespondenční volba dlouhodobě diskutována, zejména s ohledem na občany žijící v zahraničí, kteří museli dosud volit osobně na zastupitelských úřadech, což bylo často logisticky náročné. Zavedení korespondenční volby schválila Poslanecká sněmovna v červnu roku 2024 zákonem č. 88/2024 Sb., o správě voleb, a jeho novelou č. 268/2024 Sb. Následně novelu schválil Senát a podepsal prezident České republiky Petr Pavel. Korespondenční volba bude dostupná pouze pro volby do Poslanecké sněmovny, prezidentské volby a volby do Evropského parlamentu. Voliči budou muset předem požádat o zaslání hlasovacích lístků na adresu v zahraničí, vyplněné lístky pak zašlou zpět příslušným úřadům. Tento krok přibližuje Českou republiku běžným standardům v mnoha demokratických zemích a usnadňuje výkon volebního práva pro tisíce Čechů žijících v zahraničí.

V současné době většina evropských zemí tuto formu hlasování již umožňuje a v USA jde o velmi běžnou formu hlasování, zejména pak při prezidentských volbách.[10][11]

1.6.1. Princip fungování korespondenční volby

V některých zemích je nutné, aby se volič předem registroval pro korespondenční hlasování. Zaregistrovaný volič tak obdrží hlasovací lístek poštou na zadanou adresu. Dále obdrží obálku s hlasovacím lístkem, instrukcemi a často i zpáteční obálkou pro odeslání hlasu. Svůj vyplněný hlasovací lístek volič vloží do přiložené obálky a odešle poštou na příslušný volební úřad, kde je hlas započítán.[12]

1.6.2. Výhody, nevýhody a rizika korespondenční volby

Nespornou výhodou korespondenční volby proti klasické je pohodlí. Volič v tomto případě nutně nemusí navštívit volební místnost, a přesto mu bude hlas započítán. S tím úzce souvisí i flexibilita, kdy má volič více času na rozmyšlení, koho chce opravdu zvolit. Je to z toho důvodu, že nehlasuje přímo ve volební místnosti, a proto na něj není vyvíjen časový tlak. Korespondenční volbu mají dostupnou téměř všichni, a to především voliči ze zahraničí. Nemocní nebo voliči s omezenou mobilitou mohou tuto formu volby využít také. Celkově může korespondenční volba přispět ke zvýšení volební účasti, což je velmi směrodatný ukazatel. V tomto případě to tedy může některé voliče motivovat k účasti ve volbách, i když by za jiných okolností hlasovat nechtěli.

I když se tato forma hlasování může jevit jako dokonalá, není to úplně pravdou. Může zde hrozit například bezpečnostní riziko. Ať už půjde o zneužití hlasu, doručení poštou na nesprávnou adresu nebo riziko ztráty volební obálky, bez které je hlas neplatný. Někteří voliči z odlehlých oblastí mohou mít pocit nerovnosti přístupu nebo dokonce diskriminace, protože mohou mít například více omezený přístup k poštovním službám na rozdíl od voličů z méně odlehlých lokalit nebo měst. Pokud se větší množství voličů rozhodne využít právě korespondenční hlasování, může dojít také k logistickým problémům. Konkrétně mohou nastat potíže s celkovou organizací nebo distribucí a následně zpětným sběrem hlasů. Dále také hrozí nedostatek tajnosti hlasování. V důsledku toho, že hlasování často neprobíhá za plentou ve volební místnosti, ale v domácím prostředí, může být narušen základní princip voleb – princip tajnosti hlasování.

1.7. Elektronické hlasování

Systém elektronického hlasování (e-voting) je technologie, která umožňuje voličům odevzdávat své hlasy elektronicky, a to buď prostřednictvím fyzických zařízení, jako jsou elektronické hlasovací terminály, nebo prostřednictvím internetu. Takový systém se používá ke zvýšení efektivity, přesnosti a celkové rychlosti volebního procesu. Elektronické hlasování může výrazně zefektivnit volební proces, ale jeho úspěch závisí na spolehlivosti systému, transparentnosti a důvěře voličů.[13]

1.7.1. Typy systémů elektronického hlasování

Na trhu existuje několik typů systémů elektronického hlasování, mezi něž patří EVM, internetové hlasování a optické skenování.

EVM neboli Electronic Voting Machines, do češtiny přeloženo jako elektronické hlasovací přístroje, jsou speciální elektronická zařízení, která jsou používána přímo na místech, kde se volí. Může se například jednat o jistou podobu kiosku umožňujícího voličům zvolit svého kandidáta jednoduše buď stisknutím tlačítka nebo dotykem na dotykové obrazovce.

Internetové hlasování se jeví jako varianta s obrovským potenciálem. Umožňuje totiž voličům hlasovat odkudkoli, kde je připojení k internetu, prostřednictvím jednoduchého a srozumitelného webového rozhraní. Taková možnost je také zaměřena na zabezpečení. Obvykle je tato volba hlasování zabezpečena pomocí šifrování a dvoufázové autentizace.

Poslední možností je optické skenování. Jedná se o způsob hlasování, který může být podobný jako například ověření totožnosti u pasové kontroly na některých letištích. V tomto případě však voliči vyplní obyčejný papírový hlasovací lístek, který je poté naskenován optickým skenerem a elektronicky spočítán.[14]

1.7.2. Výhody, nevýhody a rizika

Tento způsob hlasování ve své podstatě eliminuje nedostatky klasického hlasování ve volebních místnostech. Má však jiné nevýhody. Mezi přednosti elektronického hlasování bezpochyby patří rychlost. Na rozdíl od klasického volení ve volebních místnostech totiž nedochází ke sčítání hlasů až po skončení voleb, ale průběžně. Výsledky hlasování tak lze získat okamžitě po ukončení hlasování. Při sčítání je taktéž kladen důraz na přesnost. Existuje

velmi malá šance, že by se systém při sčítání hlasů dopustil chyby, jako se to může stát v případě sčítání ve volebních místnostech, kde hlasy sčítají lidé. S tím také souvisí jisté úspory, a to časové i nákladové. Systém elektronického hlasování bude mít vždy rychleji sečtené výsledky, než když je počítá člověk. Stejně tak u elektronického hlasování takřka není potřeba žádný papír, ani žádné obálky. Dochází tak ke značné úspoře materiálu, který může najít využití jinde. Tento způsob hlasování také může usnadnit přístupnost k volbám i lidem s fyzickými nebo jinými omezeními, čímž se potenciálně může zvýšit volební účast jakožto klíčový parametr jakýchkoli voleb.

Dříve zmíněné nedostatky, případně potenciální rizika, mohou být výzvou pro zabezpečení uvedených systémů. V zásadě se s takovými riziky u tradičního hlasování ve volebních místnostech setkáme málokdy, což přináší do současného světa nové výzvy. Největší nevýhodou a zároveň rizikem je celková bezpečnost. Během voleb může docházet k různým typům kybernetických útoků, proti kterým musí být systém zabezpečený. Může také nastat situace, že bude probíhat manipulace s výsledky, pokud takový systém nebude mít požadované zabezpečení, aby se k hodnotám výsledků jen tak nedostal žádný uživatel. Vzhledem k tomu, že se obyvatelstvo dá nejen v České republice obecně považovat více za konzervativní než progresivní, zde může panovat nedůvěra vůči těmto systémům. Je to dáno tím, že veřejnost zkrátka nemusí důvěřovat systémům, u kterých nerozumí jejich fungování. Skepse ale může panovat i kvůli negativním zkušenostem s jinými druhy elektronických systémů nežli s těmi volebními. Často totiž dochází k výpadkům systémů zejména na začátku při jeho spouštění, což je zapříčiněno nadměrnou zátěží, na kterou systém není stavěný. Riziko výpadku nebo dokonce selhání systému během voleb hrozí právě u tohoto způsobu hlasování.

1.8. Požadavky na bezpečný systém

Pokud se rozhodneme zprovoznit systém elektronického hlasování, musíme si stanovit důležité požadavky, které nám zajistí co největší bezpečnost požadovaného systému. Je nutné zajistit především šifrování přenesených a ukládaných dat. Je důležité, aby byl použit takový šifrovací algoritmus, který zajistí jak vysokou bezpečnost, tak vysokou rychlost ověřování. Na světě existuje velké množství šifrovacích algoritmů, a proto je důležité vybrat na základě požadavků bezpečnosti a rychlosti ten nejlepší z nich. Neměli bychom proto používat takové šifrovací algoritmy, jejichž ochranu je možné prolomit v řádu hodin, dnů nebo dokonce

v reálném čase pomocí běžně dostupných hardwarových prostředků. Použitím tohoto šifrovacího algoritmu se vystavujeme riziku prolomení zabezpečení a úspěšného kybernetického útoku ze strany útočníků. Stejně tak bychom se měli vyhnout šifrovacím algoritmům, které sice využívají například 4096bitový klíč, ale kvůli své nízké rychlosti a vysoké výpočetní náročnosti jsou nevhodné a neefektivní pro nasazení v reálném použití. U šifrování dat je tedy velmi důležité brát ohled nejen na zabezpečení, ale i na výkon a celkovou efektivitu. Dále je důležité zajistit odolnost vůči hackerským útokům. Jedním z klíčových opatření pro zabezpečení systému proti hackerům je právě výše zmíněné šifrování. Měla by také být řádně zabezpečena databáze uživatelů, například kvůli nechtěnému úniku dat. Samozřejmostí je poté zabezpečení počítadla, s čímž souvisí zajištění anonymity, tedy zajištění, že hlasovací proces zůstane tajný. Nesmí proto docházet k tomu, aby si voliči mohli navzájem zpětně zjistit, jakého kandidáta kdo volil. Současně musí existovat nějaký správce celého systému, jenž bude mít možnost ověřit a přezkoumat výsledky voleb, pokud o to bude požádán nebo pokud se vyskytnou stížnosti ohledně podezřelého výsledku.

1.9. Volební aplikace na trhu

Při výběru takové aplikace vždy záleží na konkrétních preferencích uživatele a na tom, co od ní očekává za funkce a informace. Na základě těchto požadavků by měl být uživatel schopen si najít přesně takovou aplikaci, která mu bude nejvíce vyhovovat.

Pokud se zaměříme na český trh s aplikacemi tohoto typu, zjistíme, že každá z nich přistupuje k volbám trochu odlišným způsobem. Tyto aplikace pak pomáhají voličům při svém rozhodování a mohou poskytovat i aktuální informace o volbách. Zde je několik příkladů řešení na českém trhu:

Right2Vote

- On-line platforma pro ověřená hlasování, která umožňuje uživatelům vytvářet vlastní ankety a hlasování. Největší výhodou je snadná dostupnost a uživatelská přívětivost, což ji činí vhodnou pro menší organizace a neformální hlasování. Nevýhodou je ale omezená dokumentace týkající se bezpečnostních mechanismů, autentizace a anonymity hlasujících. Z tohoto důvodu se méně hodí pro případy, kde je požadována vysoká míra důvěryhodnosti a zabezpečení dat.[15]

Arbitron

- On-line aplikace vhodná pro firmy, školy, univerzity a veřejnou správu. Nabízí různé způsoby hlasování. Podporuje anonymní i jmenné hlasování, jednokolové i vícekolové volby a je kompatibilní se všemi uživatelskými zařízeními, jako jsou mobilní telefony, tablety i počítače. Díky pravidelným aktualizacím a nezávislým bezpečnostním auditům zajišťuje aplikace také vysokou úroveň zabezpečení. Nevýhodou naopak může být složitější správa ve srovnání s jinými aplikacemi.[16]

Podpisovna

- Aplikace, která byla navržena primárně pro elektronickou komunikaci s úřady. Kromě možnosti podepisovat důležité dokumenty, jako jsou například daňová přiznání, formou elektronického podpisu, nabízí Podpisovna rovněž možnost elektronických voleb. Jako způsob autentizace využívá Identitu občana, Bank ID nebo MojeID. Dokáže také vytvářet tajná hlasování zajišťující anonymitu voleb. Využití aplikace je ale úzce vázáno na prostředí e-governmentu, což toto využití značně omezuje.[17]

E-volby v IS JABOK

- Aplikace, která je součástí Informačního systému JABOK Masarykovy Univerzity v Brně, umožňuje vyhlašovat volby, hlasovat a zveřejňovat výsledky uvnitř dané instituce, což nachází využití pro vzdálené hlasování v rámci pracovních komisí. Nevýhodou je právě nemožnost přenést ji do jiného prostředí, protože jde o součást informačního systému a nejedná se tedy o univerzální řešení.[18]

Na celosvětovém trhu také existuje několik volebních aplikací, které mají velké spektrum využití, a to od monitorování volebního procesu až po poskytování informací voličům. Zde je ukázka příkladů aplikací z globálního trhu:

BallotReady

- Aplikace, která poskytuje podrobné informace o kandidátech a referendech v USA. Umožňuje také voličům prozkoumat jejich hlasovací lístek před volbami a učinit informovaná rozhodnutí. Není však určena pro ostatní státy světa, což ji činí omezenou v kontextu geografického zaměření.

ElectionGuard

- Software původem od společnosti Microsoft Corporation, který umožňuje bezpečné a ověřitelné elektronické hlasování. Výhodou je, že se jedná o open-source software. Je však primárně navržený tak, aby zvýšil důvěru veřejnosti v elektronický volební proces. Nevýhodou je ale technická náročnost implementace. Navíc se nejedná o klasickou aplikaci, ale o nástroj pro integraci do jiných systémů.

Democracy Live

- Platforma poskytující elektronické hlasovací řešení pro vzdálené voliče, včetně vojenských a zahraničních voličů. Nabízí také bezpečný přístup k hlasovacím lístkům on-line. Přesto se však objevují obavy kvůli zajištění anonymity a možných zranitelnostech v mobilním prostředí.

Helios Voting

- Open-source webový elektronický volební systém, kde uživatelé mohou volby vytvářet a účastnit se jich on-line. Aplikace používá homomorfní šifrování, aby zajistila požadavek tajnosti hlasování. Byla rovněž použita v různých institucích, včetně univerzit a profesních organizací. Není ale vhodná pro plošné politické volby, a to zejména kvůli absenci silné autentizace a složitosti správy.

Dominion Voting Systems

- Společnost původem z Kanady, která poskytuje elektronické volební systémy a software, včetně hlasovacích zařízení a skenerů pro sčítání hlasů. Technologie této společnosti byly využity při různých volbách v Kanadě a Spojených státech amerických. Nejznámější případ použití této technologie byl při konání prezidentských voleb v USA v roce 2020. Po těchto volbách se ale na systém strhla mediální pozornost kvůli nepodloženým obviněním z manipulace s výsledky.[19]

Voatz

- Mobilní aplikace, jež umožňuje bezpečné elektronické hlasování prostřednictvím mobilních telefonů. Byla použita hned v několika pilotních projektech v USA pro vzdálené hlasování. Získala uznání za inovativní přístup, ale zároveň čelila kritice kvůli netransparentnosti a obavám ze zranitelností, které později odhalily bezpečnostní audity. [20]

2. ELEKTRONICKÝ VOLEBNÍ SYSTÉM

2.1. Návrh řešení

Musíme si nejprve uvědomit, co od daného volebního systému očekáváme a jak by měl fungovat. Grafické prostředí musí být přehledné a srozumitelné, a to především pro uživatele, kteří se s informačními technologiemi setkávají zřídkakdy. Design u aplikace tohoto typu však není tou nejvyšší prioritou, takže různé animační prvky mohou vypadat líbivě, ale pokud je aplikace například nestabilní nebo není správně funkční, jsou takovéto designové prvky nepodstatné. Na stranu druhou je ale vhodné design alespoň v malé části přiblížit době, v níž se daný systém vyvíjí, a to i z důvodu uživatelského komfortu. Aplikace by také měla obsahovat minimálně 3 uživatelské role – volič, členové volební komise a předseda volební komise. Volič má právo hlasovat ve volbách jemu určených. Členové volební komise mají přístup k volbám, ke kterým je přiřadil předseda, nemají však právo zakládat vlastní volby. Společně s předsedou mají po ukončení voleb přístup k výsledkům. Předseda volební komise by měl být jakýmsi „správcem“ celé aplikace. Má právo volby zakládat, odebírat, přidávat členy volební komise. Zkrátka provádět akce spojené s elektronickým hlasováním. V případě takové volební aplikace tudíž není nutné mít ještě jednu zvláštní roli administrátora, jelikož ten by měl především spravovat implementační část aplikace a přidělovat vstupní hesla předsedům volebních komisí. Do průběhu jakýchkoli voleb nemá právo zasahovat. Je také nutné, aby splňoval všechny podmínky v souladu s platnými zákony a předpisy, jako je například GDPR.

Po stránce návrhu řešení si musíme vytyčit funkční a nefunkční požadavky na systém elektronického hlasování. Tyto funkční a nefunkční požadavky později aplikujeme do praktického použití, což v našem případě znamená implementační část tohoto systému. Nastavení požadavků musí odpovídat reálným, nikoli utopickým představám. Nelze tedy v žádném případě očekávat, že bude možné zajistit stoprocentní bezpečnost systému. Realitou totiž je, že žádný elektronický systém na světě není zabezpečený tak, že by byl stoprocentně imunní vůči prolomení ochrany. U těch nejlépe zabezpečených systémů se dá prolomení zabezpečení odhadovat na desítky, stovky, místy i tisíce let – nikdy však nelze zajistit absolutní bezpečnost. Připočítejme navíc fakt, že každým rokem se zvyšuje výpočetní výkon počítačových komponent, což dále snižuje dobu potřebnou k prolomení ochrany. Nejprve si ale ujasníme, jaký je rozdíl právě mezi funkčními a nefunkčními požadavky.

Funkční požadavky jsou takové, které definují funkce jakéhokoli požadovaného systému. Jinými slovy funkční požadavky nám říkají, co takový systém musí umět a dělat, respektive jaké má mít funkce. Popisují také konkrétní vstupy, výstupy a procesy, které musí systém podporovat.

Nefunkční požadavky už však počítají s definováním funkčních požadavků a specifikují, jak dobře má systém fungovat. Nesoustředí se tedy na funkce jako takové, ale především na jejich kvalitu, výkonnost a spolehlivost.[21]

2.1.1. Funkční požadavky

Začněme nejprve stanovením funkčních požadavků, jelikož podle nich můžeme následně definovat požadavky nefunkční.

Autentizace

Prvním požadavkem je autentizace voliče. Každý občan, který bude chtít volit elektronicky, musí být jednoznačně identifikován. To z důvodu, aby bylo zajištěno, že ve volbách hlasují pouze osoby, které mají oprávnění volit. Autentizace tedy zjednodušeně znamená ověření identity, v tomto případě konkrétního voliče. Toto ověření lze provést několika způsoby. Například vypsáním čísla občanského průkazu, kde systém bude na základě tohoto identifikátoru schopný ověřit, zda je občanský průkaz platný. Dnes můžeme mít občanský průkaz rovněž v elektronické podobě, což přináší další způsob ověření identity. Dále můžeme ověřovat přes bankovní identitu nebo jiné státem uznané systémy ověřující identitu voliče. Z hlediska bezpečnosti je však více přijatelnější variantou vícefaktorové ověření známé také pod zkratkou MFA. V takovém případě se nejčastěji setkáme s dvoufaktorovým ověřením. Tento způsob zahrnuje nejen ověření heslem nebo jednoznačným identifikátorem (například číslem občanského průkazu), ale i ověření kódem z SMS zprávy nebo pomocí biometrie (například otiskem prstu). Můžeme to označit jako další vrstvu zabezpečení naší identity. Celkově vzato je cílem autentizace zabránit neoprávněným osobám v přístupu k hlasování.

Autorizace

S autentizací voliče velmi úzce souvisí autorizace voliče, která na autentizaci de facto navazuje. Autorizace sama o sobě znamená, že se ověřují oprávnění daného uživatele. V tomto případě tedy musíme ověřit, jestli má daný volič právo hlasovat v nějakých konkrétních volbách. Autorizací se tedy rozumí například ověření, zda volič již dosáhl své

plnoletosti. Podle občanského průkazu sice bylo v případě autentizace možné ověřit totožnost daného voliče, ale až autorizace nám prozradí rozsah práv voliče. Pokud je tedy splněna podmínka autentizace, musí být splněna i podmínka autorizace, aby bylo možné přejít k samotnému hlasování. Může tedy nastat případ, že volič má platný občanský průkaz, ale pokud například nedosáhl věku 18 let, nemá právo volit. Tento princip platí i obráceně. Je-li volič plnoletý, ale nedisponuje platným průkazem totožnosti, rovněž nemá právo volit. Dosažení plnoletosti však není jediným kritériem autorizace. Prověřuje se také skutečnost, zda je volič z nějakého důvodu omezen na svéprávnosti nebo jí úplně zbaven. Pakliže je skutečně volič tímto způsobem omezen, mohlo mu být s největší pravděpodobností právo volit odebráno. V některých případech se také kontroluje volební okrsek voliče. Tato kontrola slouží k zamezení volit voličům původem ze svého okrsku v jiných okrscích. Můžeme to nazvat jako jistou formu prevence před ovlivněním voleb v určitých částech dané země. Toto opatření však není příliš směrodatné v případě elektronického hlasování, na rozdíl od voleb ve volebních místnostech. Je však nutné ověřovat, jestli volič již odhlasoval. Pokud volič už jednou odevzdal svůj hlas, není možné jej odevzdat znovu. Případný systém proto musí disponovat ochranou před dvojitým hlasováním. Stejně jako není možné hlasovat vícekrát ve volebních místnostech, nesmí to být možné ani elektronickou volbou. V neposlední řadě musí být volič součástí dané skupiny voličů pro konkrétní volby. Bude-li se například jednat o volby do akademického senátu fakulty X, pak nesmí nastat situace, aby student fakulty Y měl k těmto volbám přístup. Takový student může mít po ukončení voleb právo vidět jejich konečné výsledky, ale nesmí se žádným způsobem podílet na samotném hlasování. Kritérií může existovat více a každý, kdo organizuje jakékoli volby, musí určit specifická kritéria pro možnost hlasování a voliči je následně musí splňovat.

Zajištění anonymity

Aby mohlo být elektronické hlasování považováno za bezpečné a důvěryhodné, musí být zajištěna anonymita voleb. Jinými slovy musí být zajištěno, že v momentě, kdy volič odešle svůj platný hlas, volební systém zajistí, že tento konkrétní hlas konkrétního voliče nebude žádným způsobem zpětně propojen s jeho identitou. Nesmí tedy být možné zjistit, kdo koho volil. Opět se tedy jedná o jistou formu prevence před zmanipulováním výsledků voleb. Tento požadavek musí být splněn jakožto jeden z klíčových principů zachování tajnosti hlasování. Anonymitu voleb lze zajistit několika způsoby. Jedním z příkladů je použití některé z kryptografických metod, jako je například homomorfní šifrování nebo použití slepého podpisu.

Homomorfní šifrování je způsob šifrování, který provádí matematické výpočty nad zašifrovanými daty tak, že není nutné je dešifrovat. Znamená to tedy, že pokud máme dvě šifrované hodnoty, je možné nad nimi provádět například jednoduché aritmetické operace (tj. sčítání, odčítání, násobení, dělení). A to tak, aby výsledek po dešifrování odpovídal zvolené operaci provedené nad původními hodnotami. Kromě elektronického hlasování může tento způsob šifrování najít využití i při zpracování šifrovaných dat v cloudovém úložišti, aniž by byl odhalen jejich obsah.

Slepý podpis je technika z oboru kryptografie, která umožňuje podepisovat zprávy, aniž by signatář (autorita nebo volební systém samotný) byl schopen vidět jejich obsah. Zajišťuje to tedy anonymní a bezpečnou autorizaci. Nejprve volič zprávu zaslepí pomocí funkce pro skrytí zprávy před signatářem, poté zprávu signatář podepíše svým soukromým klíčem, aniž by viděl skutečný obsah zprávy, a nakonec volič podpis odmaskuje a získá tak od autority podepsanou zprávu, která je stále platná a ověřitelná. V elektronickém hlasování tento způsob zabezpečení nachází využití při ověřování hlasu bez odhalení soukromí voliče.

Dalším z příkladů je oddělení autentizační části od části zpracovávající jednotlivé hlasy. Tímto způsobem se ztratí jakákoli vazba tabulek s uživateli a kandidáty. Efektivní by bylo například pouze zaznamenat, zda daný volič již odvolil či nikoli. Nikde se však nebude zaznamenávat údaj o konkrétním kandidátovi. Dále je také možné zajistit anonymitu použitím anonymního elektronického tokenu, který každý volič obdrží po ověření všech podmínek.

Podání hlasu

Musíme rovněž zajistit, aby aplikace byla přehledná a aby se v ní zorientoval každý, kdo bude chtít volit. Ne nadarmo se říká, že v jednoduchosti je síla. Pro každého voliče musí být zřejmé, kam má kliknout, aby odvolil, a jaké jsou nutné kroky pro to, aby vůbec volit mohl. Toto musí být jednoduše a srozumitelně popsané, aby uvedeným krokům rozuměl i člověk, který se nesetkává každý den s elektronickými zařízeními. Prostředí aplikace se taktéž musí držet pravidel volebního systému. Volič tak musí mít výběr jedné nebo více možností (například hlasování kroužkováním) na hlasovacím lístku. Musí ale mít také možnost odevzdat prázdný hlasovací lístek. V takovém případě se však volič vzdává možnosti nového hlasování. Před odesláním hlasu je nutné, aby volič potvrdil, že chce skutečně odvolit. Toto potvrzení hlasu (například pomocí dialogového okna) má na voliče také jistý psychologický efekt, kdy si každý položí otázku, zda si je svojí volbou skutečně jistý.

Bezpečnost – šifrování a ukládání hlasů

V kapitole o požadavcích na bezpečný systém elektronického hlasování jsme si uvedli, jaké požadavky musí obsahovat. Bezpečnost dat v tomto případě opravdu nesmíme podceňovat, jelikož k jejich únikům dochází prakticky dnes a denně. V případě úniku dat se nejčastěji jedná o únik dat z databáze z důvodu, že nebyla řádně zabezpečena. Proto potřebujeme zajistit, aby data z hlasovacích lístků byla bezpečně uložena a chráněna před neoprávněnou manipulací. Tím se myslí nejen potenciální zásah do výsledků ze strany hackera na internetu, ale i ze strany personálu volební komise. Nesmí tedy nastat situace, kdy se členové volební komise domluví s předsedou volební komise a případně i administrátorem celého volebního systému. Respektive tato absolutně neetická situace nastat může, ale systém musí být proti ní odolný. Případné jednání všech tří aktérů (členové volební komise, její předseda a administrátor elektronického volebního systému) je nejen neetické, ale dokonce i trestné a netransparentní. V neposlední řadě takové počínání podkopává důvěru široké veřejnosti v tyto systémy. Aby se těmto nežádoucím situacím předešlo, je nutné použít silný šifrovací algoritmus pro ochranu všech hlasovacích dat. Také je potřeba, aby byla zajištěna integrita dat pomocí digitálních podpisů nebo technologie blockchain. Digitální podpis funguje na principu soukromého a veřejného klíče, kdy odesílatel data podepíše soukromým klíčem a příjemce ověří podpis pomocí veřejného klíče. Pokud byla data jakkoli změněna, podpis se automaticky stává neplatným. Blockchain je naproti tomu neměnná databáze, která v sobě ukládá data do spojených bloků pomocí kryptografie. Každý blok dat obsahuje samotná data, hash předchozího bloku a časové razítko. K narušení spojení s následujícími bloky stačí změna dat v jakémkoli z bloků. Každá změna dat v bloku zároveň změní i hash konkrétního datového bloku, díky čemuž se přeruší spojení bloků. Historii dat není možné zpětně upravit, proto se jedná o neměnnou databázi. V případě, že dojde k nějakému výpadku v průběhu voleb, ať už se jedná o výpadek elektrické energie nebo výpadek na počítačové síti, musí být data bezpečně uložena na redundantním úložišti s ochranou proti různým výpadkům.

Sčítání hlasů

V momentě, kdy skončí termín elektronických voleb, přichází na řadu sčítání hlasů. Elektronické hlasování má proti tradičnímu hlasování výhodu v tom, že je možné hlasy sčítat průběžně. Není tedy potřeba čekat na termín konce voleb a poté ručně přepočítávat hlasy. Tento proces zabere velké množství času v řádu jednotek hodin, zatímco u elektronického hlasování jsou výsledky dostupné takřka ihned. Je to dané díky dříve zmíněnému průběžnému a automatickému sčítání elektronických hlasů, které navíc musí systém zajistit, aby bylo

rychlé a přesné. Za účelem sčítání hlasů můžeme použít různé kryptografické metody pro ověřitelné sčítání. V případě potřeby je také vhodné mít v systému možnost manuálního (tedy tradičního) sčítání hlasů. To můžeme použít v případě, že budou výsledky hlasování vypadat podezřele nebo o tuto možnost požádá konkrétní subjekt, který se zúčastnil daného hlasování. Za těchto okolností je však nutné, aby se manuálního sčítání hlasů zúčastnilo více aktérů. Obecně však sčítání hlasů musí být transparentní a ověřitelné nezávislými subjekty. Jen tak se zvýší důvěryhodnost systémů elektronického hlasování.

Možnost revize a auditu

Kapitolou samotnou je možnost revize výsledků nezávislými subjekty. Těmito subjekty se myslí například volební komise nebo mezinárodní organizace, které by měly mít možnost ověřit správnost výsledků hlasování. Pro takový systém elektronického hlasování je důležité, aby měl možnost zaznamenávání všech důležitých akcí, které byly v průběhu voleb provedeny. Toto tzv. logování musí probíhat za předpokladu, že nebude ohrožena anonymita voličů. Systém také musí být před volbami řádně otestován, a to včetně penetračních testů bezpečnosti. Pokud bychom systém před samotným hlasováním netestovali, může se stát, že se v průběhu voleb, především v době největšího náporu uživatelů, objeví velmi závažné komplikace. Jak již bylo zmíněno, tato možnost u veřejnosti posílí důvěru v tento způsob hlasování.

Nemožnost vícenásobného hlasování

V neposlední řadě musí být systém odolný proti hlasování vícekrát za sebou. Stejně jako je tomu i u tradičního způsobu hlasování, ani zde elektronický systém voleb nesmí dovolit vícenásobné hlasování. Nesmí tedy být možné, aby mohl jeden volič odevzdat více hlasů formou elektronického hlasu. Každý volič tedy smí hlasovat pouze jednou a jakmile tento konkrétní volič odevzdá svůj hlas, systém tuto skutečnost musí zaznamenat. Odlišná je však situace, pokud bude systém podporovat změnu stávajícího hlasu. Tato funkce může být implementována, avšak je nutné, aby v případě úpravy nepřidávala hlas více kandidátům. Pokud tedy bude možné změnit hlas, musí nový hlas přepsat ten původní. Jinými slovy, jestli se volič rozhodne, že například místo kandidáta 1 bude chtít volit kandidáta 2, musí být hlas kandidátovi 1 odebrán a kandidátovi 2 přidán. Zajistit odolnost vícenásobného hlasování lze také použitím jednorázového hlasovacího tokenu, případně jednorázového elektronického podpisu, který po odvolení nebude možné znovu použít.

2.1.2. Nefunkční požadavky

V tuto chvíli již máme definované funkční požadavky, takže je vhodné si definovat požadavky nefunkční. Ty se zaměřují na to, jak dobře systém funguje. V některých aspektech jsme nefunkční požadavky zmínili i v těch funkčních, ale to pouze z důvodu, že spolu velmi úzce souvisí.

Bezpečnost – ochrana před kyberútoky

O bezpečnosti zde již byla řeč několikrát. Tuto oblast je nutné neustále připomínat, protože právě bezpečnost celého systému elektronických voleb je nejpodstatnějším aspektem celého systému. Bezpečnost je v tomto případě příliš obecný termín, a proto musíme přesněji definovat, co se onou bezpečností systému myslí. Především je to ochrana proti různým kybernetickým útokům. Může se jednat například o DDoS útoky nebo phishingové útoky. Uvědomme si, že takový systém bude fungovat přes internet a že právě k této největší počítačové síti světa má přístup přes pět miliard lidí po celém světě. Za této situace je vysoce pravděpodobné, že se v některých částech světa najdou skupiny lidí, jejichž cílem je provést co možná největší množství kybernetických útoků. Pokud bychom chtěli podrobněji rozebrat téma hackingu a kybernetických útoků, zjistíme, že také existuje činnost, která se nazývá „etický hacking“. Stručně řečeno se jedná o typ hackingu, který má za cíl upozornit vydavatele kteréhokoli softwaru, že v něm existují potenciální chyby. Naproti tomu „neetický hacking“ je činnost, při které jeden nebo více hackerů úmyslně napadá například servery, na kterých běží konkrétní služby. Může se tedy jednat například o HTTP, FTP nebo databázové servery. A právě proti těmto hackerům a případně jiným kybernetickým útokům je nutné takový systém ochránit. V systému musí také existovat nějaký způsob šifrování dat. Je tedy potřeba zajistit, aby se všechny uložené a přenášené informace zašifrovaly pomocí silných, ale zároveň rychlých, kryptografických algoritmů, kterými jsou například AES-256 nebo RSA. Tyto informace mohou zahrnovat například podrobnosti o hlasech nebo přihlašovací údaje, jako jsou uživatelské jméno a heslo. S tím souvisí i autentizace a autorizace voliče. To jsou témata, která byla vysvětlena v sekci funkčních požadavků. Pro zajištění co nejvyšší bezpečnosti je v systému vhodné využít vícefaktorovou autentizaci, konkrétně například dvoufaktorovou. To voličům zajistí, že jejich přihlašovací údaje nebudou jednoduše čitelné a zjistitelné. Bezpečnost celého systému je důležitá nejen zvenku, ale i zevnitř. To znamená, že je rovněž důležité regulovat možnosti administrátora. Na první pohled se to může zdát jako paradox vzhledem k tomu, že administrátor je správcem celého systému, a tudíž má možnost jednoduše zasahovat do funkčnosti celého systému. Z hlediska bezpečnosti však toto nemusí

být vhodné řešení. Administrátor skutečně může měnit některé parametry a nastavení elektronického volebního systému, avšak i on musí mít k určitým akcím omezený přístup. Opět by tak mohla nastat situace, kdy se například předseda volební komise dohodne s administrátorem systému (protože má vzhledem k systému nejvyšší oprávnění) na zfalšování volebních výsledků. Omezení určitých oprávnění administrátora je tedy rozhodně na místě. Cílem zajištění bezpečnosti systému je zabezpečit určitou integritu, důvěryhodnost a dostupnost celého volebního procesu.

Dostupnost

Dostupnost samotná je také důležitým bodem. Volební systém musí totiž být po celou dobu právě probíhajících voleb dostupný každému voliči a nesmí docházet k jeho výpadkům, jako tomu často bývá při přístupu velkého množství zařízení najednou. To můžeme zajistit například rozdělením celé volební aplikace, aby běžela na více serverech. Pokud tedy bude zjištěna vysoká zátěž na jednom ze serverů, mohou se požadavky přesunout na jiný server, který je zatížený méně požadavky, aniž by to uživatel zaregistroval. Tento model používá například sociální síť Facebook a nazývá se „load balancing“ neboli rovnoměrné rozložení zátěže. Pakliže nastane situace, kdy volební systém postihne výpadek, musí existovat nějaký záložní systém se stejnými nebo podobnými (tj. omezenými) funkcemi. Pokud ale systém takovýmto záložním systémem nedisponuje, musí být alespoň zajištěn rychlý návrat originálního systému do provozu – neboli jeho obnovení. V každém případě je ale nutné zajistit co nejmenší pravděpodobnost výpadků, a tedy nepřerušený průběh voleb.

Rychlost systému

Aby byl elektronický volební systém dostupný po co nejdelší dobu, je důležité, aby příchozí požadavky rychle zpracovával pomocí rychlých a optimalizovaných algoritmů pro autentizaci voliče a podání jeho hlasu. Budeme se tedy věnovat rychlosti. Je nutné, aby systém disponoval takovými hardwarovými a softwarovými prostředky, které zajistí jeho schopnost dostatečně rychle zpracovat příchozí požadavek na autentizaci voliče. Tento proces musí proběhnout bez dlouhého čekání a s co největší efektivitou. V momentě, kdy volič úspěšně projde autentizací, je na řadě proces odevzdání hlasu. Tento musí být okamžitý a není přípustné, aby docházelo k prodlevám, případně nepřesnému přiřazení hlasu kandidátovi. Jakmile nastane moment, kdy skončí celý volební proces, přichází na řadu zveřejnění výsledků. Jak již bylo zmíněno dříve, na rozdíl od tradičního hlasování je možné získat výsledky voleb ihned, jelikož se hlasy průběžně sčítají. Delší dobu může trvat například generování různých druhů grafů na základě finálních výsledků, nicméně nejedná se o proces,

který by měl řádově zabrat hodiny. Pro splnění požadavku rychlosti je tedy klíčové vhodně dimenzovat softwarové (například databáze a použité algoritmy) a hardwarové (například serverové komponenty, zejména úložiště) prostředky.

Spolehlivost

Rychlost volebního systému jako celku je tedy bezpochyby velice důležitý požadavek, ale nesmí se obejít bez spolehlivosti. Pokud je systém rychlý, ale zároveň provádí akce, které můžeme označit za chybné, není připravený k použití v reálném provozu. Musí tedy být zajištěno, aby volební systém neselhal a minimalizoval riziko vzniku potenciálních chyb. Spolehlivost systému můžeme ověřit testováním, které nám odpoví na otázku, do jaké míry je testovaný systém odolný proti chybám. Takový test může například zahrnovat scénář, kdy dojde k výpadku na síti během hlasovacího procesu a budeme tedy schopni pozorovat, jak se systém v dané situaci chová. Pokud se systém v tomto testu osvědčí jako použitelný, můžeme pokračovat s dalšími testy. Může však nastat situace, že v případě závažnější chyby se nebude systém schopný sám zotavit. Je ale důležité, aby nebylo nutné při každé sebemenší chybě manuálně do systému zasahovat, ale aby systém měl schopnost se automaticky po takové chybě zotavit. Stejně tak je důležité, aby byl systém nasazený v reálném provozu dlouhodobě udržitelný. Tedy aby nebylo nutné v něm často provádět manuální zásahy a opravy. Systém neustále vyžadující jakékoli opravy a pečlivou údržbu lze vnímat spíše jako problémový systém než užitečný. Podepisuje se na tom samozřejmě i důvěra v konkrétní systém. Celková spolehlivost elektronického volebního systému je tedy jedním z jeho základních stavebních kamenů vedoucích k tomu, aby byl veřejností považován za důvěryhodný.

Jednoduchost a uživatelská přívětivost

Aby bylo možné zpřístupnit systém široké veřejnosti, je nutné zajistit co největší uživatelskou přívětivost prostředí tohoto systému. Jinými slovy, aby se v prostředí systému zorientovali i lidé, kteří se s moderními technologiemi často nesetkávají nebo jsou méně technicky zdatní. Pro takové prostředí volebního systému je tedy potřeba zajistit co možná největší jednoduchost a intuitivnost uživatelského rozhraní tohoto systému. Ne nadarmo platí, že v jednoduchosti je síla. Proto by v prostředí systému neměly být žádné složité akce, kterým voliči neporozumí. Pokud se přesto najde jakákoli složitější funkce, měla by v sobě obsahovat rovněž přiloženou nápovědu, případně jednoduchou a srozumitelnou dokumentaci. V případě výskytu jakýchkoli problémů je vhodné mít v prostředí systému rovněž podporu. Podporou se však nemyslí jen ta pro řešení vyskytnutých problémů, ale také například podpora pro voliče se zdravotním postižením. Taková podpora by měla zahrnovat například možnost zvýšení

velikosti textu nebo hlasovou asistenci. Jednoduchost uživatelského rozhraní elektronického volebního systému je tedy důležitá především pro minimalizaci výskytu chyb způsobených například nepochopením určité funkce systému.

Soulad s platnými zákony

Pro systém je dále také důležité, aby dodržoval pevné definice volebních zákonů a regulatorních požadavků v zemi, kde je volební systém používán. Musí tak být zajištěna zejména anonymita celého hlasovacího procesu a ochrana všech osobních údajů formou šifrování. Musí rovněž být zajištěn soulad volebního systému s podmínkami GDPR a dalšími regulacemi o ochraně dat. Ověření, zda systém splňuje všechny zákony, regulace a normy nutné pro provoz, musí provést nezávislé orgány kontrolující tyto požadavky. Na základě kontroly může takový orgán udělit konkrétnímu systému certifikaci o splnění všech potřebných požadavků pro provoz. Tento proces je nutný z důvodů uznání výsledků voleb, které proběhly prostřednictvím tohoto systému.

Odolnost a zotavení ze selhání

Během procesu voleb je rovněž důležité, aby nedocházelo k výpadkům, což bylo zmíněno v předchozích odstavcích, přesněji pak v sekci zaměřené na rychlost elektronického volebního systému. Během volebního procesu je téměř jisté, že se vždy objeví nějaké více či méně závažné chyby. Důležitější však je, aby se systém buď dokázal z těchto chyb zotavit, nebo pokud zotavení nebude schopen, aby mohl být co nejrychleji obnoven bez ztráty jakýchkoli dat. Je tedy důležité, aby byla všechna data pravidelně zálohována. Pokud tento požadavek nebude splněn, hrozí ztráta dat a v případě fatálního selhání dokonce i zdlouhavá obnova systému. V případě zálohování je také důležité použít takový typ úložiště, které nebude závislé pouze na jednom záznamovém médiu, ale aby byla zajištěna redundance dat v situaci, kdy jedno záznamové médium selže. Záznamovým médiem se myslí například magnetická páska, pevný disk typu HDD nebo SSD. Při výběru záznamového média vždy záleží na konkrétních požadavcích na systém. Pokud se jedná o více rozsáhlý volební systém, je vhodné jej rozdělit na několika běžících serverech oddělených od sebe. Může nastat situace, kdy jeden ze serverů selže takovým způsobem, že jej není možné delší dobu provozovat. V tomto případě může další server převzít úlohy od serveru, který právě postihl výpadek. Cílem je tedy zajistit, aby v případě komplikací a různých výpadků bylo možné volební systém udržet v provozu.

Kompatibilita s různými druhy zařízení

Pokud již máme nastavené všechny potřebné parametry pro průběh voleb, je nutné voličům zajistit, aby mohli volit z téměř jakéhokoli dostupného elektronického zařízení. Předpokládejme, že takovými nejčastějšími a nejdostupnějšími zařízeními jsou chytré mobilní telefony, přenosné počítače, stolní počítače a tablety. Nepředpokládáme, že by voliči používali k elektronickému hlasování chytré hodinky, případně náramky. Na podobná zařízení zkrátka není možné tento systém korektně implementovat. U výše zmíněných elektronických zařízení musíme však zajistit ještě další požadavky na kompatibilitu. Jedním z nejdůležitějších požadavků je velikost obrazovky zařízení. Obrazovka disponuje u každého zařízení jinou velikostí a jiným rozlišením. Proto je nutné uživatelské rozhraní volebního systému přizpůsobit velikostem obrazovky různých zařízení. Rozhraní musí být responzivní. Každé zařízení má v sobě nainstalované různé operační systémy. Nesmí proto vznikat rozdíly mezi uživateli s operačními systémy Windows, MacOS, Android, iOS a linuxových distribucí (například Ubuntu nebo Debian). Takové rozdíly se dnes objevují spíše sporadicky, ale stále na některých systémech mohou přetrvávat. Rozdílný operační systém na voličově zařízení ale není na rozdíl od použitého webového prohlížeče takový problém. V případě, že volič použije rozdílný webový prohlížeč nebo dokonce jeho jinou verzi, může se vyskytnout riziko špatného nebo dokonce žádného zobrazení uživatelského prostředí volebního systému. Vždy je tedy doporučeno použít nejvíce aktuální verzi daného prohlížeče. Jen takovým způsobem dosáhneme jistoty, že se uživatelské rozhraní načte úplně a správně. Ideálně by systém měl být schopen fungovat z důvodu použití staršího operačního systému i na verzích prohlížeče staršího data. Jakmile ale použijeme některé novější technologie, jako jsou například nové frameworky nebo novější verze programovacích jazyků, je pravděpodobné, že starší webový prohlížeč nemá v sobě integrovanou podporu pro tyto technologie. Vždy je tedy na místě systém naprogramovat pro co největší množství zařízení, která jsou používána.

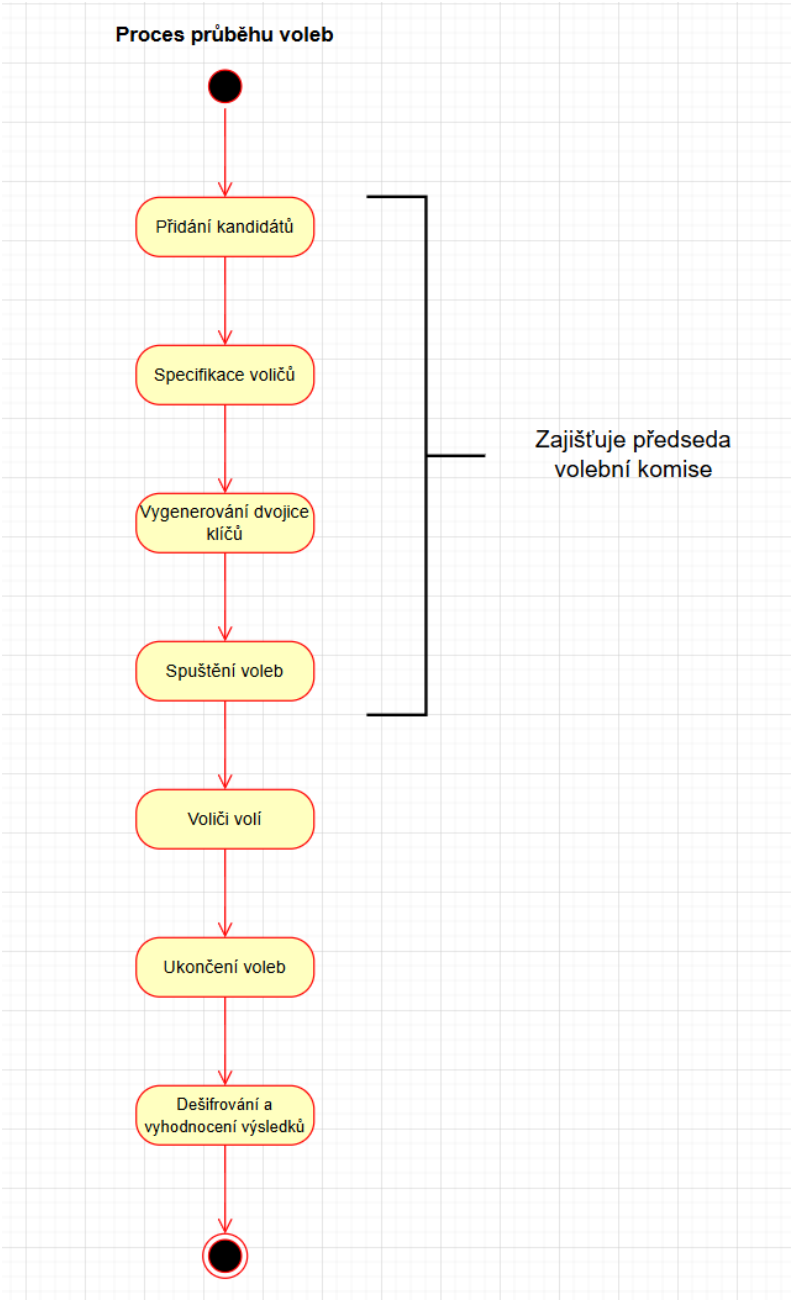
Transparentnost

V neposlední řadě je nutné, aby takový volební systém byl důvěryhodný a ověřitelný. K tomu je potřeba, aby byl systém maximálně transparentní. Všechny specifikace a audity tedy musí být zpětně dohledatelné. Pokud by některé skutečnosti byly utajeny, může nastat důvodné podezření a případná nedůvěra v daný systém. V momentě ukončení voleb musí v systému existovat možnost externího ověření integrity výsledků. Jinými slovy, pokud některý subjekt bude vyžadovat kontrolu nebo revizi výsledků voleb, musí v systému tato možnost existovat. Systém, respektive jeho vývojáři, musí být otevřen k odbornému přezkoumání

systému nebo bezpečnostním testům. A to jak na pravidelné bázi nebo pokud o to požádá některý konkrétní subjekt. Celkově lze shrnout, že čím více je systém transparentní, tím větší důvěru u voličů vzbuzuje.

2.2. Diagramy

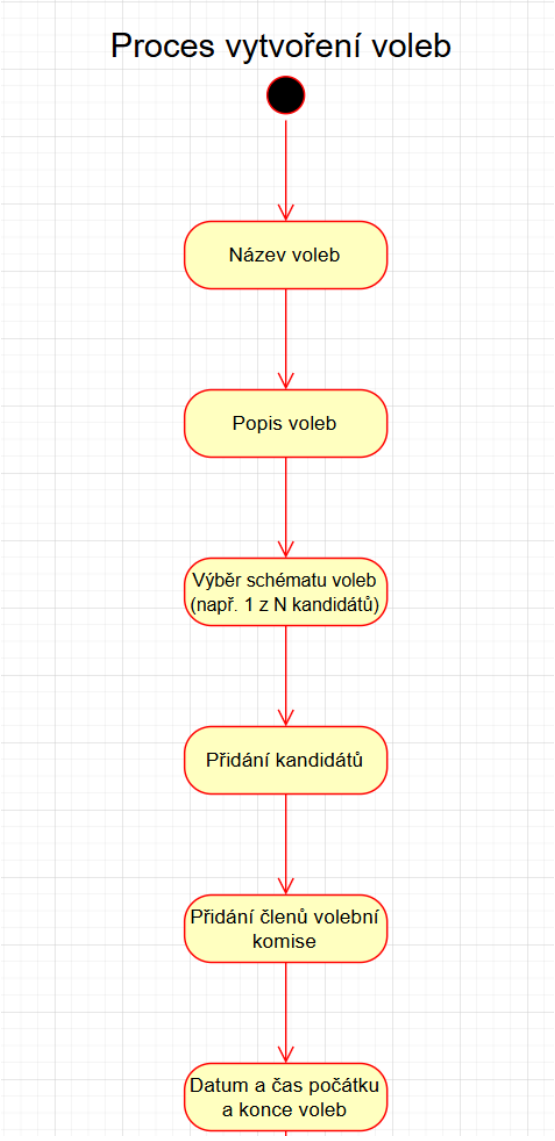
V rámci experimentální části se podrobněji podíváme na celou funkčnost elektronického volebního systému, respektive tohoto navrhovaného řešení. Celý princip fungování si ukážeme na několika diagramech. Prvním z nich je velmi zjednodušený princip celého volebního systému.



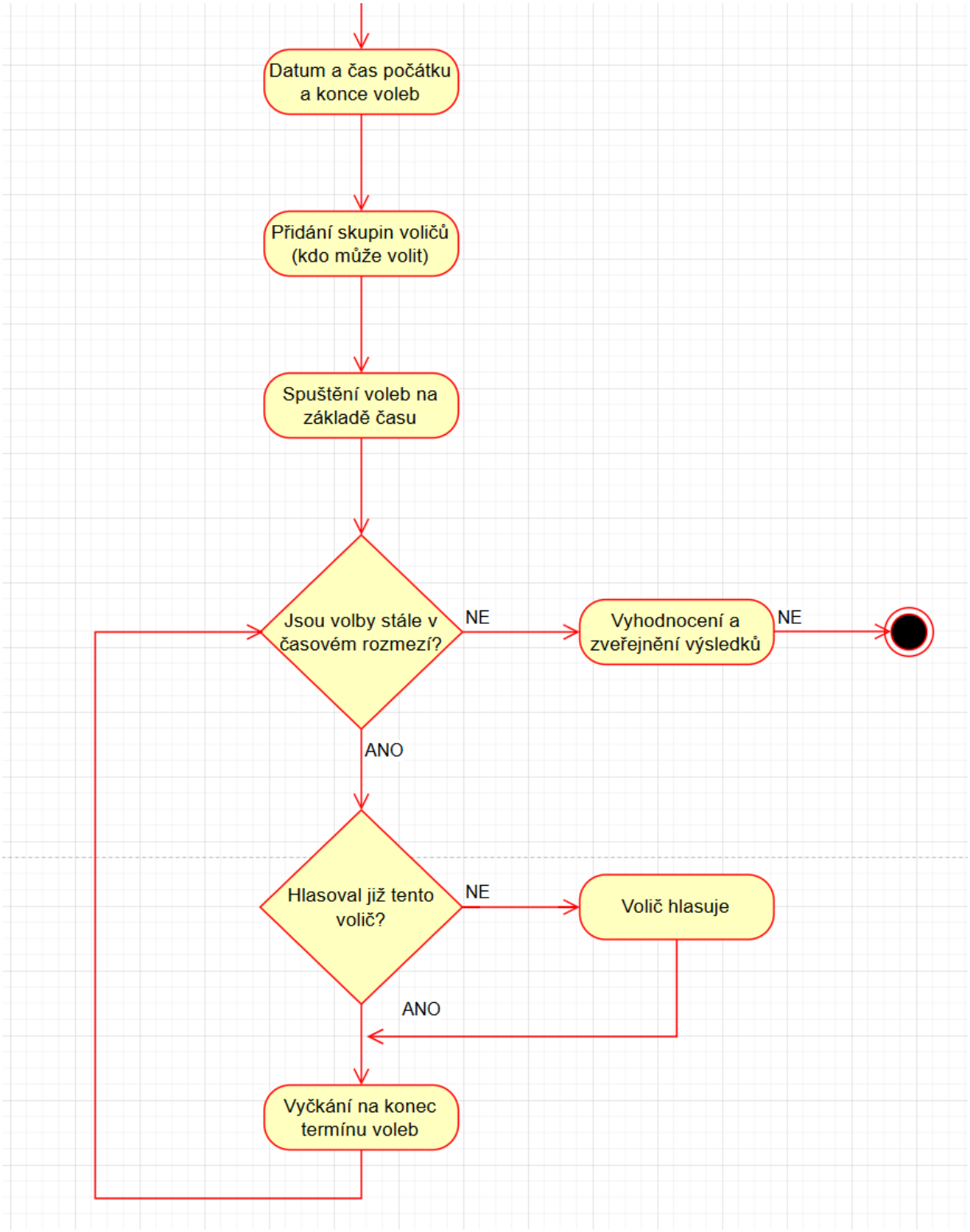
Obrázek 1: Zjednodušené schéma průběhu voleb

Z uvedeného diagramu je zřejmé, že první tři kroky zajišťuje předseda volební komise. Provádí proces zakládání voleb, do kterých přidá určitý počet kandidátů a specifikuje, jaké skupiny voličů budou mít oprávnění provést volbu a kdo bude členem volební komise. Členů může být více než jeden. Ve chvíli, kdy se volby založí, ověří se aktuální datum a čas s datem a časem nastaveným na začátek konkrétních voleb. Pokud aktuální čas odpovídá času začátku voleb, mohou definované skupiny voličů začít provádět volbu. Po vypršení času určeného pro volbu nastává vyhodnocení výsledků voleb. Nelze je vyhodnotit dříve, než je definovaný čas ukončení voleb.

Jelikož je ale tento diagram příliš obecný a nezahrnuje některé výše popsané kroky, je na místě přiložit ještě jeden diagram, který detailněji popíše princip vytvoření voleb v tomto volebním systému, jejich následné spuštění a ukončení.



Obrázek 2: Podrobnější schéma průběhu voleb (část 1)



Obrázek 3: Podrobnější schéma průběhu voleb (část 2)

Nyní již lze vidět kompletní implementaci znázorněnou pomocí diagramu aktivit. Protože je diagram příliš rozsáhlý, aby se vešel pouze na jednu stranu, je rozdělený, mj. i kvůli lepší čitelnosti, na dvě strany. Popíšeme si tedy jednotlivé kroky, jak jdou za sebou, a vysvětlíme si, co každý krok vykonává.

Název voleb – předseda volební komise při vytváření voleb zvolí stručný a výstižný název pro nadcházející volební proces.

Popis voleb – s vhodným pojmenováním voleb souvisí i vhodný a stručný popis, čeho se volby konkrétně týkají; může se tak jednat o podrobnosti a podmínky k hlasování.

Výběr schématu voleb – předseda určí, jaké schéma budou volby používat; příkladem může být výběr jednoho z N kandidátů nebo hlasování pomocí kroužkování (volič může vybrat více kandidátů).

Přidání kandidátů – v rámci volebního procesu je nutné, aby v něm byli přítomni kandidáti, které předseda zadá; počet kandidátů není nijak omezen, avšak musí být vložen vždy alespoň jeden.

Přidání členů volební komise – současně s kandidáty je nutné rovněž přidat členy volební komise, kteří budou na průběh voleb společně s předsedou dohlížet.

Datum a čas počátku a konce voleb – při zakládání voleb je rovněž potřeba zadat i časové rozmezí volebního procesu; datum a čas počátku voleb nesmí být pozdější než datum a čas ukončení voleb.

Přidání skupin voličů – tato část velmi úzce souvisí s přidáním kandidátů a členů volební komise; skupiny voličů tedy také přidává předseda volební komise a rozhoduje tak o tom, kdo se může účastnit jakých voleb.

Spuštění voleb na základě času – aby se předešlo použití například cronjobu, je potřeba nějakým způsobem ověřit, kdy se volby spustí; v tomto případě se tedy volby zahájí v momentě, kdy aktuální čas odpovídá nastavenému času počátku voleb.

Jsou volby stále v časovém rozmezí? – podmínka, která se jinými slovy ptá na to, zda lze stále ve volbách hlasovat; pokud ne, přejde systém k bloku vyhodnocení výsledků; pokud ano, přecházíme k další podmínce.

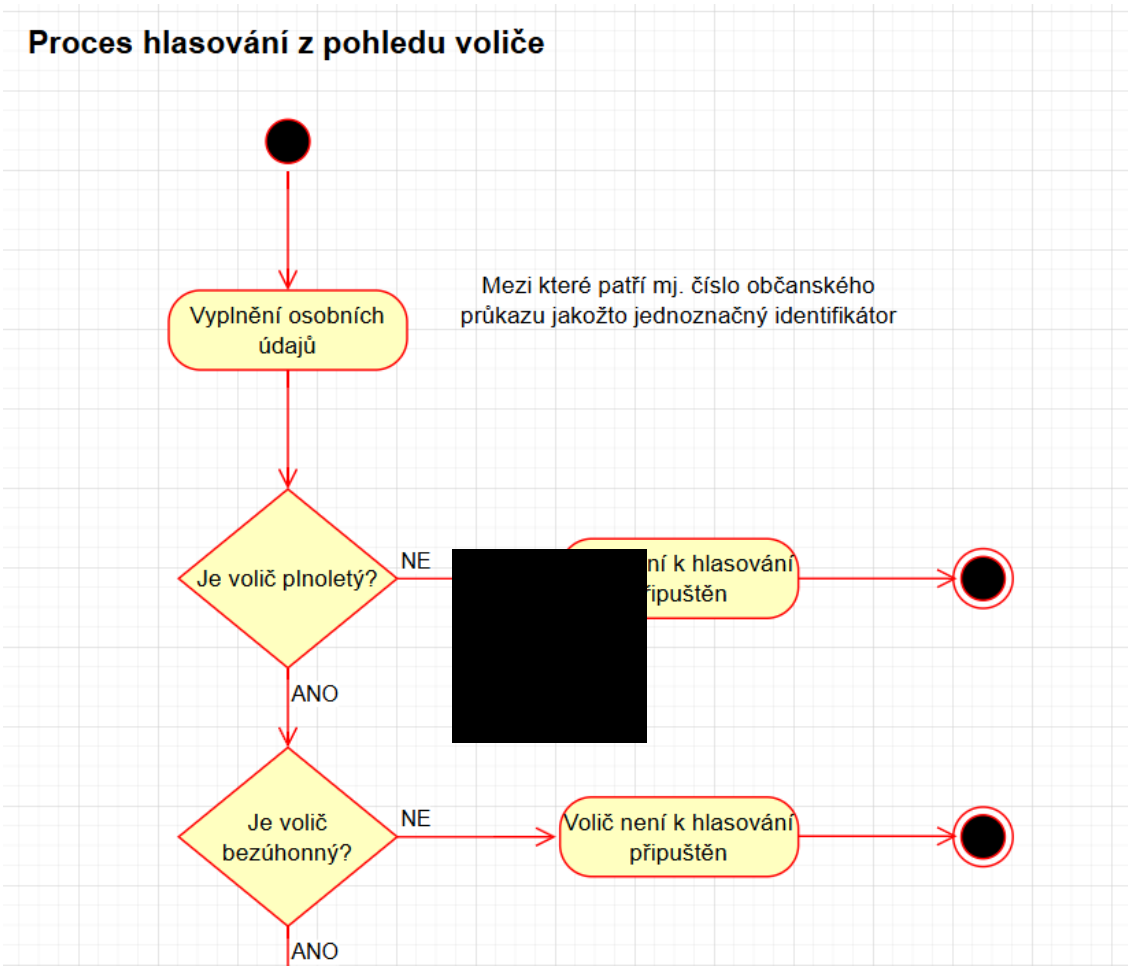
Hlasoval již tento volič? – podmínka, ke které systém přejde v případě, že jsou volby stále aktivní; pokud volič ještě nehlasoval, má možnost hlasovat; pokud už volič odevzdal hlas, vyčká, až volby skončí, jelikož není přípustné vícenásobné hlasování.

Volič hlasuje – volič ještě neodevzdal svůj hlas a má tedy možnost se hlasovacího procesu zúčastnit nebo již právě hlasuje; po odevzdání hlasu vyčká do konce voleb.

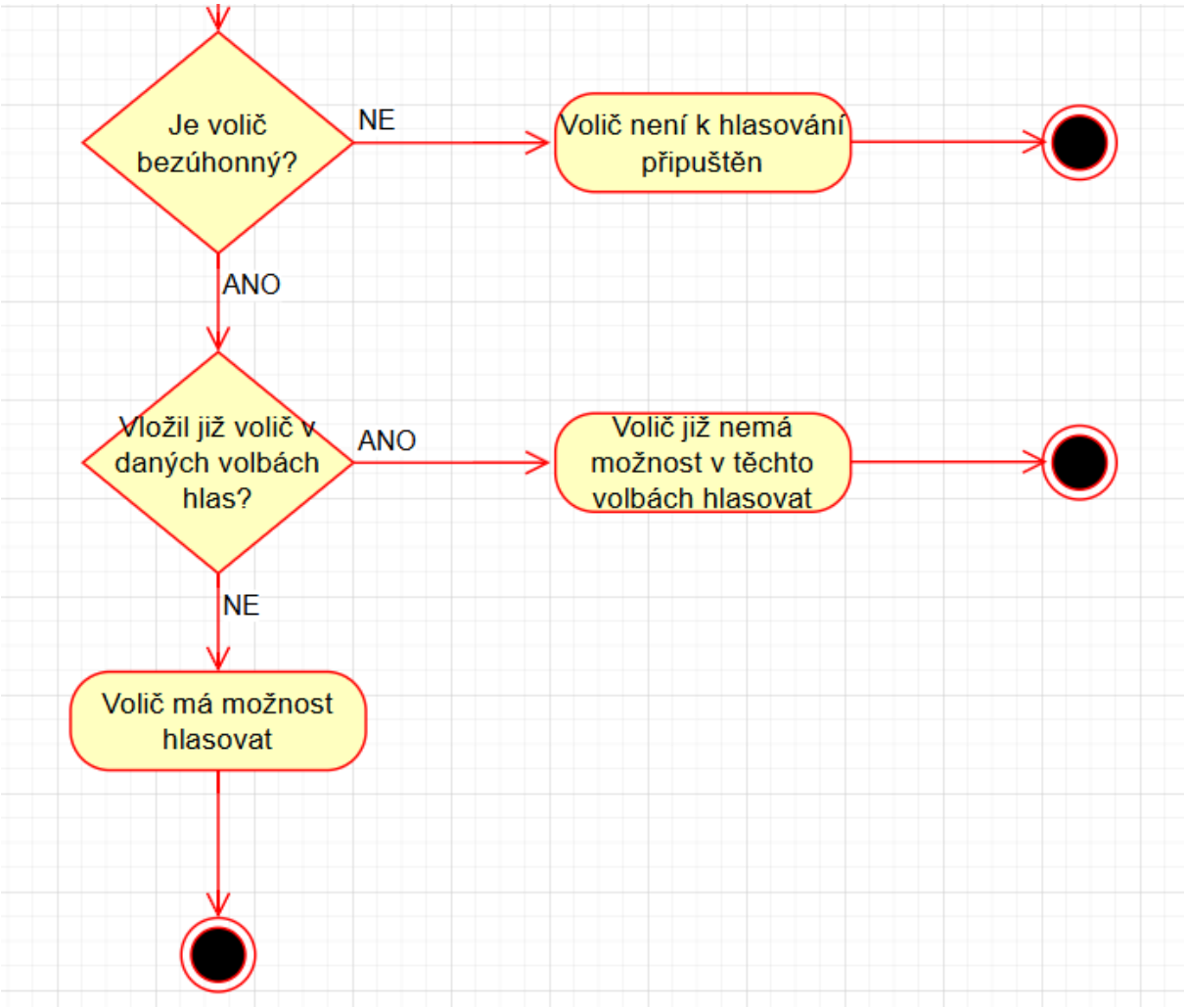
Vyčkání na konec termínu voleb – pokud už volič odhlasoval, čeká až do konce časového limitu možnosti hlasování, vícenásobná volba není možná; celý proces ověření, zda jsou volby stále aktivní, proběhne znovu.

Vyhodnocení a zveřejnění výsledků – tento proces nastává v momentě, kdy již volby nejsou aktivní (čili dosáhly časového limitu ukončení); vyhodnocení a zveřejnění výsledků může provést jak předseda volební komise, tak i členové volební komise; zveřejnění výsledků může proběhnout například uložením výsledků do souboru typu PDF a následným umístěním na webovou stránku (v budoucnu může být přidáno jako funkce).

Na zobrazených diagramech je tedy možné vidět, jak volební systém funguje od zahájení do ukončení volebního procesu. Z tohoto důvodu uvedené diagramy postrádají jakékoli zobrazení procesu autentizace voliče. Pro takový případ je určen diagram na zobrazení samotného procesu hlasování, který je uveden níže.



Obrázek 4: Schéma procesu hlasování z pohledu voliče (část 1)



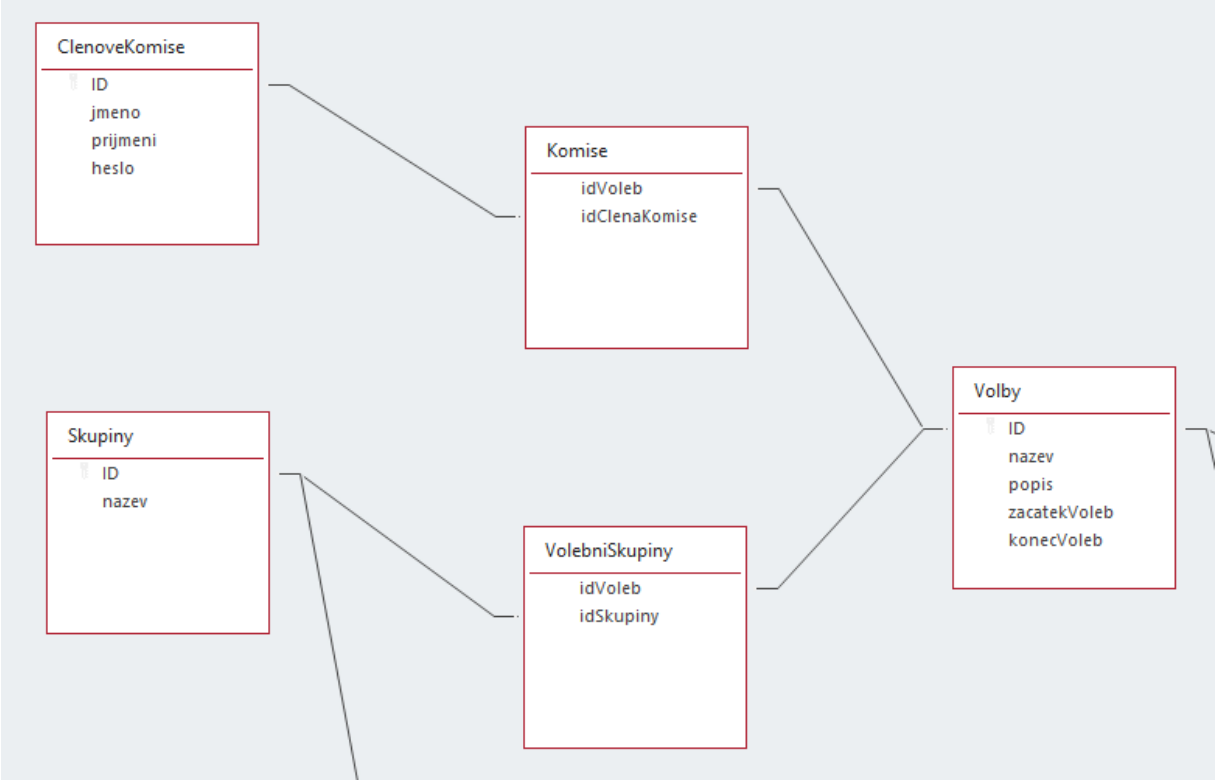
Obrázek 5: Schéma procesu hlasování z pohledu voliče (část 2)

Z uvedeného diagramu aktivit lze usoudit, že proces ověření identity voliče a odevzdání hlasu není nijak zvlášť složitý. Předpokládejme, že volič korektně vyplnil osobní údaje, a to včetně identifikačního čísla na občanském průkazu. V takovém případě lze ověřit, zda již volič dosáhl plnoletosti. Pokud volič není plnoletý, není možné jej k volbám připustit. Pakliže platí opak, obvykle se kontroluje i bezúhonnost voliče. V případě uvedeného elektronického volebního systému není tato funkce nijak implementována, avšak je možné toto ověření v budoucnu implementovat. Faktem však zůstává, že pokud zletilý volič není účastníkem jakéhokoli trestního řízení, může být účastníkem hlasovacího procesu. Nakonec systém ověří, zda již volič v některých pro něj dostupných voleb provedl volbu. Pokud už volič jednou odevzdal v některých volbách svůj hlas, není možné, aby se volebního procesu znovu účastnil. Toto ověření slouží jako pojistka proti vícenásobnému hlasování. [22]

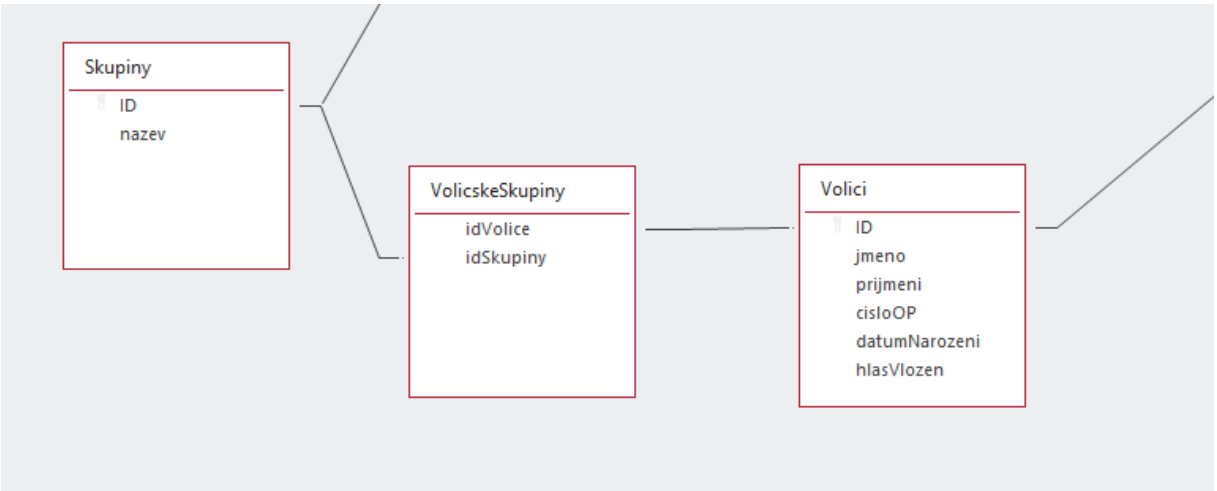
2.3. Databázové schéma

Tyto diagramy názorně ukazují zjednodušený princip fungování celého elektronického volebního systému, respektive jeho implementace. Z praktického hlediska je však také vhodné přiložit, jak volební aplikace skutečně vizuálně vypadá, jak vypadá její implementace ve zdrojovém kódu a také jaké je databázové schéma.

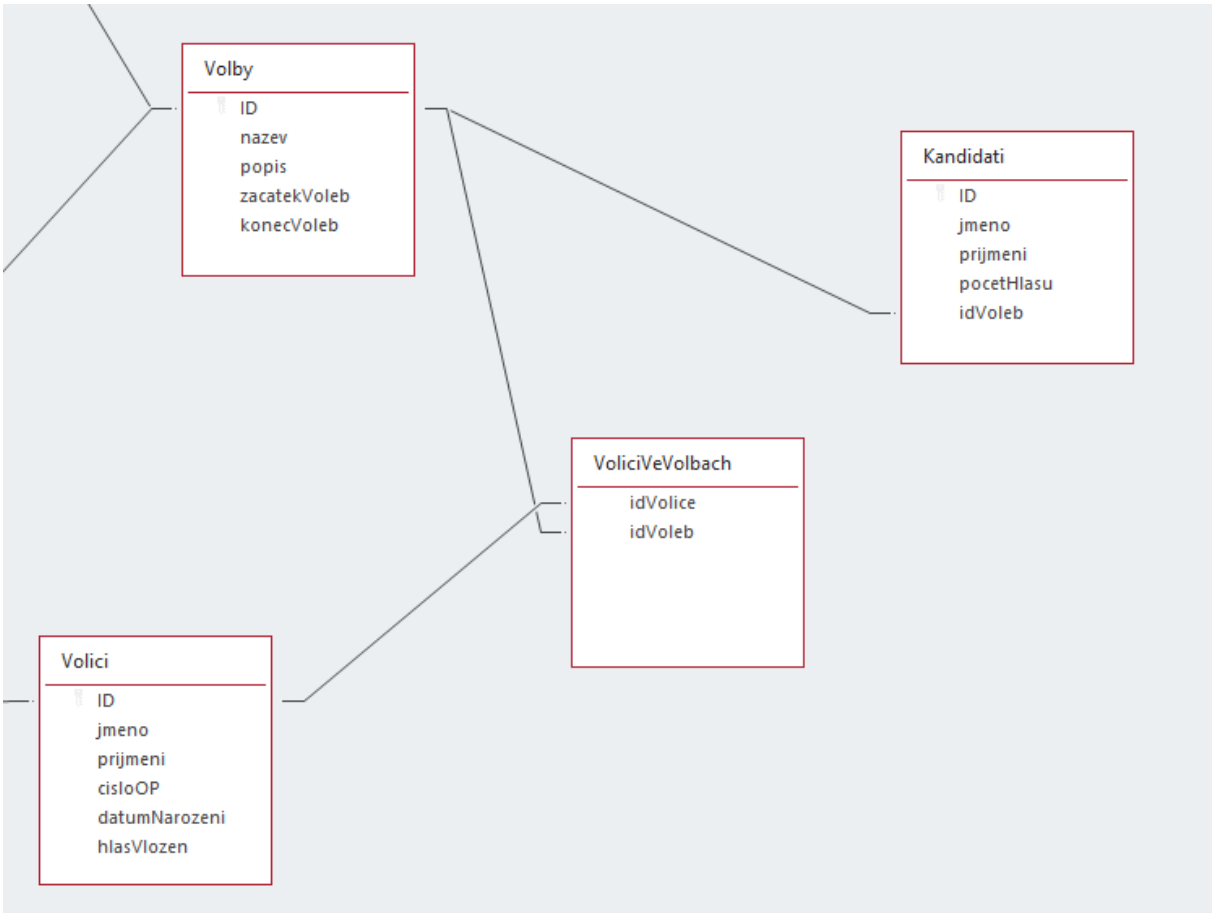
Celý elektronický volební systém, respektive jeho aplikace, je naprogramována za pomocí programovacích jazyků PHP a JavaScript a značkovacích jazyků HTML a CSS. Jedná se tedy o webovou aplikaci. Databáze je řešena pomocí databázového systému SQLite. Tento databázový systém je v projektu implementován z důvodu jeho vysoké rychlosti, jednoduchosti a přenositelnosti. Programovací jazyk PHP podporuje použití SQL databází, ať už se jedná o tradiční MySQL databáze nebo právě SQLite, pomocí rozhraní PDO, které přispívá k pohodlnější práci. Databázový systém SQLite má na rozdíl od tradičního systému MySQL výhodu v podstatně jednodušší konfiguraci, kdy není potřeba provádět zvláštní nastavení databázového serveru a zároveň nabízí většinu potřebných funkcí. Proto se může systém SQLite využít i například v seznamu telefonních kontaktů. Podívejme se však na databázovou strukturu celé aplikace.



Obrázek 6: Databázové schéma – popis entit (část 1)



Obrázek 7: Databázové schéma – popis entit (část 2)



Obrázek 8: Databázové schéma – popis entit (část 3)

Přiložené snímky obrazovky znázorňují vztahy jednotlivých entit v databázovém systému. Na první pohled se může zdát, že databáze obsahuje více než deset entit, avšak zdání klame. Takto je s velkou přesností názorně vidět, jak vypadají vztahy mezi entitami. Pro doplnění je vhodné zmínit, že většina entit je ve vztahu 1:N. Existují však výjimky, kdy je mezi entitami

vztah M:N. V takovém případě je nutné tento vztah rozložit z jednoho M:N na dva 1:N, což je obvykle doplněno zvláštní vazební tabulkou obsahující pouze primární klíče dvou entit. S vazebními tabulkami je tedy v databázi celkem devět entit a nyní následuje jejich podrobný popis.

ClenoveKomise – jedná se o entitu uchovávající informace o jednotlivých členech volební komise; uchovává se ID člena volební komise, jméno, příjmení a heslo; samozřejmostí u hesla je použití šifrování ke zvýšení bezpečnosti uložení.

Volici – entita uchovávající veškeré osobní údaje voličů v této aplikaci; kromě ID voliče také entita uchovává jméno, příjmení, datum narození, identifikační číslo občanského průkazu a stav, který ukazuje, zda již volič vložil hlas či nikoli; samozřejmostí je u osobních údajů rovněž jejich šifrování.

Skupiny – voliči jsou rozmístěni do skupin, které poté mohou hlasovat; volič může být součástí více skupin; skupiny od sebe kromě ID odděluje i název.

Volby – tato entita slouží k uchovávání údajů o jednotlivých volebních procesech; obsahuje jednoznačný identifikátor (ID), název voleb, stručný popis, datum a čas začátku voleb a datum a čas jejich ukončení.

Kandidati – v této entitě jsou umístěny údaje o jednotlivých kandidátech; každý kandidát má své ID, kromě toho je tam umístěno i jeho jméno, příjmení, počet získaných hlasů a také ID voleb, kterých se právě účastní.

Komise – vazební tabulka mezi entitami ClenoveKomise a Volby; uchovává informace o tom, kteří členové volební komise patří ke kterým volbám.

VolebniSkupiny – vazební tabulka mezi entitami Skupiny a Volby říká, které skupiny voličů se účastní kterých voleb; nutno podotknout, že více skupin s voliči se může účastnit jedněch nebo více voleb najednou.

VolicskeSkupiny – vazební tabulka mezi entitami Skupiny a Volici; určuje, do které skupiny voličů patří který volič; platí tedy, že součástí jedné skupiny může být více voličů.

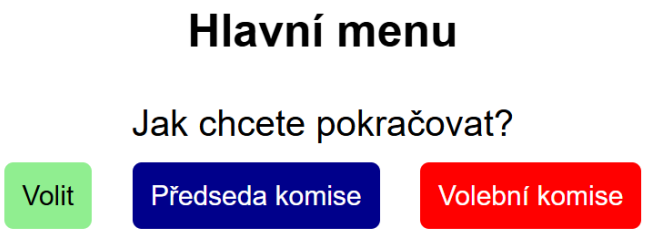
VoliciVeVolbach – vazební tabulka mezi entitami Volici a Volby; sbírá ID voličů a voleb jakožto souhrn voličů, kteří se účastní kterých voleb.

Z popisů jednotlivých entit můžeme soudit, že jejich počet je dohromady devět, kde se čtyři z nich chovají jako vazební tabulky. Celkový počet tedy není příliš velký a k řádné funkčnosti

není potřeba více entit. Je také důležité zmínit, že primární klíče prvních pěti jmenovaných entit se vztahují výhradně k atributu ID. Jen jedna z těchto entit, konkrétně Kandidati, obsahuje jak primární klíč, tak i cizí klíč, a to na atributu idVoleb.

2.4. Grafické prostředí aplikace

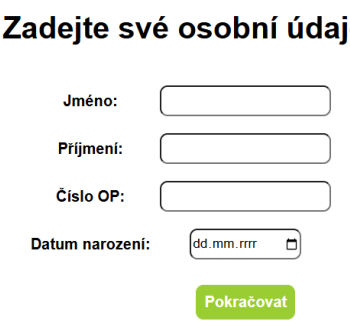
Nyní následuje ukázka celé volební aplikace ve webovém prohlížeči tak, jak ji uvidí všichni aktéři účastnící se jakéhokoli volebního procesu. Prvním snímkem je domovská stránka, již uvidí všichni bez ohledu na to, jestli se jedná o voliče, předsedu volební komise nebo členy volební komise.[23]



Obrázek 9: Hlavní menu aplikace

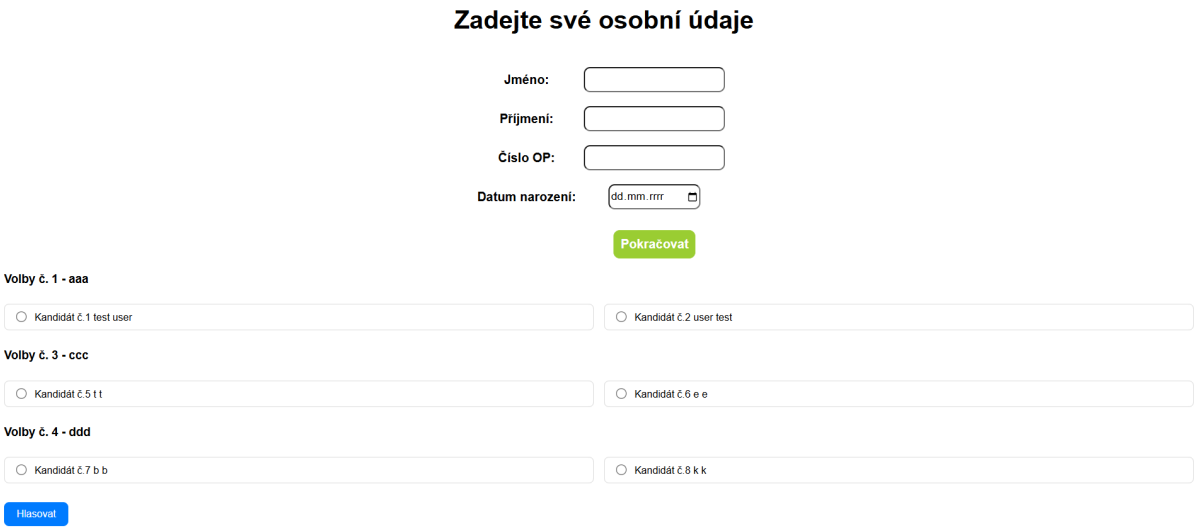
2.4.1. Možnosti voliče

Po stisknutí tlačítka „Volit“ se objeví následující obrazovka, která voliče vyzve, aby zadal své osobní údaje. Konkrétně je požadováno zadání jména, příjmení, identifikačního čísla občanského průkazu a data narození. Vzhledem k faktu, že v České republice občanský průkaz obdrží každý občan dovršením věku 15 let, je nutné ověřit i věk voliče, jelikož k volbám nejsou připuštěni občané mladší 18 let. Datum narození volič zadává ve formátu DD.MM.YYYY (den.měsíc.rok – např. 01.04.1999) nebo kliknutím na ikonu kalendáře, kde je možné zadat datum narození bez znalosti jakéhokoli formátování data.



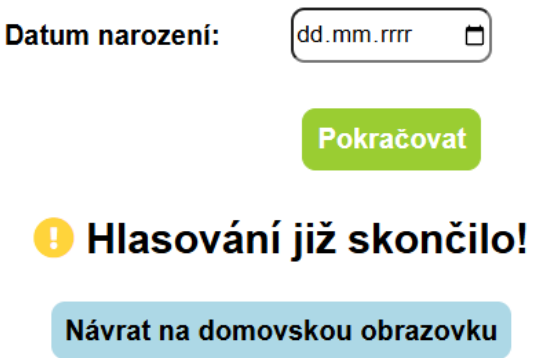
Obrázek 10: Vstupy, které volič zadá, aby se mohl účastnit voleb

Po zadání osobních údajů voliče, který je řádně zaregistrovaný včetně přidělené voličské skupiny, se ve stejném okně zobrazí nabídka voleb, v nichž je daný volič oprávněný volit. Pokud má volič možnost odevzdat svůj hlas ve více volbách, vypíší se všechny pod sebou, a to včetně všech kandidátů v daných volbách. Pokud však v jedněch z nich již svůj hlas odevzdal a bude chtít odevzdat hlas v těchto konkrétních volbách znovu, nebude to možné, jelikož se dané volby zkrátka nezobrazí. V ostatních volbách ale nadále může hlasovat.

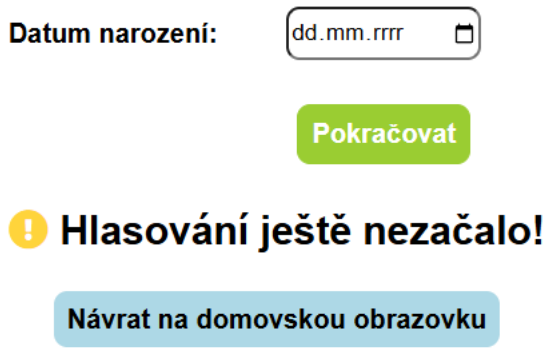


Obrázek 11: Výpis dostupných voleb pro daného voliče

Během odevzdávání hlasu mohou nastat určité problémy. Zejména v případě, že již vypršel termín možnosti odevzdání hlasu v konkrétních volbách nebo naopak, že ještě nenastal termín, kdy by bylo možné začít hlasovat.

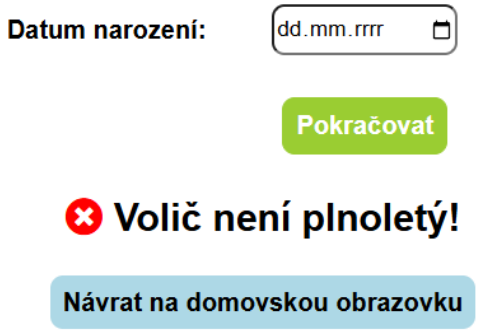


Obrázek 12: Upozornění voliče, že se pokusil hlasovat po termínu voleb

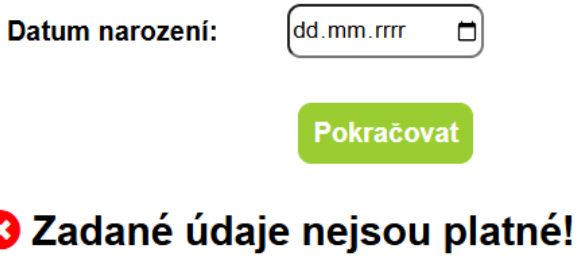


Obrázek 13: Upozornění voliče, že se pokusil hlasovat před termínem voleb

Před odevzdáním hlasu je také možné narazit na podstatně závažnější problémy, než jsou ty, které byly zmíněny výše. Potíže mohou nastat už během pokusu o ověření uživatele. A to zejména v případě, že volič ještě nedosáhl plnoletosti. V této situaci sice může mít platný občanský průkaz, nicméně dosažení plnoletosti je klíčovou podmínkou k možnosti hlasování. Může také nastat situace, kdy volič zadá chybné osobní údaje. Může se jednat o jakoukoli z vlastností výše zmíněných. Pokud volič zadává správné údaje, ale v databázi jsou údaje chybné nebo zastaralé, je volič povinný o této skutečnosti informovat kohokoli z příslušné volební komise.

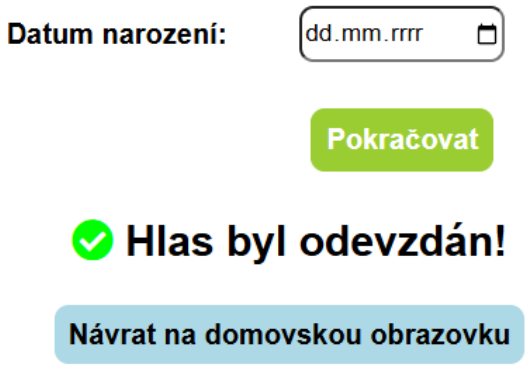


Obrázek 14: Upozornění voliče, že nedosáhl plnoletosti



Obrázek 15: Upozornění voliče, že zadal nesprávné osobní údaje

Ve většině případů by však k žádným podobným chybám nemělo docházet. Toto byly ty nejzásadnější, které během celého procesu hlasování mohou nastat. Běžnou by měla být situace, kdy aplikace voliče informuje o odevzdání svého hlasu, jako je tomu u obrázku níže.

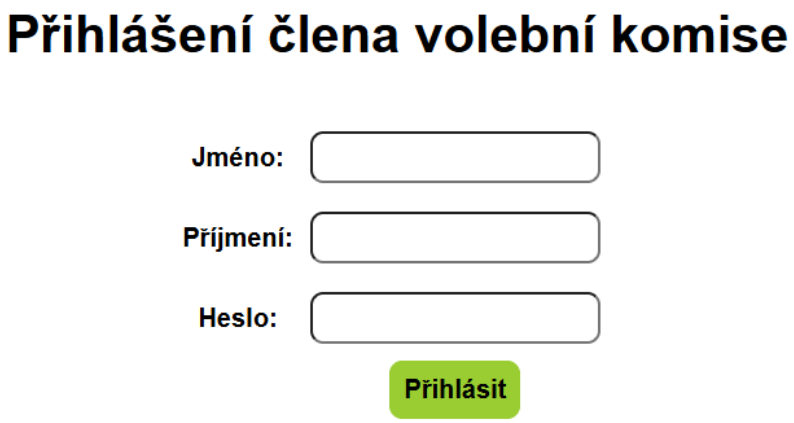


Obrázek 16: Potvrzení pro voliče, že byl jeho hlas zaznamenán

Toto byly všechny možnosti, které má běžný volič. Nyní následuje popis prostředí určeného pro členy volební komise.

2.4.2. Možnosti členů volební komise

Členové volební komise se ověřují pomocí jejich jména, příjmení a hesla. Stisknutím přihlašovacího tlačítka se aplikace dostane k panelu určenému pouze pro volební komise. K tomuto dialogovému oknu se lze dostat přes tlačítko „Volební komise“ v hlavním menu aplikace.

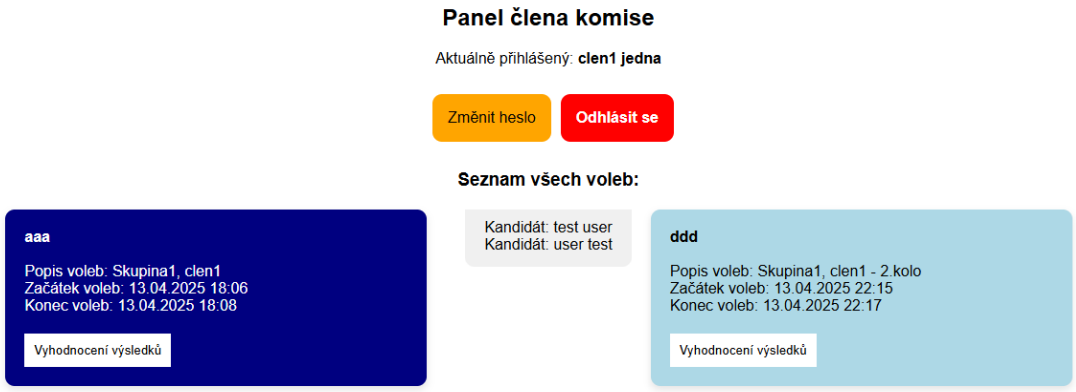


Obrázek 17: Přihlašovací okno pro členy volební komise

Níže uvedený obrázek zobrazuje prostředí, v němž se člen volební komise bude pohybovat. Je velice jednoduché, přehledné a obsahuje výčet pouze těch voleb, u kterých předseda volební komise vybral přítomnost členů komise.

Obrázek 18: Prostředí určené pro členy volební komise

Po stisknutí na určený druh voleb celá karta změní barvu na tmavě modrou a text v ní na bílou, aby byl dobře čitelný. Zároveň s tím se vedle karty s volbami zobrazí také karta světle šedé barvy, v níž jsou vypsáni jednotliví kandidáti v daných volbách. Karty jsou od sebe dostatečně vzdáleny tak, aby se navzájem nepřekrývaly, ale zároveň neměly mezi sebou až příliš velké mezery.



Obrázek 19: Prostředí určené pro členy volební komise

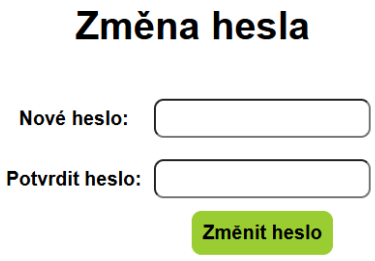
Na obrázku níže je vidět prostředí z pohledu jiného člena volební komise, který skutečně vidí jen svoje volby.

Obrázek 20: Prostředí určené pro členy volební komise (jiný uživatel)

Členové volební komise jsou také oprávněni vyhodnotit výsledky voleb. Tuto možnost však mohou využít pouze za předpokladu, že předseda volební komise již ověřil výsledky svým soukromým klíčem. Pokud tak předseda neučinil, jsou o tom členové tímto informováni způsobem přiloženým na následujícím snímku.

Obrázek 21: Pokud předseda komise nevložil svůj soukromý klíč, jsou pro členy komise výsledky nedostupné

Každý člen volební komise má možnost si změnit přístupové heslo. Tento krok je důrazně doporučený zejména při prvním přihlášení, jelikož výchozí heslo, které se nastaví v momentě, kdy je konkrétní člen volební komise vytvořen předsedou volební komise, je slabé a snadno prolomitelné.

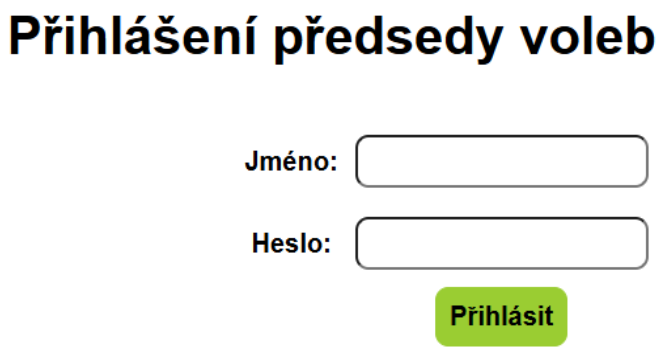


Obrázek 22: Dialog pro změnu hesla člena volební komise

Tyto snímky obrazovky tedy pokryly popis grafického prostředí, v němž se budou pohybovat členové volební komise. Následuje popis prostředí pro předsedu volební komise.

2.4.3. Možnosti předsedy volební komise

K tomuto dialogovému oknu se lze dostat pomocí tlačítka „Předseda komise“ v hlavním menu aplikace. Předseda volební komise se přihlašuje pouze svým uživatelským jménem a heslem.



Obrázek 23: Přihlašovací okno pro předsedu volební komise

Po úspěšném přihlášení si lze všimnout obdobného panelu, jako mají členové volební komise, jen s několika rozdíly. Předseda volební komise, na rozdíl od členů, vidí všechny volby, které byly v této aplikaci vytvořeny. Zároveň má k dispozici tři zelená tlačítka, která při nasměrování kurzoru myši na ně zobrazí další možné akce. Vedle těchto tlačítek je dále ještě tlačítko pro odhlášení předsedy ze systému, schází však tlačítko pro změnu hesla. Tuto možnost předseda volební komise primárně nemá z toho důvodu, že by tento účet měl být co nejlépe zabezpečený proti napadení (tj. mít velmi silné heslo).

Obrázek 24: Prostředí určené pro předsedu volební komise

Ukázka, co vše může předseda komise přidat.

Obrázek 25: Vlastnosti, které může předseda přidat

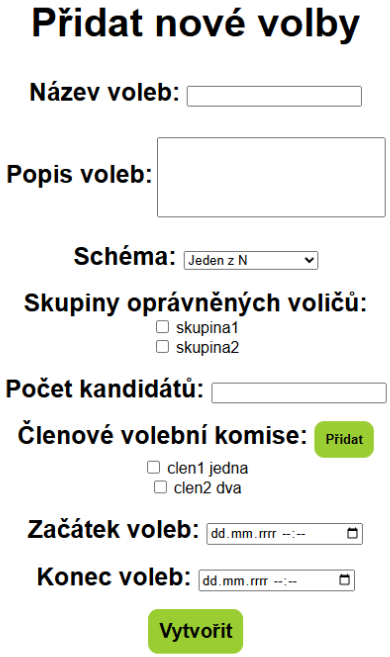
Následuje ukázka, co vše může předseda upravit či změnit.

Obrázek 26: Vlastnosti, které může předseda upravit

V neposlední řadě má předseda komise možnost odstraňovat veškeré záznamy. Účet předsedy volební komise se tedy z programátorského hlediska může tvářit jako administrátorský, jelikož má možnost spravovat téměř jakoukoli tabulku v databázi.

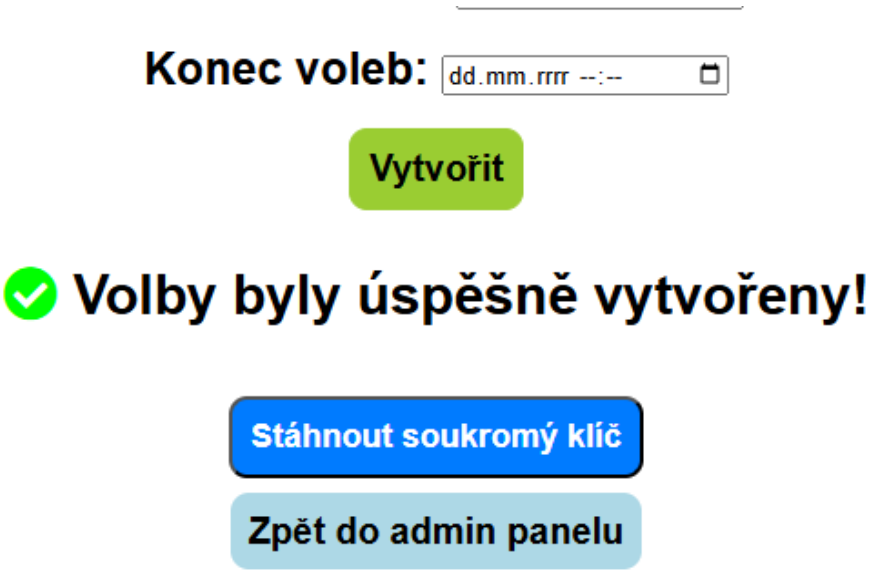
Obrázek 27: Vlastnosti, které může předseda odstranit

Pomocí tlačítek „Přidat“ -> „Volby“ v panelu pro předsedu má předseda komise možnost vytvořit nové volby. Na snímku níže lze vidět, co vše musí předseda volební komise vyplnit, aby mohl nové volby skutečně vytvořit.



Obrázek 28: Ukázka povinných parametrů při vytváření nových voleb

Během vytváření voleb se rovněž generuje dvojice klíčů (soukromý a veřejný) a zpráva, která je touto dvojicí klíčů zašifrována. Předseda je tedy vyzván, aby si soukromý klíč stáhnul k sobě do počítače, případně na externí záznamové médium.

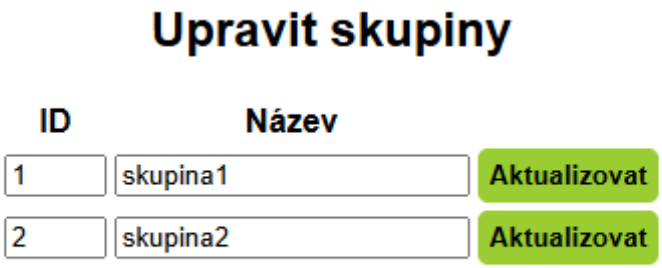


Obrázek 29: Při vytvoření voleb si předseda stáhne soukromý klíč

Pomocí tlačítka „Přidat“ u části „Členové volební komise“ má předseda tímto způsobem možnost přidat člena volební komise, kterému vytvoří jméno a příjmení. Heslo (aaaaaa) je generováno automaticky, a to ihned po stisknutí tlačítka „Uložit“. Tím se rovněž celé toto modální okno zavře.

Obrázek 30: Modální okno pro přidání člena volební komise

Na dalším snímku je vidět možnost úpravy názvu skupiny. Název se upraví tak, že se do kolonky, kde je umístěný, napíše nový. Ten se pak potvrdí stiskem tlačítka „Aktualizovat“.



Obrázek 31: Ukázka možnosti úpravy skupin voličů

Jak již bylo dříve zmíněno, předseda má možnost záznamy rovněž odstraňovat. Na níže uvedeném obrázku je ukázka tabulky s kandidáty. Předseda smí záznamy odstraňovat stiskem tlačítka „Smazat“ jednotlivě u každého záznamu nebo všechny najednou stiskem tlačítka „Smazat vše“. Záznamy v jednotlivých buňkách není možné dále upravovat, jelikož je na nich nastavený atribut „readonly“.

Obrázek 32: Ukázka možnosti odstranění kandidátů

Předseda i členové komise mají možnost si zobrazit výsledky voleb ve chvíli, kdy se volební proces ukončí. Dříve to není možné, a to jak u členů volební komise, tak ani u předsedy. Aby byly výsledky dostupné, je navíc nutné je dešifrovat soukromým klíčem předsedy. Jak je možné vidět na následujícím snímku, předseda je vyzván k vložení svého soukromého klíče. Poté už jen stiskne tlačítko „Ověřit klíč“.

Obrázek 33: Zde předseda vloží svůj soukromý klíč

Pokud se ověření soukromým klíčem nezdaří, vypíše se chybová hláška na následujícím snímku. Tato situace může nastat, pokud předseda vloží zcela jiný soubor nebo pokud se zpráva dešifrovala s jiným než očekávaným výsledkem.

Obrázek 34: Pokud se ověření nezdaří, je o tom předseda informován

Pakliže ale předseda vloží správný klíč, je o této skutečnosti rovněž informován. Jen s tím rozdílem, že tato hláška o úspěšném ověření do dvou vteřin zmizí, daná stránka se obnoví a zobrazí se tabulka s dešifrovanými výsledky.

Obrázek 35: Pokud se ověření podaří, je o tom předseda rovněž informován a zobrazí se jemu a všem příslušným členům volební komise výsledky

Výsledky se zobrazí do tabulky níže s tím, že je u ní u konkrétních voleb vždy uvedena volební účast. V rámci možnosti zveřejnění výsledků je implementována funkce exportování do souboru formátu PDF. Tento soubor je tedy možné stáhnout stisknutím na tlačítko „Export do PDF“. Po stažení je možné jej následně umístit na webovou stránku tomu určenou. Tento systém sám o sobě nedisponuje sekcí pro zveřejněné výsledky voleb.

Obrázek 36: Ukázka výsledků voleb po jejich ukončení

Tímto je prostředí pro předsedu volební komise alespoň rámcově popsáno.

2.5. Ukázka zdrojových kódů a popis zabezpečení

Zde je uveden zdrojový kód pro šifrování citlivých údajů, jako jsou například hesla nebo identifikační čísla občanských průkazů. Kód obsahuje funkce pro šifrování a dešifrování dat, získání šifrovacího klíče a inicializačního vektoru a získání obsahu z chráněného souboru .env, který v sobě tyto údaje uchovává.

```php
<?php
define('ENCRYPTION_METHOD', 'AES-256-CBC');

// Funkce pro načtení .env proměnných
function loadEnv($key)
{
    if (!file_exists(__DIR__ . '/.env')) {
        throw new Exception('.env soubor nenalezen');
    }
    $lines = file(__DIR__ . '/.env');
    foreach ($lines as $line) {
        $line = trim($line);
        if (strpos($line, '=') !== false) {
            list($envKey, $envValue) = explode('=', $line, 2);
            if (trim($envKey) == $key) {
                return trim($envValue);
            }
        }
    }
    throw new Exception("Proměnná $key nenalezena v .env souboru");
}

function getKey()
{
    return hex2bin(loadEnv('ENCRYPTION_KEY'));
}

function getIV()
{
    return hex2bin(loadEnv('ENCRYPTION_IV'));
}

function encrypt($data)
{
    $key = getKey();
    $iv = getIV();
    return base64_encode(openssl_encrypt($data, ENCRYPTION_METHOD, $key, 0, $iv));
}

function decrypt($data)
{
    $key = getKey();
    $iv = getIV();
    return openssl_decrypt(base64_decode($data), ENCRYPTION_METHOD, $key, 0, $iv);
}
```

Obrázek 37: Ukázka zdrojového kódu pro šifrování občanských průkazů a hesel

Použitý šifrovací algoritmus AES-256-CBC pro účely zašifrování těchto citlivých údajů stačí. Jedná se tedy o výkonný a bezpečný způsob symetrického šifrování. Na co však symetrické šifrování nestačí je dříve zmíněné ověřování klíčů.

K tomuto kroku je nutné využít asymetrické šifrování, které zajistí vytvoření páru klíčů – soukromého a veřejného. Mezi nejrozšířenější asymetrické šifrovací algoritmy patří RSA. U tohoto algoritmu je však pro zajištění zabezpečení doporučeno používat klíče minimálně o velikosti 2048 bitů. To může zpomalit ověřování, což v případě tohoto systému není žádoucí. Proto je v systému použito šifrování pomocí elyptické křivky (ECC), konkrétně Curve25519, která využívá klíče X25519. Nevýhodou proti RSA klíčům je fakt, že k šifrování pomocí

elyptických křivek obecně je zapotřebí externí knihovna Sodium. V základu PHP je již implementována, nicméně je nutné ji ručně aktivovat. Výhod je na druhou stranu mnohem více. V prvé řadě se jedná o novější algoritmus než RSA, což je jedna z klíčových vlastností. Dále lze zmínit výkonnost a celkovou efektivitu tohoto způsobu šifrování. Z pohledu zabezpečení se totiž základní šifra s velikostí klíčů 256 bitů dá považovat za ekvivalent ke klíčům algoritmu RSA s velikostí 3072 bitů. Požadavky na výpočetní výkon jsou tak z tohoto pohledu značně přívětivější, což jen potvrzuje, že ECC šifrování je vhodnější variantou. Následuje tedy ukázka zdrojového kódu pro vytvoření páru klíčů při zakládání voleb.

```php
$keypair = sodium_crypto_box_keypair();
$publicKey = sodium_bin2base64(sodium_crypto_box_publickey($keypair), SODIUM_BASE64_VARIANT_ORIGINAL);
$privateKey = sodium_bin2base64(sodium_crypto_box_secretkey($keypair), SODIUM_BASE64_VARIANT_ORIGINAL);

$publicKeyPath = "../keys/publickey_$idVoleb.env";
file_put_contents($publicKeyPath, "PUBLIC_KEY_$idVoleb=\"$publicKey\"\n");

$privateKeyContent = "PRIVATE_KEY_$idVoleb=\"$privateKey\"\n";
$tempPrivateKeyFile = "../keys/temp_privatekey_$idVoleb.txt";
file_put_contents($tempPrivateKeyFile, $privateKeyContent);

$message = "verify:$idVoleb";
$nonce = random_bytes(SODIUM_CRYPTO_BOX_NONCEBYTES);
$testEncrypted = sodium_crypto_box($message, $nonce, $keypair);

file_put_contents("../keys/verify_$idVoleb.txt", base64_encode($nonce) . ":" . base64_encode($testEncrypted));
```

Obrázek 38: Ukázka zdrojového kódu pro asymetrické šifrování volebních výsledků

V kódu si lze všimnout, že do adresáře keys se ukládají veřejné klíče a zpráva verify zašifrována dvojící vygenerovaných klíčů. Lze si také ale všimnout jednoho potenciálního bezpečnostního problému. Do stejného adresáře se uloží i soukromý klíč. Je však nutné zdůraznit, že v tomto adresáři nezůstává trvale, ale pouze do chvíle, než si jej předseda stáhne. Po stisknutí tlačítka „Stáhnout soukromý klíč“ se soukromý klíč smaže a je dostupný pouze u předsedy. Pokud však předseda toto tlačítko stiskne, ale nikam si klíč neuloží, nebude pak již možné výsledky voleb dešifrovat. V adresáři keys tedy zůstane pouze obsah přiložený na následujícím snímku.

Obrázek 39: Ukázka adresářové struktury klíčů

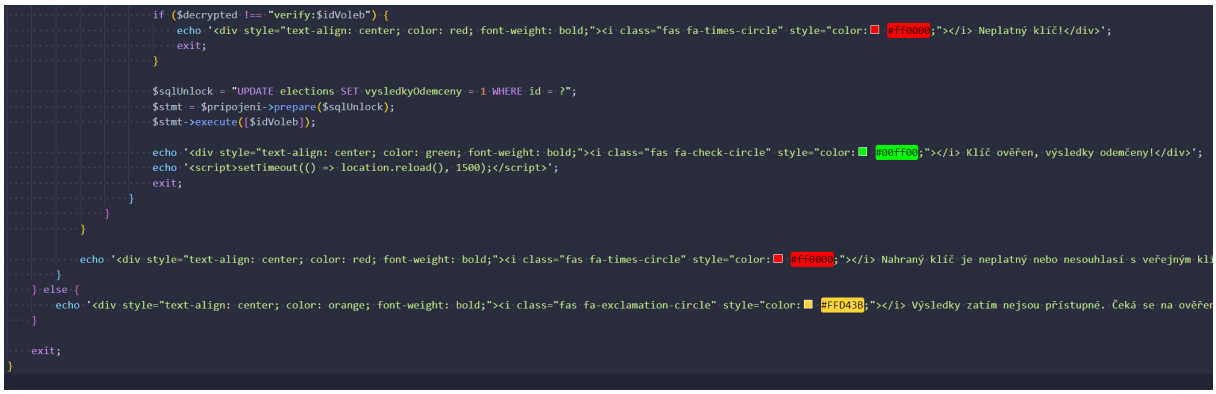
Následuje ukázka zdrojového kódu souboru stahnoutKlic.php. Klíčový je zde příkaz unlink, kterým se odstraní dočasně uložený soukromý klíč ze serveru. Není tedy možné jej již žádným způsobem získat. Soukromý klíč se uloží jako klasický textový soubor.

```php
<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['file'])) {
    $filename = basename($_POST['file']) . '.txt';
    $filepath = "../keys/$filename";

    if (file_exists($filepath)) {
        header('Content-Description: File Transfer');
        header('Content-Type: text/plain');
        header('Content-Disposition: attachment; filename="' . $filename . '"');
        header('Content-Length: ' . filesize($filepath));
        readfile($filepath);
        unlink($filepath); // Smazat po stažení
        exit;
    } else {
        echo '<div style="text-align: center; color: red; font-weight: bold;">Soubor nenalezen nebo již byl stažen.</div>';
    }
} else {
    echo '<div style="text-align: center; color: red; font-weight: bold;">Neplatný požadavek.</div>';
}
```

Obrázek 40: Ukázka zdrojového kódu pro stažení soukromého klíče

Na dalších dvou snímcích je ukázka zdrojového kódu pro odemknutí zašifrovaných výsledků voleb. Když se volební proces ukončí, je možné přejít k vyhodnocení výsledků. Ty jsou však zašifrované a k dešifrování je potřeba dříve zmíněný soukromý klíč předsedy komise. Pokud ještě výsledky předseda nedešifroval, je k tomu vyzván. Pokud je již jednou dešifroval, už se znovu nedešifrují.

```php
$idVoleb = intval($_GET['id']);

$sqlCheck = "SELECT vysledkyOdemceny FROM elections WHERE id = ?";
$stmt = $pripojeni->prepare($sqlCheck);
$stmt->execute([$idVoleb]);
$vysledkyOdemceny = $stmt->fetchColumn();

$isChairman = ($_SESSION['admin'] === 'yes');

if (!$vysledkyOdemceny) {
    if ($isChairman) {
        echo '<div style="text-align: center; margin-top: 20px;">
            <form method="post" enctype="multipart/form-data">
                <label for="keyfile">Pro odemknutí výsledků nahrajte svůj privátní klíč:</label>
                <input id="insertKey" type="file" name="keyfile" required>
                <button type="submit" name="uploadKey" id="overit">Ověřit klíč</button>
            </form><br><br>
        </div>';

        if (isset($_POST['uploadKey']) && isset($_FILES['keyfile'])) {
            $content = file_get_contents($_FILES['keyfile']['tmp_name']);

            if (preg_match('/PRIVATE_KEY_' . $idVoleb . '="(.+)"/', $content, $matches)) {
                $privateKey = sodium_base642bin($matches[1], SODIUM_BASE64_VARIANT_ORIGINAL);

                $publicKeyPath = "./keys/publickey_$idVoleb.env";
                if (file_exists($publicKeyPath)) {
                    $publicEnv = file_get_contents($publicKeyPath);
                    if (preg_match('/PUBLIC_KEY_' . $idVoleb . '="(.+)"/', $publicEnv, $matchesPub)) {
                        $publicKey = sodium_base642bin($matchesPub[1], SODIUM_BASE64_VARIANT_ORIGINAL);

                        list($nonce_b64, $ciphertext_b64) = explode(':', file_get_contents("./keys/verify_$idVoleb.txt"));
                        $nonce = base64_decode($nonce_b64);
                        $ciphertext = base64_decode($ciphertext_b64);

                        $keypair = sodium_crypto_box_keypair_from_secretkey_and_publickey($privateKey, $publicKey);
                        $decrypted = sodium_crypto_box_open($ciphertext, $nonce, $keypair);
```



```
                    if ($decrypted !== "verify:$idVoleb") {
                        echo '<div style="text-align: center; color: red; font-weight: bold;"><i class="fas fa-times-circle" style="color: #ff0000;"></i> Neplatný klíč!</div>';
                        exit;
                    }

                    $sqlUnlock = "UPDATE elections SET vysledkyOdemceny = 1 WHERE id = ?";
                    $stmt = $pripojeni->prepare($sqlUnlock);
                    $stmt->execute([$idVoleb]);

                    echo '<div style="text-align: center; color: green; font-weight: bold;"><i class="fas fa-check-circle" style="color: #00ff00;"></i> Klíč ověřen, výsledky odemčeny!</div>';
                    echo '<script>setTimeout(() => location.reload(), 1500);</script>';
                    exit;
                }
            }
        }

        echo '<div style="text-align: center; color: red; font-weight: bold;"><i class="fas fa-times-circle" style="color: #ff0000;"></i> Nahraný klíč je neplatný nebo nesouhlasí s veřejným kl
    }
} else {
    echo '<div style="text-align: center; color: orange; font-weight: bold;"><i class="fas fa-exclamation-circle" style="color: #FFD438;"></i> Výsledky zatím nejsou přístupné. Čeká se na ověře
}

exit;
}
```

Obrázek 41 a 42: Ukázka zdrojového kódu pro dešifrování výsledků voleb

2.6. Zprovoznění řešení

Ke spuštění celé této aplikace je potřeba spustit webový (Apache nebo nginx) a databázový (MySQL) server. K tomu je možné využít například nástroj XAMPP. Je však nutné ověřit, že PHP běží minimálně na verzi 7.4 kvůli podpoře knihovny Sodium. U starších verzí PHP není možné zaručit kompatibilitu. Dále je pro korektní funkčnost nutné do adresáře C:\Windows\System32\ nakopírovat knihovnu libsodium.dll z adresáře, kde je umístěno PHP. V neposlední řadě je nutné v konfiguračním souboru php.ini zapnout rozšíření Sodium (jinými slovy odstranit znak středníku z části extension=sodium). Tyto náležitosti zajistí správce kódu neboli administrátor systému. Předseda a členové komise budou potřebovat pouze webový prohlížeč ke zprovoznění aplikace.

ZÁVĚR

Návrh a implementace elektronického volebního systému představuje rozsáhlý a po technické stránce náročný úkol. Zvláště velký důraz je však nutné klást na oblast zabezpečení, jelikož ochrana dat a důvěryhodnost celého systému představuje nejzásadnější část jakéhokoli volebního systému. Jak bylo zmíněno na několika již existujících implementacích v zahraničí, dnešní výpočetní technologie umí zajistit opravdu sofistikované zabezpečení. V zemích světa, kde elektronické volby probíhají pravidelně, nejsou z dostupných informací v tuto chvíli žádné důkazy o bezpečnostních incidentech, které by měly přímý dopad na pravost výsledků voleb. Lze tedy konstatovat, že při správném návrhu jsou elektronické volby bezpečné, a mohou tak v budoucnu potenciálně nahradit tradiční prezenční hlasování. I přes podezření, které padlo v roce 2020 na elektronický volební systém v USA během prezidentských voleb, nebyly potvrzeny žádné zásahy, kterými by byla způsobena kompromitace volebních výsledků. Kromě tohoto případu nebyl zaznamenán žádný podobný incident, v němž by figuroval elektronický volební systém, který byl napaden útočníky a následně byla prolomena ochrana dat. Pokud by opravdu existoval případ, kdy byly výsledky voleb kompromitované, jednalo by se s největší pravděpodobností o lidský faktor, kdy by se domluvil předseda volební komise a minimálně jeden další aktér na účelovém zneplatnění volebních výsledků.

Tato bakalářská práce se pokusila shrnout všechny důležité aspekty moderního elektronického volebního systému, a to od úplných teoretických základů přes požadavky týkající se právních a technologických záležitostí až po konkrétní příklady implementací používané v praxi. Součástí práce byla rovněž i návrhová a implementační část, která přinesla jednoduchý model funkční aplikace pro elektronické hlasování. Praktická implementace tohoto systému sice obsahuje základní funkční prostředí, ale existují oblasti, jež by bylo možné dále rozvíjet. Tím je myšleno zejména vylepšení grafického prostředí nebo možnost konfigurace podle cílové skupiny s ohledem na věk. Aplikaci je teoreticky možné použít i například při volbách do školské rady na středních školách a víceletých gymnáziích. Problémem ale zůstává fakt, že všichni žáci středních škol a víceletých gymnázií ještě nedosáhli plnoletosti, přestože disponují platným občanským průkazem. V takovém případě je nutné, aby konkrétní předseda volební komise o této skutečnosti informoval administrátora systému, který má na starost celý zdrojový kód a provedl v něm drobné změny.

POUŽITÁ LITERATURA

[1] WIKIPEDIA. *Volební právo žen*. Online. 2011, aktualizováno 17.2.2025. Dostupné z: https://cs.wikipedia.org/wiki/Volebn%C3%AD_pr%C3%A1vo_%C5%BEen. [cit. 2025-05-01].

[2] WIKIPEDIA. *Volební právo*. Online. 2008, aktualizováno 27.8.2023. Dostupné z: https://cs.wikipedia.org/wiki/Volebn%C3%AD_pr%C3%A1vo. [cit. 2025-05-01].

[3] ČESKÁ REPUBLIKA. *Zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky, ve znění pozdějších předpisů*. Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/1995-247. [cit. 2025-05-01].

[4] ČESKÁ REPUBLIKA. *Zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů, ve znění pozdějších předpisů*. Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-130. [cit. 2025-05-01].

[5] ČESKÁ REPUBLIKA. *Zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí, ve znění pozdějších předpisů*. Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2001-491. [cit. 2025-05-01].

[6] ČESKÁ REPUBLIKA. *Zákon č. 62/2003 Sb., o volbách do Evropského parlamentu, ve znění pozdějších předpisů*. Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2003-62. [cit. 2025-05-01].

[7] ČESKÁ REPUBLIKA. *Zákon č. 275/2012 Sb., o volbách prezidenta republiky, ve znění pozdějších předpisů*. Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-275. [cit. 2025-05-01].

[8] WIKIPEDIA. *Volby*. Online. 2005, aktualizováno 28.3.2025. Dostupné z: https://cs.wikipedia.org/wiki/Volby. [cit. 2025-05-01].

[9] WIKIPEDIA. *Volební systém*. Online. 2006, aktualizováno 29.12.2024. Dostupné z: https://cs.wikipedia.org/wiki/Volebn%C3%AD_syst%C3%A9m. [cit. 2025-05-01].

[10] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Korespondenční volba pro zahraničí*. Online. 2024. Dostupné z: https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/krajane/aktualni_informace/korespondencni_volba_pro_zahranicni.html. [cit. 2025-05-01].

[11] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Korespondenční volba v České republice*. Online. 2024, aktualizováno 31.1.2025. Dostupné z: https://mzv.gov.cz/sarajevo/cz/viza_a_konzularni_informace/konzularni_usek/X_2024_11_04_korespondencni_volba_v_ceske_republice.html. [cit. 2025-05-01].

[12] SEZNAMZPRAVY.CZ. *Co je korespondenční volba a návod, jak hlasovat*. Online. 2025. Dostupné z: https://www.seznamzpravy.cz/clanek/volby-korespondencni-volba-272108.

[cit. 2025-05-01].

[13] WIKIPEDIA. *Elektronické hlasování*. Online. 2017, 23.2.2025. Dostupné z: https://cs.wikipedia.org/wiki/Elektronick%C3%A9_hlasov%C3%A1n%C3%AD. [cit. 2025-05-01].

[14] WIKIPEDIA. *Electronic voting*. Online. 2004, 16.4.2025. Dostupné z: https://en.wikipedia.org/wiki/Electronic_voting. [cit. 2025-05-01].

[15] RIGHT2VOTE INFOTECH PRIVATE LIMITED. *Right2Vote*. Online. 2017. Dostupné z: https://right2vote.in/. [cit. 2025-05-01].

[16] MF GROUP. *Arbitron – bezpečný nástroj pro elektronické hlasování*. Online. 2024. Dostupné z: https://www.mfgroup.cz/produkty/arbitron. [cit. 2025-05-01].

[17] ČESKÉ NOVINKY. *Tajné online volby: Jak elektronický podpis šetří čas a zajišťuje anonymitu*. Online. 2025. Dostupné z: https://www.ceske-novinky.cz/2025/02/09/tajne-online-volby-jak-elektronicky-podpis-setri-cas-a-zajistuje-anonymitu/. [cit. 2025-05-01].

[18] IS JABOK. *E-Volby*. Online. 2020. Dostupné z: https://is.jabok.cz/napoveda/komunikace/volby. [cit. 2025-05-01].

[19] WIKIPEDIA. *Dominion Voting Systems*. Online. 2012, aktualizováno 18.4.2025. Dostupné z: https://en.wikipedia.org/wiki/Dominion_Voting_Systems. [cit. 2025-05-01].

[20] WIKIPEDIA. *Voatz*. Online. 2020, aktualizováno 30.3.2025. Dostupné z: https://en.wikipedia.org/wiki/Voatz. [cit. 2025-05-01].

[21] SOMMERVILLE, Ian. *Softwarové inženýrství*. Brno: Computer Press, 2013. ISBN 978-80-251-3826-7.

[22] KANISOVÁ, Hana a MÜLLER, Miroslav. *UML srozumitelně*. 2. aktualiz. vyd. Brno: Computer Press, 2007. ISBN 80-251-1083-4.

[23] FLANAGAN, David. *JavaScript: the definitive guide*. 7th edition. Sebastopol: O'Reilly, 2020. ISBN 1491952024.

SEZNAM PŘÍLOH

Příloha A: bakalarskaPrace.zip

PŘÍLOHA A*:* bakalarskaPrace.zip

ZIP archiv obsahující vlastní implementaci elektronického volebního systému. Konkrétně se v archivu nachází všechny potřebné soubory a skripty ke spuštění.