

Bakalářská práce

**STUDIE
PROVEDITELNOSTI
NASAZENÍ
ELEKTRONICKÉHO
VOLEBNÍHO SYSTÉMU**

Yana Paluyan

Fakulta informačních technologií ČVUT v Praze
Katedra softwarového inženýrství
Vedoucí: Ing. David Buchtela, Ph.D.
27. června 2021

České vysoké učení technické v Praze
Fakulta informačních technologií

© 2021 Yana Paluyan. Všechna práva vyhrazena.

Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bez uplatněných zákonných licencí nad rámec oprávnění uvedených v Prohlášení, je nezbytný souhlas autora.

Odkaz na tuto práci: Yana Paluyan. *Studie proveditelnosti nasazení elektronického volebního systému*. Bakalářská práce. České vysoké učení technické v Praze, Fakulta informačních technologií, 2021.

Obsah

Poděkování	v
Prohlášení	vi
Abstrakt	vii
Shrnutí	viii
Seznam zkratek	ix
1 Analýza	1
1.1 Úvod do elektronického hlasování	1
1.1.1 Výzvy pro online hlasování	2
1.2 Přehled volebního systému ČR	2
1.2.1 Schéma hlasování	3
1.2.2 Volební účast	4
1.3 Zkušenosti s elektronickými volbami ve světě	6
1.3.1 Estonsko	6
1.3.2 Norsko	8
1.4 Výhody a nedostatky e-voleb	10
1.5 Důvody nízké volební účasti	11
2 Návrh zlepšení systému elektronických voleb	13
2.1 Odůvodnění zavedení nových funkcí	13
2.2 Analýza požadavků	14
2.2.1 Funkční požadavky	14
2.2.2 Nefunkční požadavky	14
2.3 Popis řešení	15
2.3.1 Dostupnost potřebných technologií	16
2.4 Případy užití a uživatelé systému	17
2.4.1 Uživatelé a jejich práva v systému	17
2.5 Diagram případu užití	18
2.5.1 Klíčové uživatelské scénáře	18
3 Studie proveditelnosti	23
3.1 Výhody navrhovaného řešení	23
3.2 Plán nasazení systému	23
3.3 Finanční náklady	25
3.4 Hodnocení rizik	25
4 Závěr	27
Obsah přiloženého média	31

Seznam obrázků

1.1	Volební účast v ČR	4
1.2	Účast ze zahraničí, ČR	5
1.3	Estonská ID karta	7
2.1	Architektura navrhovaného řešení	17
2.2	Případy užití systému	19

Seznam tabulek

1.1	Volební účast v jednotlivých volbách, Estonsko	9
2.1	Use Case 1: Přihlášení	20
2.2	Use Case 2: Autentizace	20
2.3	Use Case 7: Odevzdání hlasu	21
2.4	Use Case 3: Hlasování o návrhu	21
2.5	Use Case 5: Tvorba návrhů	21
2.6	Use Case 6: Testování	22
2.7	Use Case 10: Vytvoření voleb	22
3.1	Přibližná výše platu členů týmu	25
3.2	RZ1: Dokončení projektu po termínu	25
3.3	RZ2: Nedostatečná kvalita projektového týmu	26
3.4	RZ3: Podvádění během profilového testování	26
3.5	RZ4: Nekompatibilita použitých technologií	26
3.6	RZ5: Nízký zájem uživatelů	26

Seznam výpisů kódu

Chtěla bych poděkovat vedoucímu bakalářské práce, Ing. Davidu Buchtelovi, Ph.D., za odborné vedení, rady a ochotu po dobu tvorby této práce. Dále chci poděkovat svým rodičům a přátelům za jejich podporu během celého studia.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 29. března 2021

.....

Abstrakt

V současné době se po celém světě aktivně vyvíjí teoretický a praktický základ elektronických hlasovacích systémů. Tato práce je zaměřena na analýzu stávajících elektronických hlasovacích systémů za účelem identifikace jejich silných a slabých stránek. Na základě analýzy je navrženo možné zlepšení systémů online voleb a dostupnost potřebných k tomu technologií, popsány hlavní případy použití a uživatelské scénáře. Výsledkem práce je studie proveditelnosti, na jejímž základě je možné posoudit výhody a relevantnost vylepšení elektronických hlasovacích systémů navrženým způsobem.

Klíčová slova elektronické hlasování, studie proveditelnosti, volby, uživatelské scénáře, analýza rizik, elektronická demokracie

Abstract

Currently, the theoretical and practical basis of electronic voting systems are being actively developed around the world. This thesis focuses on the analysis of existing electronic voting systems to identify their strengths and weaknesses. Based on the analysis, possible improvements to electronic voting systems and the availability of the necessary technology to make them possible are offered, and the main use cases and usage scenarios are described. As a result of the thesis, a feasibility study is conducted to assess the benefits and relevance of improving electronic voting systems in the proposed manner.

Keywords electronic voting, feasibility study, elections, use cases, risk analysis, electronic democracy

Motivace

Aktivní rozvoj sféry informačních technologií ovlivnil mnoho oblastí našeho života, včetně vztahů mezi státem a občany. To vedlo k začátku přechodu hlasovacích systémů na digitální prostor. V danou chvíli se aktivně rozvíjí teoretická a praktická základna elektronického hlasování. To poskytuje širokou příležitost pro analýzu různých mechanismů elektronického hlasování v každé jednotlivé zemi, provádění srovnání, identifikaci společných a odlišných trendů a analýzu perspektiv rozvoje.

Volební proces je důležitou součástí každého státu a kvalita voleb přímo ovlivňuje procesy probíhající v zemi. Díky elektronickému hlasování mohou být volby transparentnější, spravedlivější a pohodlnější pro voliče, v důsledku čehož se v nadcházejících desetiletích může elektronické hlasování začít používat všude.

Cíl práce

Cílem teoretické části práce je analyzovat stávající elektronické hlasovací systémy a určit jejich silné a slabé stránky. Cílem praktické části práce je navrhnout zlepšení stávajících systémů elektronického hlasování a posoudit dostupnost technologií, které jsou k tomu nezbytné. Provést analýzu uživatelských požadavků a popsat klíčové uživatelské scénáře. Následně vypracovat studii proveditelnosti navrhovaného systému s cílem posoudit význam a přínosy zavedení vylepšení elektronických hlasovacích systémů.

Postup

Práce obsahuje dvě části. V první části je popsána teoretická stránka problematiky, kde jsou rozebrány základní pojmy týkající se elektronických hlasovacích systémů, zkušenosti s těmito systémy v evropských zemích s určením výhod a nevýhod jejich zavedení. Dále se teore-

tická část zabývá strukturou volebního systému v České republice a předpoklady pro zavedení elektronického hlasování v zemi.

Ve druhé části práce je navrženo zlepšení elektronického hlasovacího systému na základě předchozí analýzy a posouzena dostupnost potřebných technologií. Kromě toho jsou v této části popsány uživatelské požadavky a případy použití systému elektronického hlasování.

Poslední část práce je věnována vytvoření studie proveditelnosti navrhovaného systému a identifikaci hlavních rizik spojených s jeho zaváděním.

Výsledky práce

Zavedení vylepšení online hlasovacích systémů má značné výhody. Kromě toho navrhovaná funkcionality nevyžaduje řešení bezpečnostních otázek a všechny potřebné technologie pro její implementaci jsou k dispozici. Navrhovaná zlepšení jsou relevantní a doporučená pro zapojení do stávajících elektronických hlasovacích systémů.

Závěr

Vzhledem ke složitosti elektronických hlasovacích systémů a vysokým bezpečnostním požadavkům je zlepšení těchto systémů obecně náročné. V práci byly analyzovány zkušenosti s elektronickými volebními systémy a bylo zjištěno, že k očekávanému zvýšení volební účasti po zavedení online volebních systémů nedošlo. Proto byly v této práci navrženy vylepšení v podobě zavedení dalších funkcí, které by řešily problém nízké volební účasti. Posouzení dostupných technologií potřebných k zavedení nových funkcí přineslo pozitivní výsledek. V práci byly rovněž zkoumány uživatelské požadavky a scénáře pro online hlasovací systém s navrhovanými vylepšeními. Studie proveditelnosti ukázala, že zavedení nových funkcí do systémů elektronického hlasování je relevantní a doporučené.

Seznam zkratek

ID	Identity document
JVM	Java Virtual Machine
TLS	Transport Layer Security

Kapitola 1

Analýza

Systémy elektronického hlasování mají mnoho aplikací. Nejvíce patrné jsou státní volby. Ale elektronické volby vypadají logicky ve vzdělávání, společné správě majetku, a dokonce i v sociálním výzkumu. Tato práce se bude zabývat aplikací elektronického hlasování v kontextu státních voleb.

Na začátku jsou definovány důležité pojmy a principy, které se týkají systémů elektronických voleb a popsané některé legislativní omezení s tím spojené.

1.1 Úvod do elektronického hlasování

Hlasování se obvykle nazývá elektronické (označováno jako e-volby), když hlasovací proces využívá technické elektronické prostředky pro hlasování, sčítání hlasů a oznamování výsledku. Hlavní typy elektronického hlasování jsou [5]:

- E-volby: Při hlasování se používají elektronické přístroje instalované ve volebních místnostech nebo na obecních úřadech. Hlasování fyzicky sledují zástupci vlády nebo nezávislých volebních orgánů.
- Vzdálené e-volby: V procesu hlasování je za voliče odpovědný pouze on sám, představitelé státních orgánů jej fyzicky nesledují. Volič hlasuje na dálku pomocí digitálních technologií. Hlasování lze provádět z osobního počítače pomocí internetu (i-hlasování), pomocí mobilních telefonů, digitální televize a dalších technologií určených pro hlasování na dálku.

V kontextu této práce se pojem e-volby používá pro označení volebního procesu, který umožňuje voličům hlasovat vzdáleně prostřednictvím internetu.

Elektronické hlasovací systémy se zavádějí proto, aby se vyřešily problémy s tradičním papírovým hlasováním. Proto by tyto systémy měly být navrženy tak, aby byly v souladu s volebním zákonem a poskytovaly přinejmenším stejnou úroveň bezpečnosti a spolehlivosti jako demokratické volby a referenda, které neuvítají elektronické prostředky ve volebním procesu. Z toho vyplývá, že systém musí podporovat následující zásady volebního práva [10]:

- **Univerzálnost** - každý občan určitého věku má právo volit.
- **Rovnost** - volič nemůže hlasovat více než jednou a každý hlas má stejnou váhu.
- **Přímost** - volič nemůže přenést svůj hlas na třetí stranu, může hlasovat pouze přímo.
- **Tajnost** - Tento princip zahrnuje dva aspekty:

1. Anonymita - systém online hlasování musí zaručovat, že hlasy jsou a zůstanou anonymní a že není možné rekonstruovat spojení mezi voličem a hlasem.
2. Soukromost - systém by měl zajistit, aby byl volič chráněn před jakýmkoli nátlakem nebo ovlivňováním jeho volby.

Demokratický systém elektronického hlasování by navíc měl zajistit dostupnost, spolehlivost a bezpečnost. Kromě toho musí systém prokázat jasný přínos elektronického hlasování pro občany. Praxe elektronického hlasování však ukázala, že v současnosti dostupné technologie nejsou vždy schopny tyto požadavky plně splnit, protože zavedení takového systému je spojeno s mnoha bezpečnostními problémy.

1.1.1 Výzvy pro online hlasování

Během rozvoje elektronického hlasování se státy setkávají s řadou právních, politických a technických problémů. V této části práce jsou uvedeny základní problémy online hlasovacích systémů. Patří mezi ně nedostatek možností pozorovatelů, členů komise a kandidátů ověřit a zdokumentovat, že:

1. Volič se přihlásil k účasti ve volbách samostatně.
2. Volič hlasoval osobně a při hlasování na něj nikdo netlačil.
3. Na stránce hlasování a v místnosti, kde volič hlasuje, se neprovádí volební kampaň.
4. Hlas voliče byl správně započítán.
5. V žádné fázi přenosu dat nebylo s daty manipulováno.
6. Tajnost hlasování je dodržena, neboť elektronické volby předpokládají autorizaci uživatele v systému.
7. Mezi voličem a systémem pro záznam hlasů je zajištěno nepřerušované internetové spojení.
8. Systém je zabezpečen proti útokům.
9. V den hlasování byl použit stejný programový kód, který byl účastníkům voleb ukázán před začátkem hlasování.

Uvedené potenciální problémy elektronického hlasování na dálku nevypovídají o problematičnosti samotného elektronického hlasování jako formy vyjádření vůle voličů, ale pouze o určitých technických a organizačních obtížích. V současné době se země aktivně snaží tyto problémy řešit a některé z nich dosáhly určitého úspěchu.

Pro hlubší pochopení problematiky bude nejprve prozkoumán samotný volební proces. Jako příklad poslouží přehled volebního systému v České republice.

1.2 Přehled volebního systému ČR

Stejně základní principy svobodných voleb, které platí pro volební právo obecně, platí i pro volební právo v České republice.

V demokratickém právním státě je právo na účast ve volebním procesu základním lidským právem a jeho dodržování je zaručeno jak na mezinárodní úrovni prostřednictvím mezinárodních smluv a úmluv, tak na vnitrostátní úrovni prostřednictvím právních předpisů.

Listina základních práv a svobod stanovuje [2]:

1. Občané mají právo podílet se na správě veřejných záležitostí, a to buď přímo, nebo svobodnou volbou svých zástupců.
2. Volby se mohou konat pouze ve lhůtách stanovených zákonem.
3. Podle zákona, který stanoví podmínky výkonu volebního práva, je volební právo všeobecné a rovné a vykonává se tajným hlasováním.
4. Občanské právo na volené a jiné veřejné funkce musí být zajištěno za rovných podmínek.

V současné době existuje v České republice několik typů voleb: prezidentské volby, volby do dvou komor Parlamentu ČR, volby do zastupitelstev krajů a obcí a volby do Evropského parlamentu.

1.2.1 Schéma hlasování

Dle [11] volební proces lze popsat v několika fázích:

Identifikace

Identifikace je určení totožnosti neznámého objektu se známým objektem na základě shodných charakteristik. Při identifikaci osoby je třeba odpovědět na dvě otázky: kdo je daná osoba a co má jako důkaz, že je danou osobou.

Podle volebního zákona mají právo účastnit se voleb občané starší 18 let, kteří jsou zapsáni v seznamu voličů podle místa trvalého pobytu zapsaného v systému evidence obyvatel.

Aby mohl volič hlasovat, musí se dostavit do volební místnosti a prokázat svou totožnost cestovním pasem nebo občanským průkazem. Identifikace bude provedena na základě občanského průkazu a seznamu voličů, v němž byl oprávněný volič dříve zapsán. Po úspěšném provedení identifikace obdrží volič volební lístek. Z volebních zákonů vyplývá, že volič může hlasovat pouze osobně, bez možnosti přenést své hlasovací právo na třetí osobu. Může se však stát, že volič nebude schopen se do volební místnosti dostavit, např. bude v zahraničí nebo bude mít zdravotní omezení. Proto byly v zemi zavedeny voličské průkazy.

Voličské průkazy

Pokud se volič nemůže dostavit do určené volební místnosti, má právo požádat o vydání voličského průkazu v papírové podobě předem. Voličský průkaz slouží výhradně k hlasování a není to náhrada dokladu totožnosti. Volič proto musí u volební komise potvrdit svou totožnost předložením občanského průkazu nebo cestovního pasu. Po obdržení takového průkazu volič je vyškrtnut ze seznamu ve volební místnosti, která mu byla přidělena a může hlasovat v kterékoli jiné dostupné volební místnosti. Jakmile volič odevzdá svůj hlas, voličský průkaz bude komisí odebrán zpět, čímž se vyloučí možnost opakovaného hlasování v daných volbách.

Vlastní hlasování

Po prokázání totožnosti je voliči umožněno hlasovat a může hned odevzdat svůj hlas pro vybraného kandidáta. Pro dokončení hlasování vstoupí volič do kabiny za zástěnou, ve které se musí nacházet sam, vyplní svůj hlasovací lístek a vloží ho do obálky a vhodí jej do volební schránky. Na průběh hlasování dohlíží volební pozorovatelé, aby vyloučili možnost pochybení voličů a zajistila, že hlasování proběhne v souladu se zákonem.

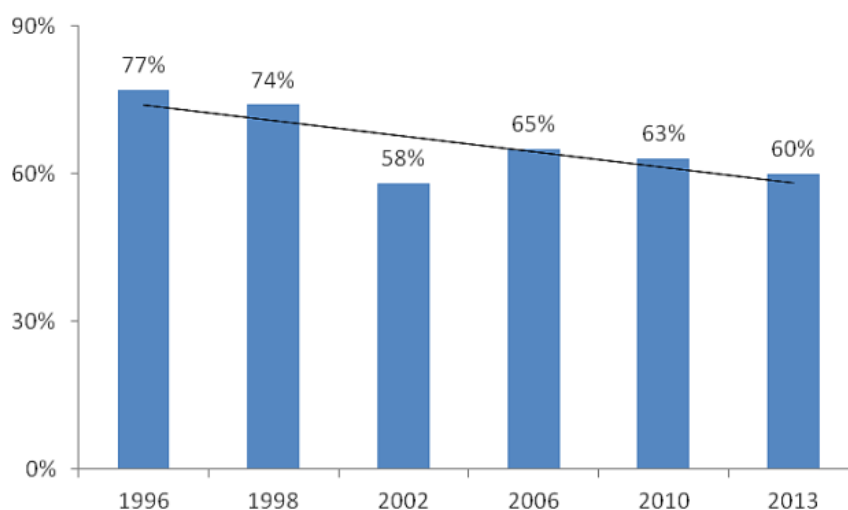
Hlasy odevzdané voliči jsou anonymní, takže není možné zjistit, jak volič hlasoval. Tímto způsobem je dodržována jedna z hlavních zásad demokratických voleb.

Hlasování do přenosné volební schránky Pokud se volič nemůže ze zdravotních nebo jiných závažných důvodů dostavit do volební místnosti, může požádat o hlasování pomocí přenosné hlasovací schránky. Volební schránku, obálku a hlasovací lístek voliči poskytne volební komise, která k voliči vyšle dva své členy. Hlasování tímto způsobem musí být v souladu se zákonem, takže hlasování musí zůstat tajné.

Sčítání hlasů

Sčítání hlasů probíhá po skončení hlasování. Členové volební komise sčítají hlasy z volební urny ručně. Svou roli zde hraje lidský faktor, protože sčítání vyžaduje čas a úsilí členů komise, nelze si být jistý, že všechny hlasy budou sečteny přesně. Výsledky sčítání se zasílají volební komisi nejvyššího stupně a nakonec Českému statistickému úřadu.

1.2.2 Volební účast



■ **Obrázek 1.1** Volební účast u voleb do Poslanecké sněmovny, zdroj:

<https://ihned.cz/c1-61774220-o-volebni-ucasti-aneb-proc-ne-chodime-k-volbam>. Přístup 16.05.2021

Vysoká volební účast je důležitým ukazatelem demokratických voleb, zatímco nízká účast spíše svědčí o slabé legitimitě politiků a samotného systému.

Tady je stručný přehled statistiky volební účasti ve volbách do Poslanecké sněmovny Parlamentu ČR a prezidentských voleb, které jsou mezi voliči nejoblíbenější. Graf (viz Obrázek 1.1) ukazuje statistiky volební účasti u voleb do Poslanecké sněmovny v letech 1996 až 2013. Je vidět, že účast v průběhu let klesá. Ve volbách po roce 2013 a doposud účast se stabilizovala a pohybovala se kolem 60 %.

Největší účast v danou chvíli mají prezidentské volby, tam je to o něco více než 60 %. [7]

Ostatní volby

[7]

Komunální volby jsou pro voliče zajímavější, protože jejich kandidáti jsou blíže lidem. Volený zástupce řeší problémy, které se přímo dotýkají občanů žijících v určitých městech a obcích. Procento voličů je však poměrně nízké a pohybuje se v průměru kolem 50 %.

O senátní volby měli voliči od počátku malý zájem. První volby se konaly s účastí 30 % a v dalších letech se účast jen snižovala.

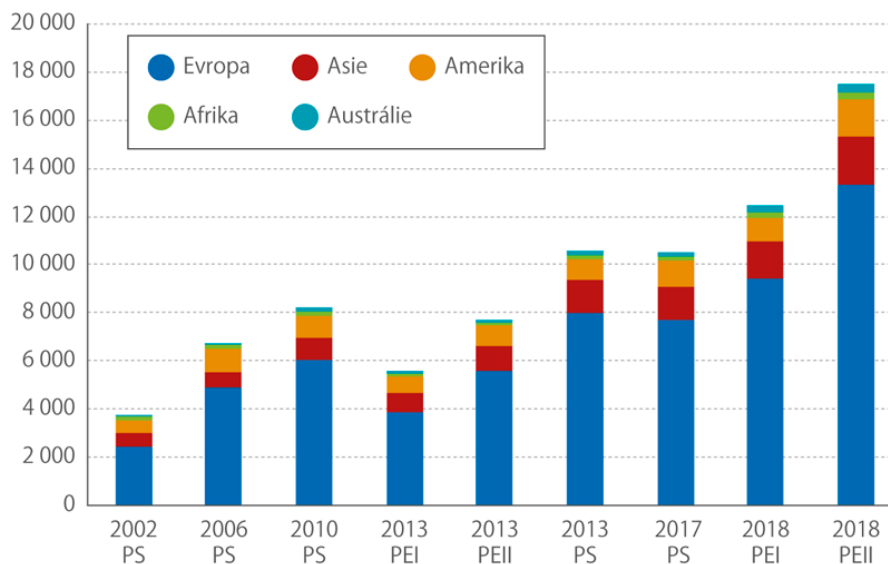
První regionální volby se konaly v roce 2000 s účastí 34 %, další volby v roce 2004 s účastí 30 %, v roce 2008 se 40 % a v roce 2012 s 37 %. Zde došlo k mírnému nárůstu, ale procento je stále příliš nízké.

Nejnižší volební účast je u voleb do Evropského parlamentu a to kolem 23 %.

Volby v zahraničí

[8]

Od roku 2002 se mohou občané České republiky účastnit ve volbách do Poslanecké sněmovny a od roku 2003 i prezidentských voleb ze zahraničí. Podle statistik Českého statistického úřadu (viz Obrázek 1.2) je vidět, že volební účast občanů v zahraničí každoročně roste. Zároveň se zvyšuje jejich podíl na celkovém počtu voličů, kteří se účastní voleb. V případě prezidentských voleb to ovlivňuje konečný výsledek v malé míře, protože tyto volby jsou jednomandátové. Ve volbách do Poslanecké sněmovny však mohou hlasy ze zahraničí výrazně ovlivnit výsledek, protože volby jsou vedeny na principu proporcionálního zastoupení ve volebních obvodech na území České republiky. Pokud by ve volbách do Poslanecké sněmovny nebyly započítány hlasy ze zahraničí, změnilo by to výsledek tří z pěti voleb, v nichž bylo dosud možné hlasovat ze zahraničí.



■ **Obrázek 1.2** Počet vydaných obálek v zahraničí podle roku, zdroj: <https://www.czso.cz/>

Nedostatky papírového hlasování

Tradiční papírové hlasování nespĺňuje očekávání moderní společnosti a navíc má některé nevýhody:

- Dnes stále více služeb umožňuje provádět různé transakce přes internet. Vzhledem k tomu se papírové hlasování jeví jako zastaralé, což vede k menšímu zájmu mladých lidí o volební systém a k poklesu volební účasti.
- Hlasování ve volebních místnostech znamená, že volič se tam musí dostavit osobně, aby mohl hlasovat. To však může být problematické pro občany, kteří jsou v zahraničí, mají zdravotní omezení nebo nemají čas.
- Proces hlasování zahrnuje zpracování velkého množství dat. Ukládání dat v papírové podobě

je nepraktické, vyžaduje mnoho času a úsilí při zpracování. Kromě toho se papírové hlasy sčítají ručně, což může vést k nežádoucí manipulaci s hlasy nebo k chybám při sčítání.

- Tisk hlasovacích lístků, přidělení velkého počtu volebních místností a komisí, jakož i prostor pro uložení hlasů vyžadují značné finanční náklady.

1.3 Zkušenosti s elektronickými volbami ve světě

V předchozí části této práce byl zkoumán proces hlasování v České republice, který obsahuje tři hlavní fáze: identifikaci, hlasování a sčítání hlasů. Při elektronickém hlasování prochází volič stejnými fázemi jako při tradičním hlasování, ale samotné mechanismy se mění díky digitalizaci procesu. Počet fází online hlasování však může být i vyšší, například ověření, zda byl hlas správně započítán.

Tato část práce se bude zabývat analýzou několika elektronických hlasovacích systémů, včetně klíčových principů a stručného přehledu hlasovacího schématu. Na základě uvažovaných systémů budou určeny jejich silné a slabé stránky.

1.3.1 Estonsko

Jedním z neúspěšnějších příkladů využití systému elektronického hlasování je systém v Estonsku a proto hlasování v této zemi se proto budeme věnovat podrobněji.

V globálním žebříčku OSN, který hodnotí vývoj elektronických služeb a infrastruktury, zaujímá Estonsko třetí místo na světě. V tuto chvíli lze téměř vše v zemi provést přes internet. Jedním z důvodů tohoto úspěchu je skutečnost, že v roce 2000 přijal estonský parlament zákon, který uznává přístup k internetu jako nezczitelné lidské právo. Vláda pokryla většinu lokalit bezplatným Wi-Fi, v důsledku čehož se mnoho veřejných služeb pro občany a podniky stalo digitálním. [1] V danou chvíli 91,6 % obyvatel pravidelně používá internet.

O zavedení elektronického hlasovacího systému se začalo diskutovat v roce 2001. Za účelem realizace této myšlenky se v roce 2002 začaly v zemi vydávat ID karty s čipem. V roce 2005 se v zemi konaly první elektronické volby na komunální úrovni. Během referenda o umístění Památníku svobody, v němž bylo možné hlasovat online, odevzdalo svůj hlas online 14 % z celkového počtu voličů. a v roce 2007 se v Estonsku konaly první elektronické volby na celostátní úrovni. [6]

ID karta

ID karta v Estonsku (viz Obrázek 1.3) je primární doklad totožnosti. Karta má zabudovaný elektronický čip, který kromě informací o držiteli uchovává také informace o kryptografických klíčích (veřejných a soukromých) a certifikátech. Identifikační karta umožňuje bezpečné vzdálené ověřování, digitální podpis a šifrování a dešifrování souborů za účelem bezpečného doručení. V roce 2000 byl v Estonsku přijat zákon o digitálním podpisu, podle něhož je elektronický digitální podpis právně ekvivalentní podpisu vlastnoručnímu. Karty slouží také jako digitální průkaz totožnosti pro získání veřejných služeb prostřednictvím internetu nebo internetového bankovníctví. Dnes v Estonsku 91,6 % obyvatel má elektronický občanský průkaz.

V systémech elektronického hlasování se čipové karty používají pro bezpečnou identifikaci voličů, autentizaci a pro podepisování a šifrování hlasů. Aby mohl volič hlasovat přes internet, musí mít ID kartu, počítač s přístupem na internet a speciální čtečku karet. [6]

1.3.1.1 Koncept elektronického hlasování

Elektronické hlasování je dobrovolní

Elektronické hlasování není povinné, volič může hlasovat i tradičním papírovým způsobem, protože elektronické hlasování je v zemi považováno jenom za doplňkový způsob voleb. E-volby



■ **Obrázek 1.3** Estonská digitální ID karta, zdroj: <https://taltech.ee/en/estonian-id-card/>. Přístup 14.05.2021

nemají nahradit tradiční formu hlasování ve volebních místnostech.

Identifikace

Identifikace voliče probíhá pomocí ID karty s čipem.

Vícenásobné hlasování

Voliči mohou v systému e-voleb hlasovat několikrát a změnu volby lze provést mezi desátým a čtvrtým dnem před volebním dnem, ale započítává se pouze konečné hlasování. Každý hlas digitálně podepsán a opatřen elektronickým časovým razítkem. Voliči mají také právo hlasovat v den voleb osobně ve volební místnosti, čímž se zneplatní všechny dříve odevzdané elektronické hlasy.

Priorita tradičního hlasování

Voliči, kteří hlasovali online, mají možnost navštívit volební místnost a vyplnit tradiční papírový hlasovací lístek. Hlasování v papírové podobě má vyšší prioritu než hlasování online. [6]

Schéma elektronického hlasování

Proces elektronického hlasování v Estonsku lze rozdělit do následujících fází [9]:

1. Pro účast v internetovém hlasování vstoupí volič do systému pomocí ID karty a prvního PIN kódu, hlasuje pro vybraného kandidáta a zadá druhý PIN kód, čímž potvrdí hlasování digitálním podpisem. Takto je hlas šifrován a digitálně podepsán ve schématu „dvojitě obálky“. Schéma „dvojitě obálky“ zahrnuje vnitřní obálku a vnější obálku, která převádí jména voličů na náhodný řetězec znaků pomocí šifrovacího algoritmu. K dešifrování tohoto řetězce se používá algoritmus stanovený volební komisí. Důvěrnost hlasování zajišťuje vnitřní obálka, zatímco vnější obálka zaručuje, že hlas odevzdal občan oprávněný volit.
2. Podepsaný a zašifrovaný hlas se odesílá zabezpečeným spojením založeným na protokolu TLS do digitální hlasovací schránky. Hlasy zůstávají zašifrované až do ukončení voleb. Systém

používá digitální podpis k ověření pravosti hlasu a poté jej odstraní, aby ochránil anonymitu hlasujícího.

Protokol TLS používá k navázání spojení mezi počítačem voliče a volebními servery symetrické šifrování. Tento protokol zajišťuje šifrování, ověřování a integritu. Aby bylo možné vytvořit kryptograficky bezpečný datový kanál, musí se hlasovací zařízení a server dohodnout na používaných šifrovacích metodách a klíších.

3. Po skončení volebního období a zaznamenání všech hlasů začíná fáze míchání, během níž jsou hlasy anonymizovány, což ztěžuje opětovné přiřazení hlasu k jeho digitálnímu podpisu. Systém odstraní vnější obálky od hlasů a otevře vnitřní obálky, čímž získá zašifrované hlasy. Výsledné hlasy se zamíchají, aby randomizovat pořadí, v jakém byly podány. Směšování se provádí tak, že se zašifrované hlasy předávají přes směšovací síť. V této síti jsou hlasy smíchány na třech až pěti úrovních serverů nebo uzlů. Každý směšovací uzel hlasy přeskupí a znovu zašifruje a náhodným způsobem předá je jako vstup dalšímu uzlu.
4. Po smíchání jsou hlasy přeneseny na dešifrovací server, což je počítač bez fyzického nebo bezdrátového připojení k nezabezpečeným systémům a sítím. V této fázi jsou hlasy připraveny k počítání. Hlasy lze dešifrovat pouze pomocí soukromého klíče, který je vygenerován kvorem členů volební komise a je mezi nimi rozdělen. Klíč je možné použít k dešifrování pouze v případě, že jsou k dispozici všechny jeho části.
5. V poslední fázi jsou dešifrované hlasy spočítány serverem bez fyzického nebo bezdrátového připojení k internetu nebo jiným částem systému.

Kontrola zápisu hlasu

Volič má možnost zkontrolovat správnost zápisu svého hlasu. K tomu slouží speciální QR kód, který vygeneruje aplikace, jejímž prostřednictvím uživatel hlasoval.

QR kód je zakódován pomocí náhodného čísla, které bylo vygenerováno v počítači voliče během hlasování, a identifikátoru, který server přidělil po zpracování hlasu voliče. Náhodné číslo spolu s údaji o volbě voliče bylo předem odesláno na server volební komise. A to v podobě šifrogramu zakódovaného veřejným klíčem serveru volební komise.

Volič přes mobilní aplikaci naskenuje QR kód na obrazovce počítače, zjistí identifikátor a vyžádá si s ním šifrogram zasláný volební komisí. Aplikace tedy vytvoří šifrogram pro každého z kandidátů a provede porovnání jej s šifrogramem obdržným od volební komise, najde jedinou shodu. [4] Na základě ověření obdrží volič potvrzení, že jeho hlas byl úspěšně přijat a zpracován volební komisí.

Volební účast

V tabulce (viz Tabulka 1.1) jsou uvedeny statistiky volební účasti v Estonsku od roku zavedení online hlasování v zemi. Údaje v tabulce se týkají různých typů voleb, protože mají pro občany různý význam, takže je nelze hodnotit společně. Statistiky ukazují, že používání elektronických voleb získává na popularitě, přičemž podíl voličů hlasujících online se od roku 2005 do roku 2019 zvýšil o více než 40 %. Očekávalo se, že použití elektronického hlasování zvýší celkový počet hlasů, ale výsledky to nepotvrzují.

1.3.2 Norsko

Myšlenka zavést v Norsku elektronické volby se objevila v roce 2009. V 2011 se v zemi konaly pilotní volby, které dopadly úspěšně a systém byl schválen parlamentem. Online hlasování proběhlo v komunálních a krajských volbách v 10 vybraných obcích a 17 % z celkového počtu voličů využilo možnost online hlasování. Ve volbách v roce 2013 byl proto tento systém znovu

■ **Tabulka 1.1** Volební účast v jednotlivých volbách v Estonsku od roku 2005.

Zdroj dat: <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/>

	2005 Místní	2007 Parlament	2009 EP	2013 Místní	2017 Místní	2019 Parlament	2019 EP
Volební účast celkem	47,4 %	61,9 %	43,9 %	58,0 %	53,3 %	63,7 %	37,6 %
Poměr online hlasů ke všem hlasům	1,9 %	5,5 %	14,7 %	21,2 %	31,7 %	43,8 %	46,7 %

použit ve 12 volebních okrscích, tentokrát prostřednictvím internetu hlasovalo 36 % voličů z celkového počtu voličů, které se k volbám dostavily.

Proces zavádění online hlasovacího systému byl však zastaven, protože voliči se obávali, že by se jejich hlasy mohly stát veřejnými, což by narušilo samotnou myšlenku demokratických voleb. Považuje se, že norský systém potřebuje modernizaci, protože volby v roce 2013 byly kontroverzní, neboť bezprostředně před volbami byla kritizována šifrovací schémata používaná k ochraně hlasů zasílaných po síti.

Hlavní principy systému [3]:

- Zajištění transparentnosti systému prostřednictvím otevření zdrojového kódu.
- Plná integrace se stávajícími norskými metodami ověřování, autorizace pomocí elektronického identifikátoru MinID.
- Vícenásobné hlasování
- Ověřitelnost systému zajišťuje, že voliči mohou ověřit, že jejich hlas byl odevzdán pro kandidáta, pro kterého hlasovali.

MinID

Elektronický systém MinID umožňuje elektronickou identifikaci, aby bylo možné bezpečně přistupovat k široké škále online služeb různých státních institucí v Norsku. K ochraně informací uživatelů se používá šifrování komunikace se systémovým serverem. Uživatel, který chce být oprávněn používat MinID, musí mít národní identifikační číslo.

Prvky systému [3]:

- Služba sběru hlasů (VCS): Poskytuje úložiště pro zašifrované hlasy.
- Generátor návratového kódu (RCG): Generuje návratový kód, na jehož základě volič ověří, že jeho hlas byl správně započítán a vložen do elektronické hlasovací schránky.
- Služba správy klíčů (KMS): Odpovídá za šifrovací klíče a provádí jejich vytváření a distribuci, včetně vytváření soukromého klíče, který se používá ve fázi dešifrování hlasů.

Norský systém elektronického hlasování využíval standardní schéma online hlasování s doplněním dvou nezávislých kanálů, jako je pošta a SMS. Přítomnost těchto kanálů v systému zvyšuje bezpečnost, protože útok na dva kanály najednou je obtížně proveditelný.

Schéma elektronického hlasování

Volič se přihlásí do volební aplikace a prostřednictvím MinID se identifikuje. Pokud je identifikace úspěšná a volič je zapsán v seznamu voličů, může přistoupit k hlasování. Uživatel si prostřednictvím aplikace vybere volby, ve kterých chce hlasovat, a hlasuje pro vybraného kandidáta nebo mění svůj hlas, pokud již hlasoval dříve. Systém také umožňuje odeslat hlas bez uvedení kandidáta.

VCS zkontroluje hlasy a zašle je RCG. RCG vygeneruje návratový kód a odešle jej voliči ve formě SMS zprávy. VCS uloží zašifrovaný hlas do elektronické hlasovací urny.

Na konci voleb se elektronická volební urna exportuje do systému pro sčítání hlasů. Hlasy voličů, kteří kromě elektronického hlasování hlasovali i v papírové podobě, jsou odstraněny, zbývající hlasy jsou smíchány pomocí sítě mixnet. V posledním kroku se spočítají platné elektronické hlasy. [3]

1.4 Výhody a nedostatky e-voleb

Elektronické hlasování je dalším nevyhnutelným krokem ve vývoji volebních systémů. Stávající "papírový" volební systém není neměnným měřítkem - je spíše kompromisem mezi plně centralizovaným řízením a přímou demokracií starověkého řeckého modelu, což je složitý a nákladný způsob, jak zjistit názor občanů země. Přestože má systém dálkového hlasování řadu zjevných výhod, je třeba vyřešit řadu důležitých problémů, a to jak technických, tak sociálních, než bude možné jej zavést v měřítku státu. Mezi výhody patří:

- Snadné hlasování ze zahraničí.
- Snížení pracovní zátěže členů volebních komisí.
- Odstranění nebo snížení množství papírové dokumentace.
- Automatizace procesu sčítání hlasů (ale to nezamítá otázky, jak zajistit transparentnost a spravedlnost voleb.
- Přesnost systému při sčítání hlasů.
- Možnost kontroly správnosti odevzdaného hlasu.

Více o výše uvedeném.

Zřejmou výhodou je možnost volit mimo volební místnosti a volební okrsky za známých podmínek. Tím se otevírá možnost pokrýt značné množství občanů:

- V odlehlých nebo nepřístupných oblastech.
- Občané se sníženou pohyblivostí a zdravotním postižením
- občané pracující mimo stát.

Systém umožňuje přístup k informacím, a dává tak mladým lidem příležitost pochopit, jak funguje politický systém, k čemu jsou volby a jak důležitý je hlas každého občana.

Důležitým faktem je, že to bude stát mnohem méně než obvyklý formát voleb. Vzhledem k nižším nákladům na zaměstnance zajišťujících průběh voleb a snížení množství papírových dokumentů. V podmínkách nadcházejících krizí je to velmi důležité. Zvyšuje se rychlost a přesnost sčítání hlasů a následně i výsledků hlasování.

Pokud jde o nevýhody používání elektronického hlasovacího systému:

- Nedůvěra uživatelů v nový systém.
- Nedostatečná technická vybavenost občanů.
- Svobodný projev vůle a tajnost hlasování.
- Problém s zabezpečením informací v procesu.
- Nedostatečné zabezpečení identifikace voličů.

- hybějící připojení k internetu.

Lidé se zcela jistě obávají nového systému hlasování kvůli nemožnosti zkontrolovat, kam svůj hlas odevzdali. Důvěra však není jedinou překážkou na cestě k zavedení nového systému; navzdory rostoucímu počtu uživatelů moderních přístrojů stále existuje mnoho lidí, kteří si příslušný přístroj nemohou dovolit nebo ho prostě nechtějí.

Dalším bodem je zabezpečení dat. Nikdo nemůže zaručit úplné zabezpečení serverů, které obsahují potřebné informace.

Aby se zabránilo falšování údajů nebo neoprávněným zásahům, vytvořila estonská vláda v Lucemburku depozitář záložních kopií všech karet. Ani to však neposkytuje stoprocentní záruku ochrany. U elektronického hlasování také není možné ověřit svobodnou vůli voliče, stejně jako není možné mít jistotu, že hlasovala právě tato osoba. Nadále přetrvávají otázky ohledně transparentnosti sčítání hlasů na sčítacích serverech. Kromě toho je při elektronickém hlasování prakticky nemožné provést přepočítání hlasů.

Během analýzy systémů elektronického hlasování bylo také zjištěno, že navzdory očekávanému zvýšení volební účasti nedošlo k žádnému nárůstu.

1.5 Důvody nízké volební účasti

Efektivita politického systému do značné míry závisí na úrovni politické participace občanů, na potenciálu jejich porozumění, formování jejich zájmů, přání a schopnosti uplatnit svá volební práva. Spravedlivé volby s vysokou volební účastí jsou nedílnou součástí každého demokratického systému, neboť poskytují obyvatelům možnost rozhodovat o vývoji státního zřízení a země, které důvěřují. Nicméně světový trend posledních desetiletí ukazuje, že počet občanů, kteří se účastní voleb, klesá. Tento trend je potenciální hrozbou pro demokratický systém. Nejčastější důvody neúčasti voličů ve volbách:

- Názor, že jejich volba nic nezmění.
- Nízká důvěra ke státním orgánům.
- Jistota vítězství prioritního kandidáta.
- Malý zájem o politiku.
- Nejistota při výběru kandidáta.

Návrh zlepšení systému elektronických voleb

Spousta služeb, které se dříve poskytovaly pouze offline, byly časově náročné a byrokratické, se nyní poskytují online. Kromě snadného používání a úspory času se díky přechodu na online prostředí také zvýšila funkčnost a dostupnost řady služeb. V předchozí části byly probrány příklady zemí, které mají zkušenosti s elektronickými volebními systémy. V současné době nabízí internetové hlasování voličům jen málo dalších funkcí nad rámec těch, které poskytuje tradiční způsob hlasování. Informační technologie však umožňují rozšířit možnosti systému elektronického hlasovacího systému a zavést změny, které by bylo obtížné provést při standardním způsobu hlasování.

Jedním z očekávaných přínosů zavedení elektronického hlasování byla vyšší volební účast. Analýza zkušeností s online hlasovacími systémy v různých zemích takový výsledek neprokázala. Zájem o elektronické hlasování mezi voliči roste a počet voličů, kteří hlasují online, se zvyšuje, ale na zvýšení celkové volební účasti to má malý nebo žádný vliv.

Z teoretické analýzy lze vyvodit závěr, že zavedení elektronického hlasování v současné podobě nemůže výrazně zvýšit volební účast. Důvodem je, že systém neřeší problémy voličů, kteří nevěří, že jejich hlas něco změní, mají malý zájem o politiku a nedůvěřují kandidátům. Protože takových občanů je poměrně hodně a celková volební účast ve většině zemí není pro demokratický systém dostatečně přijatelná, bylo rozhodnuto zavést do elektronického volebního systému další funkce, které by přilákaly k volbám více občanů.

2.1 Odůvodnění zavedení nových funkcí

Pro voliče, který kandidáty nezná, je volba nového představitele moci poměrně netriviální problém. Na základě informací získaných z různých zdrojů je obtížné se rozhodnout a udělat si představu o kandidátovi v souladu se skutečností. Zvolený zástupce často může nespĺňovat původní očekávání voličů. Na tomto základě vzniká potřeba systému, který by umožňoval voliči nejen zvolit zástupce vlády, ale také se dozvědět více o jeho vládní činnosti, účastnit se diskusí o návrzích zákonů předložených zvolenými úředníky, navrhnout pozměňovací návrhy a předkládat vlastní návrhy zákonů a to při zachování principů volebních systémů a práv občanů. Zavedení takového systému zlepšit interakci občanů se státem, potenciálně zvýší volební účast a zájem o politiku.

2.2 Analýza požadavků

V této části jsou popsány hlavní funkční a nefunkční požadavky na systém.

2.2.1 Funkční požadavky

- Bezpečná autentizace uživatelů.
- Bezpečné volební hlasování.
- Kontrola odevzdaného hlasu.
- Zobrazení konečných výsledků a statistik.
- Tvorba návrhů a účast na diskusích.
- Hlasování o návrzích vytvořených jinými uživateli.
- Vytváření a odesílání petic příslušným úřadům.
- Absolvování profilových testů.
- Vyhledávání stávajících právních předpisů a návrhů uživatelů podle filtru.
- Administrativní prostředí umožňující vytvářet volby, upravovat informace o kandidátech a testy.

2.2.2 Nefunkční požadavky

- Online přístup z počítače nebo notebooku prostřednictvím prohlížečů Microsoft EDGE, Mozilla Firefox, Google Chrome, Opera a Safari ve verzích aktuálních v momentě nasazení systému.
- Uživatelské rozhraní by mělo být jednoduché a srozumitelné.
- Provedení více voleb ve stejný okamžik.
- Zpracování tisíců uživatelských požadavků v jeden okamžik.
- Dostupnost systému 99,9 % 24/7, zejména v době voleb.
- Rychlá odezva systému.
- Systém musí být snadno rozšiřitelný v případě, že budou v budoucnu zavedeny nové funkce.
- Absence chyb, které by kriticky ovlivnily systém.
- Video a textové materiály pro uživatele o způsobu používání systému.
- Hlasovací systém by měl být bezpečný a spolehlivý

2.3 Popis řešení

Hlavním účelem systému je poskytnout voličům možnost uplatnit své volební právo v online prostředí, sledovat kroky výkonné moci a podílet se na veřejném rozhodování. Pro dosažení těchto cílů je třeba do systému zavést další funkce.

Struktura navrhovaného systému:

- Volby
- Diskuse
- Testování

Volby

Volební modul umožňuje voliči, který byl identifikován a je zapsán v seznamu voličů, uplatnit své volební právo na kterékoli úrovni veřejné správy. Volby proběhnou v zákonných lhůtách elektronicky. Kromě toho bude mít každý volič možnost seznámit se s biografií, programem kandidátů a jejich dosavadní činností. Jakmile se kandidát nastoupí do funkce, lze v systému sledovat jeho aktivity, úspěchy a prohlížet si jeho návrhy zákonů.

Tato část systému je zaměřena především na hlasování. Vzhledem k tomu, že potřebná funkcionalita odpovídá stávajícím systémům elektronického hlasování a zůstává nezměněna, nebude v práci popisována architektura a implementace této části, neboť za základ bude vzat model systému elektronického hlasování v Estonsku, který se úspěšně používá již řadu let.

Diskuse

Výběr nejlepšího kandidáta z pohledu voliče nezaručuje, že volič bude spokojen s jeho následnou činností a návrhy zákonů. Občané proto mohou ovlivňovat jeho práci tím, že navrhnou nové návrhy zákonů a změny návrhů zákonů, které pak mohou být zohledněny při přijímání nebo změně návrhu zákona příslušným státním orgánem. V této sekci se volič může zúčastnit národní diskuse o návrzích zákonů, které projednávají zákonodárné orgány státu. Někdy se projednávají návrhy zákonů týkající témat, o kterých je skutečně třeba mít znalosti, nejlépe s vysokoškolským vzděláním v daném oboru. To může být problém pro lidi, kteří nemají dostatečné znalosti, ale chtějí se zapojit do politického života země. To může vést k velkému množství návrhů a pozměňovacích návrhů, které nejsou ničím podloženy. K vyřešení tohoto problému bude umožněno projednávat a navrhovat projekty zákonů všem občanům země, kteří složili speciální profilové zkoušky potvrzující jejich způsobilost v oblasti, které se daný návrh zákona týká.

Každý občan bude moci hlasovat o návrzích zákonů, pozměňovacích návrzích a stížnostech navržených jinými občany. Nejvýznamnější z nich budou předloženy příslušným orgánům ve formě elektronické petice, která bude posouzena a zohledněna při přípravě návrhů zákonů. O konečné podobě návrhu zákona rozhoduje orgán odpovědný za tento proces.

Testování

Vzhledem k tomu, že systém navrhuje větší zapojení občanů do politiky, je třeba zajistit, aby každý občan, který se účastní diskusí a návrhů zákonů, měl dostatečnou gramotnost a odpovědnost. Obvykle se jedná o důležitá a složitá témata, která ovlivňují život celé země. Proto musí každý občan prokázat své znalosti v tématech (např. ekonomie, finance, ekologie), kterých se daný návrh zákona týká, a to prostřednictvím profilového testu, který bude zahrnovat nejpodstatnější otázky z dané oblasti. Systém umožňuje po určité době test opakovat. V případě neúspěchu v testu může uživatel absolvovat online školení na dané téma a zkusit to znovu. V případě úspěšného absolvování testu se uživatel může účastnit diskusí a navrhovat návrhy zákonů, pozměňovacích návrhů a stížností ke všem otázkám souvisejícím s tímto tématem.

Takový přístup zvýší kvalitu a sníží počet unáhlených návrhů zákonů a pozměňovacích návrhů.

2.3.1 Dostupnost potřebných technologií

Tato práce se zabývá možností vylepšení online hlasovacích systémů přidáním nových funkcí do stávajících systémů. Na základě analýzy systémů online voleb v teoretické části práce lze konstatovat, že online hlasovací systémy poměrně úspěšně využívají dostupné technologie. Volební modul bude implementován stejným způsobem jako stávající online hlasovací systémy, dostupnost technologie pro jeho implementaci nebude v této práci zvažována. Systémy s potřebnými funkcemi již byly zavedeny a aktivně se používají, takže dostupnost potřebných technologií je prokázána.

Ostatní části navrhovaného systému nejsou závislé na modulu pro hlasování ve volbách, proto budou technologie nezbytné pro jejich implementaci posuzovány samostatně. Obrázek (viz Obrázek 2.1) ukazuje architekturu navrhovaného řešení bez zohlednění volebního modulu. Tato architektura obsahuje tři klíčové komponenty nezbytné pro správné fungování systému, konkrétně: databázi, aplikační jádro a webovou aplikaci.

Databáze

Uvažovaná část systému bude zpracovávat velké množství informací. Systém by měl například uchovávat informace o registrovaných uživateli, biografii kandidátů, návrhy uživatelů a výsledky testování. Pro tyto účely je nutné používat databázi. Na rozdíl od volebního modulu nejsou ukládaná data kritická, takže na databázi nejsou kladeny žádné zvláštní požadavky. Kromě toho není potřeba velká propustnost databáze. Na základě toho bylo pro ukládání dat v systému rozhodnuto použít objektově-relační databázi PostgreSQL. Dlouhodobá praxe používání této technologie ve světě ukázala její dostatečnou spolehlivost a dobré výkonové charakteristiky. Navíc je tato technologie poskytována zdarma.

Aplikační jádro

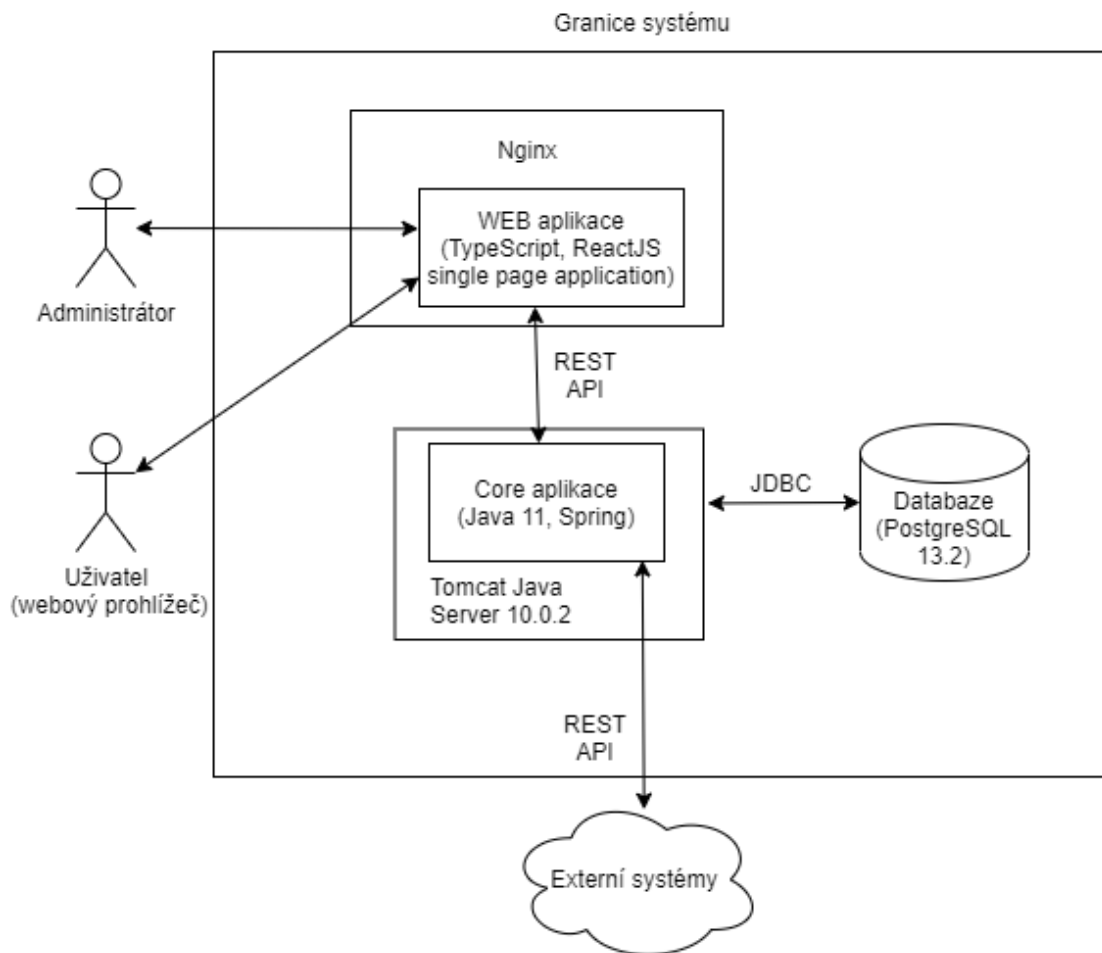
Aplikační jádro je zodpovědné za veškerou business logiku systému, přihlašování do systému, integraci s externími službami (např. integrace se státními registry obsahujícími informace potřebné pro systém), odesílání vytvořených petic. Pro realizaci této komponenty se nabízí použití Javy 11, Spring 5.3.8. Spring usnadňuje tvorbu firemních aplikací Javy. Poskytuje vše potřebné pro použití Javy v korporáčním prostředí s podporou Groovy a Kotlinu jako alternativních jazyků pro JVM a flexibilitou pro vytváření různých architektur v závislosti na potřebách aplikace.

Aplikace je nabízena ke spuštění na open-source Java serveru Tomcat. V porovnání s produktem Tomcat nabízejí komerční produkty obvykle vyšší spolehlivost a lepší zabezpečení. Tomcat naproti tomu nabízí jednoduchost, přehlednost, menší nároky na výpočetní výkon a mnohem rychlejší vývoj.

Webová aplikace

Webová aplikace je hlavním a jediným grafickým uživatelským rozhraním systému, jehož prostřednictvím uživatel komunikuje s prvky elektronického systému. Způsob interakce s rozhraním bude podrobněji popsán v uživatelských scénářích systému. Pro jeho implementaci se navrhuje použít populární open-source technologii TypeScript. TypeScript umožňuje rychleji a snadněji psát rozsáhlé komplexní programy a odpovídajícím způsobem usnadňuje jejich údržbu, vývoj, škálování a testování než standardní JavaScript. Je také multiplatformní, což znamená, že pro vývoj můžete používat jak systém Windows, tak MacOS nebo Linux.

Jako nástroj pro nasazení webového serveru bude použit Nginx. Webový server Nginx je ve srovnání s Apachem rychlejší při poskytování statických dat a spotřebovává méně serverových prostředků. Webový server Apache sice nabízí více funkcí, ale v kontextu tohoto systému budou možnosti Nginxu dostačující.



■ **Obrázek 2.1** Architektura navrhovaného řešení

2.4 Případy užití a uživatelé systému

V této části práce budou popsány typy uživatelů systému z hlediska práv, která v systému mají, a procesy, kterými uživatel prochází, aby dosáhl cíle prostřednictvím navrhovaného systému.

2.4.1 Uživatelé a jejich práva v systému

Přihlášený uživatel

Úspěšné absolvování testu odborné způsobilosti rozšiřuje možnosti autentizovaného uživatele, takže navíc má právo:

- Prohlížet informace o kandidátech a zmocněncích.
- Prohlížet návrhy a pozměňovací návrhy k návrhům zákonů předloženým jinými uživateli.
- Hlasovat o pozměňovacích návrzích a návrzích zákonů.
- Absolvovat profilové testy a školící materiály.
- Prohlížet konečné výsledky voleb.

- Účastnit se diskusí.
- Vytvářet vlastní návrhy zákonů a pozměňovací návrhy.

Poslední dvě položky jsou uživateli k dispozici pouze v těch tematických kategoriích, v nichž uživatel potvrdil svou kompetenci.

Autentizovaný a přihlášený uživatel

Autentizovaný uživatel, který vhodným způsobem (např. národní id karta s čipem) potvrdil svou totožnost, navíc k výše popsaným právům má další práva:

- Účastnit se hlasování pro kandidáta.
- Ověřit správnosti přijetí zasláného hlasu.

Administrátor

Administrátor je člen volební komise, což je zvláštní typ autentizovaného uživatele. Má přístup do administrační části systému s následujícími právy:

- Upravování informací o kandidátech a zmocněncích.
- Vytvoření volebního hlasování.

Anonymní uživatel

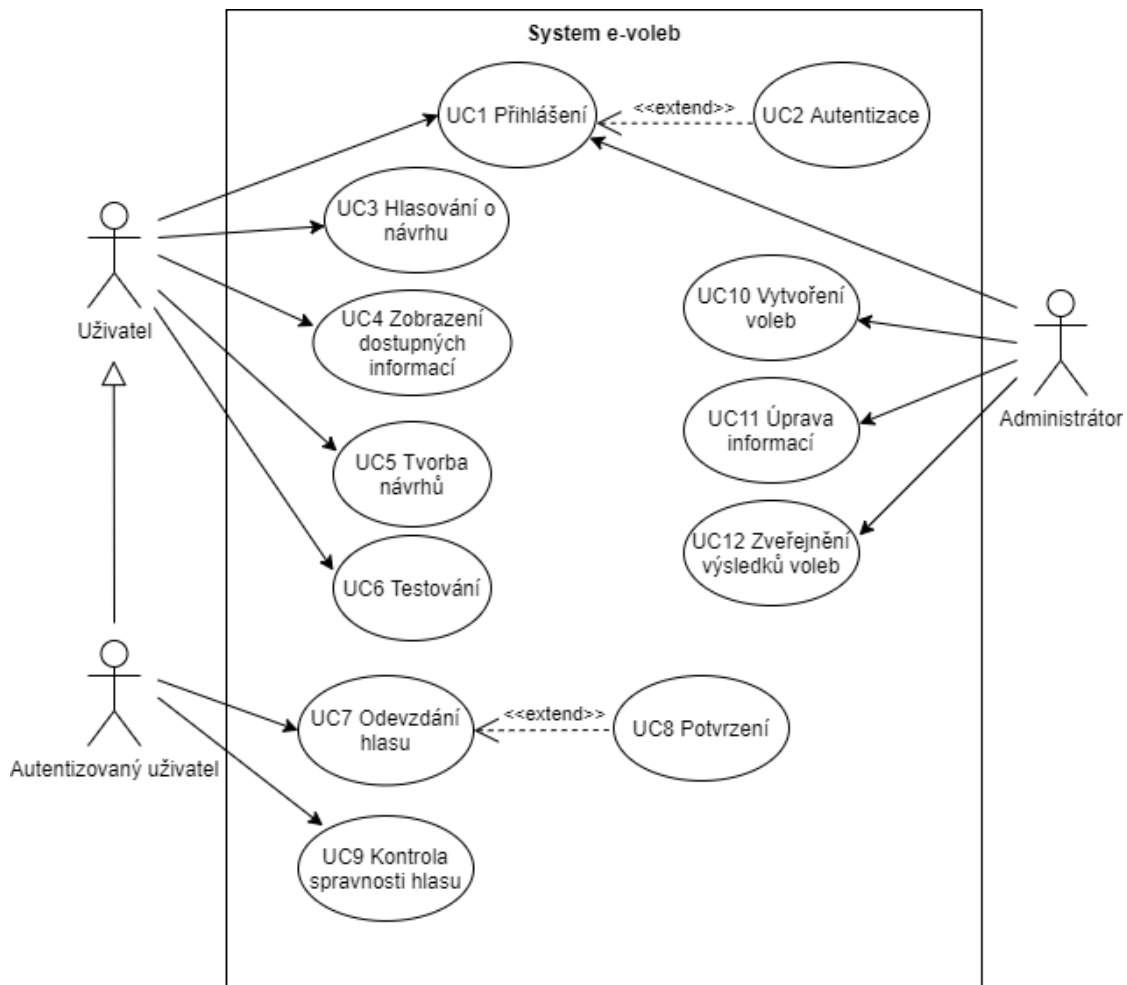
Anonymní uživatel nemá přístup k používání systému.

2.5 Diagram případu užití

Pro lepší přehled chování systému z pohledu uživatele byl vytvořen diagram (viz Obrázek 2.2) případů užití.

2.5.1 Klíčové uživatelské scénáře

Klíčové uživatelské scénáře jsou popsány v tabulkách. Každá tabulka popisuje konkrétní scénář a obsahuje seznam aktérů, kteří mohou scénář provést, podmínky, bez nichž scénář nelze provést, akce, které nastanou po úspěšném provedení scénáře, a stručný popis kroků spojených s provedením scénáře.



■ Obrázek 2.2 Případy užití systému

■ **Tabulka 2.1** UC1: Přihlášení

Název	UC1 Přihlášení
Aktér	Uživatel, administrátor
Předběžné podmínky	Uživatel přistoupil na stránku systému
Úspěšné záruky	Uživatel je přihlášen
Popis	<ol style="list-style-type: none"> 1. Uživatel stiskne přihlašovací tlačítko 2. Zadá své přihlašovací jméno a telefonní číslo, na které následně obdrží dočasný PIN kód 3. Uživatel zadá PIN kód na webové stránce

■ **Tabulka 2.2** UC2: Autentizace

Název	UC2 Autentizace
Aktér	Uživatel, administrátor
Předběžné podmínky	Úspěšné přihlášení pomocí PIN kódu
Úspěšné záruky	Uživatel je autorizován a je mu uděleno právo účastnit se hlasování; administrátor je autorizován a má přístup do administrátorského prostředí
Popis	<ol style="list-style-type: none"> 1. Uživatel přejde na stránku určenou k autentizaci 2. Uživatel předloží identifikační kartu s čipem prostřednictvím čtečky karet 3. Systém ověří totožnost uživatele 4. Pokud je totožnost úspěšně potvrzena, je uživatel autorizován

■ **Tabulka 2.3 UC7: Odevzdání hlasu**

Název	UC7 Odevzdání hlasu
Aktér	Autentizovaný uživatel
Předběžné podmínky	Uživatel byl ověřen a je na seznamu voličů; doba hlasování ještě neuplynula
Úspěšné záruky	Uživatel obdržel potvrzení o odeslání hlasu
Popis	<ol style="list-style-type: none"> 1. Volič přejde na stránku pro hlasování 2. Volič vybírá volby 3. Volič vyplní a odešle elektronický hlasovací lístek 4. Volič obdrží potvrzení

■ **Tabulka 2.4 UC3: Hlasování o návrhu**

Název	UC3 Hlasování o návrhu
Aktér	Uživatel
Předběžné podmínky	Uživatel je přihlášen
Úspěšné záruky	Hlas uživatele je zohledněn
Popis	<ol style="list-style-type: none"> 1. Uživatel si vybere návrh, o který má zájem. 2. Uživatel bude informován o významu svého hlasování 3. Uživatel stiskne tlačítko „Hlasovat“ 4. Systém zaznamená hlas uživatele

■ **Tabulka 2.5 UC5: Tvorba návrhů**

Název	UC5 Tvorba návrhů
Aktér	Uživatel
Předběžné podmínky	Uživatel je přihlášen pomocí PIN kódu a úspěšně absolvoval test na téma, které se týká jeho návrhu
Úspěšné záruky	Návrh byl vytvořen a je zobrazen v systému pro ostatní uživatele
Popis	<ol style="list-style-type: none"> 1. Uživatel klikne na tlačítko „Vytvořit“ ve svém profilu 2. Uživatel si vybere téma a provede formulář podle svých záměrů, systém nabízí tři možnosti: <ol style="list-style-type: none"> a) Uživatel navrhne návrh zákona b) Uživatel navrhne pozměňovací návrhy c) Uživatel navrhne diskuzi 3. Uživatel uloží návrh, který nyní mohou vidět ostatní uživatelé

■ Tabulka 2.6 UC6: Testování

Název	UC6 Testování
Aktér	Uživatel
Předběžné podmínky	Uživatel je přihlášen pomocí PIN kódu; pro případ opakování testu uplynula dostatečně dlouhá doba
Úspěšné záruky	Uživatel obdrží výsledek testu a právo vytvářet a diskutovat o návrzích na konkrétní témata, pokud test úspěšně absolvuje
Popis	<ol style="list-style-type: none"> 1. Uživatel přejde na testovací stránku a vybere si téma 2. Uživatel vyplní test 3. Systém zobrazí výsledky a uloží je do profilu uživatele 4. Systém zobrazí vzdělávací kurzy, které se vztahují k tématu testu

■ Tabulka 2.7 UC10: Vytvoření voleb

Název	UC10 Vytvoření voleb
Aktér	Administrátor
Předběžné podmínky	Administrátor byl úspěšně autentizován; toto hlasování nebylo vytvořeno dříve
Úspěšné záruky	Hlasování bylo úspěšně vytvořeno
Popis	<ol style="list-style-type: none"> 1. Správce klikne na tlačítko „Vytvořit volby“ 2. Správce vyplní formulář podle specifik voleb 3. Správce uloží formulář, tím je hlasování připraveno

Studie proveditelnosti

Pro stanovení realizovatelnosti vývoje navrhovaného systému je nutné provést studii proveditelnosti implementace a zavedení nových funkcí do stávajících systémů a posoudit možná rizika a benefity.

Na základě analýzy v teoretické části práce bylo zjištěno, že zavedení elektronického hlasování nezvýšilo volební účast. Proto bylo rozhodnuto doplnit tyto systémy o nové funkce. S jejich pomocí je možné zvýšit zapojení občanů do politiky a zvýšit jejich důvěru ke vládě. Za tímto účelem bylo navrženo doplnit online hlasovací systém o možnost sledovat aktivity politiků, například návrhy zákonů, vést o nich diskuse, navrhopvat vlastní návrhy zákonů a změny stávajících zákonů, z nichž nejlepší budou vygenerovány v petici a zaslány příslušným orgánům.

3.1 Výhody navrhovaného řešení

Hlavními přímými přínosy zavedení nových funkcí do online hlasovacího systému jsou:

- Zvýšení volební účasti.
- Zvýšení zájmu občanů o politiku.
- Zvýšení gramotnosti občanů.
- Snížení počtu nerozvážených petic.

3.2 Plán nasazení systému

Etapu 1: Plánování

- Rozsah:
 - Identifikace požadovaných technických funkcí.
 - Definování a dokumentace technického rozsahu.
- Architektura:
 - Definice hierarchie a toku obsahu.
 - Vytvoření mapy stránek a architektury.

Časový plán

Předpokládaná časová náročnost etapy: 2 týdnů.

Předpokládaný začátek etapy - 20. září 2021.

Předpokládaný konec etapy - 4. října 2021.

Potřebný personál: 1 analytik, 1 SW architekt.

Etapa 2: Design

- Návrh uživatelského rozhraní.
- Vytvoření vizuálních prostředků.
- Vytvoření frontendového prototypu.

Časový plán

Předpokládaná časová náročnost etapy: 4 týdnů.

Předpokládaný začátek etapy - 6. října 2021.

Předpokládaný konec etapy - 6. listopadu 2021.

Potřebný personál: 1 UI/UX designér.

Etapa 3: Vývoj

- Projektování logiky backendu.
- Programování veškerých uživatelských funkcí.
- Vývoj backendu.
- Instalace a konfigurace potřebných pluginů.

Časový plán

Předpokládaná časová náročnost etapy: 7 týdnů.

Předpokládaný začátek etapy - 9. listopadu 2021.

Předpokládaný konec etapy - 30. prosince 2021.

Potřebný personál: 3 programátoři.

Etapa 4: Testování a nasazení

- Testování výkonnosti na různých zařízeních a platformách.
- Sledování a oprava chyb.
- Provádění uživatelského testování.
- Optimalizace a úpravy podle potřeby.

Časový plán

Předpokládaná časová náročnost etapy: 3 týdnů.

Předpokládaný začátek etapy - 2. ledna 2022.

Předpokládaný konec etapy - 25. ledna 2022.

Potřebný personál: minimálně 1 QA inženýr, členové týmu podle potřeby.

Po nasazení projektu je nutná projektová podpora ve formě pravidelné monitorování a aktualizace systému.

Očekává se, že zavedení nových funkcí do systému elektronického hlasování bude trvat 4 měsíce.

■ **Tabulka 3.1** Přibližná výše platu členů týmu

Pozice	Plat/den
Projektový manažer	1500 Kč
Analytik	1200 Kč
SW architekt	1700 Kč
Programátor	1400 Kč
GUI designer	1300 Kč
Tester	900 Kč

3.3 Finanční náklady

Finanční náklady na vývoj systému budou analyzovány z hlediska nákladů na vývojový tým, protože náklady na jeho práci vyžadují největší finanční investici do vývoje systému. V tabulce (viz Tabulka 3.1) jsou uvedeny informace o hodinových mzdách vývojářů potřebných pro realizaci projektu. Uvedené částky jsou jenom hrubým odhadem a ve výsledků se mohou lišit. Technologie zvolené pro implementaci systému prakticky nevyžadují náklady, protože jsou volně dostupné.

Přibližné náklady v každé etapě:

Etapa 1 - 120 000 Kč

Etapa 2 - 150 000 Kč

Etapa 3 - 300 000 Kč

Etapa 4 - 90 000 Kč

Předpokládané celkové náklady na všechny fáze jsou tedy 660 000 Kč. Odchylna odhadu nákladů na implementaci může činit až 25 %.

3.4 Hodnocení rizik

V této kapitole jsou uvedena rizika, která mohou ovlivnit používání navržených funkcí systému.

■ **Tabulka 3.2** RZ1

Název	Dokončení projektu po termínu
Pravděpodobnost výskytu	Střední
Vlastník	Zadavatel
Dopad	Zvýšené náklady na implementaci
Mitigace	Včasně vyjádření problému Kontrola provádění prací
Krizový plán	Zvýšení počtu vývojářů

■ Tabulka 3.3 RZ2

Název	Nedostatečná kvalita projektového týmu
Pravděpodobnost výskytu	Nízká
Vlastník	Projektový manažer
Dopad	Nízká kvalita systému Delší doba vývoje Nespokojenost uživatelů
Mitigace	Závažný přístup k výběru vývojářů
Krizový plán	Nahrazení vývojářů

■ Tabulka 3.4 RZ3

Název	Podvádění během profilového testování
Pravděpodobnost výskytu	Střední
Vlastník	Vývojový tým
Dopad	Snížení kvality návrhu uživatelů
Mitigace	Omezení možnosti podvádění
Krizový plán	Zavedení dalších způsobů kontroly kompetence uživatele

■ Tabulka 3.5 RZ4

Název	Nekompatibilita použitých technologií
Pravděpodobnost výskytu	Nízká
Vlastník	Dodavatel
Dopad	Výpadky funkčních celků Problémy s provozem systému
Mitigace	Testování jednotlivých funkčních modulů a jejich vzájemného propojení před nasazením
Krizový plán	Zlepšení kompatibility pomocí vytvoření adaptéru

■ Tabulka 3.6 RZ5

Název	Nízký zájem uživatelů
Pravděpodobnost výskytu	Střední
Vlastník	Zadavatel
Dopad	Nízký počet uživatelů
Mitigace	Kvalitní uživatelské rozhraní Informování o výhodách systému
Krizový plán	Provádění reklamních kampaní s cílem přilákat uživatele



Kapitola 4

Závěr

Vzhledem ke složitosti elektronických hlasovacích systémů a vysokým bezpečnostním požadavkům je zlepšení těchto systémů obecně náročné.

V práci byly analyzovány zkušenosti s elektronickými volebními systémy a bylo zjištěno, že k očekávanému zvýšení volební účasti po zavedení online volebních systémů nedošlo. Proto byly v této práci navrženy vylepšení v podobě zavedení dalších funkcí, které by řešily problém nízké volební účasti. Posouzení dostupných technologií potřebných k zavedení nových funkcí přineslo pozitivní výsledek. V práci byly rovněž zkoumány uživatelské požadavky a scénáře pro online hlasovací systém s navrhovanými vylepšeními.

Studie proveditelnosti ukázala, že zavedení nových funkcí do systémů elektronického hlasování je relevantní a doporučené.

Literatura

- [1] E-estonia: Why estonia? [online], Dec 2020, [cit. 2021-04-17]. URL: <https://www.visitestonia.com/en/why-estonia/estonia-is-a-digital-society>.
- [2] Listina základních práv a svobod. In *Sbírka zákonů*, 1992. čl. 17. ISSN: 1211-1244.
- [3] Spycher Oliver, Volkamer Melanie, Koenig Reto. Transparency and technical measures to establish trust in norwegian internet voting. In *International Conference on E-Voting and Identity*, pages 19–35. Springer, 2011. ISBN: 9783642327469. doi:10.1007/978-3-642-32747-6_2.
- [4] Springall Drew, Finkenauer Travis, Durumeric Zakir, Kitcat Jason, Hursti Harri, MacAlpine Margaret, Halderman J. Alex. Security analysis of the Estonian internet voting system. Association for Computing Machinery, 2014. ISBN: 9781450329576. doi:10.1145/2660267.2660315.
- [5] Zisis Dimitrios and Lekkas Dimitrios. Securing e-government and e-voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2):239–251, 2011. URL: <https://www.sciencedirect.com/science/article/pii/S0740624X10001383>, doi:<https://doi.org/10.1016/j.giq.2010.05.010>.
- [6] Maaten Epp. Towards remote e-voting: Estonian case. In *Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG*, pages 83–100, 2004. URL: <https://dl.gi.de/20.500.12116/29132>.
- [7] Mazák Jaromír. O volební účasti aneb Proč (ne)chodíme k volbám, Hospodářské noviny (ihned.cz) [online], Feb 2014, [cit. 2021-05-10]. URL: <https://ihned.cz/c1-61774220-o-volebni-ucasti-aneb-proc-ne-chodime-k-volbam>.
- [8] Kučera Josef. V zahraničí volí stále více Čechů [online], Sep 2018, [cit. 2021-04-17]. URL: <https://www.statistikaamy.cz/2018/09/18/v-zahranici-voli-stale-vice-cechu>.
- [9] Summers Mike. Online voting isn't as flawed as you think—just ask Estonia. IEEE Spectrum: Technology, Engineering, and Science News [online], Oct 2016, [cit. 2021-04-27]. URL: <https://spectrum.ieee.org/telecom/internet/online-voting-isnt-as-flawed-as-you-thinkjust-ask-estonia>.
- [10] Lilian Mitrou, Dimitris Gritzalis, and Sokratis Katsikas. *Revisiting Legal and Regulatory Requirements for Secure E-Voting*, pages 469–480. 2002. doi:10.1007/978-0-387-35586-3_37.
- [11] Altair Valášek Michal. Lesk a bída elektronických voleb. ALTAIR.blog [online], July 2020, [cit. 2021-05-18]. URL: <https://www.altair.blog/2020/07/evolby#fn:1>.

Obsah přiloženého média

	readme.txt.....	stručný popis obsahu média
	exe.....	adresář se spustitelnou formou implementace
	src	
	impl.....	zdrojové kódy implementace
	thesis.....	zdrojová forma práce ve formátu L ^A T _E X
	text.....	text práce
	thesis.pdf.....	text práce ve formátu PDF