

Драгољуб Пилиповић

**Системи за електронско гласање
(научна монографија)**

Слобомир П универзитет

Добој

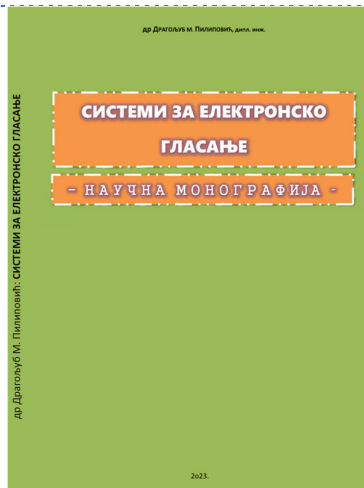
2023.

ISBN: 978-99955-54-29-3

Број страна: 305

Повез: брош

Формат: B5



Dragoljub Pilipovic

**Electronic voting systems
(scientific monograph)**

Slobomir P University

Doboj

2023.

ISBN: 978-99955-54-29-3

Pages: 305

Cover: paperback

Paper size: B5

Монографија коју ћете прочитати пада на раскршће два значајна појма данашњице: е-демократије и е-влада. Електронска демократија би требала бити интеракција свих дијелова друштва у процесу доношења важних одлука по друштвени развој, уз велико учешће информационо-комуникационих технологија (ИКТ). На основу групно донешене одлуке, електронска влада би употребила такође ИКТ у садејству са одговарајућим организационим пројенама, све са циљем унапређења квалитета јавних услуга.

Свака државна структура се може посматрати као сервис грађана па тако и е-влада. Описаће се зато један такав сервис – сервис електронског гласања, кроз приказ теоријских поставки али и примјењених система за електронско гласање (СЕГ). Сваки систем за е-гласање има своје захтјеве, карактеристике и особине, а на основу њих се може изабрати оптимална варијанта за неку ситуацију. Додатно, описаће се конкретни СЕГ и шеме на којима су засновани. Посебна пажња обратиће се на сигурност СЕГ и врсте напада на њих. У

Monograph that you read the falls at a crossroads of two important idea today: e-democracy and e-government. Electronic democracy should be the interaction of all parts of society in the process of making important decisions on social development, with a large participation of information and communication technologies (ICT). On the basis of the collectively decisions made, the electronic government used the ICT in conjunction with the appropriate organizational changes, with the aim of improving the quality of public services.

Each state structure can be regarded as a service to citizens and accordingly it be also the e-government. Therefore, in the dissertation will be describe one such service - service of electronic voting, by way of the view theoretical schemes and applied electronic voting systems (EVS). Any e-voting system has its own requirements, characteristics and properties, and based on them it can be choose optimal solution for any situation. It will be describe the specific e-voting systems and e-voting schemes in which based on. Special attention

најбитнијем поглављу ће се предложити нова архитектура СЕГ са особинама вишевекторности, вишемодалности и вишепрофилности. Студија случаја на крају ће кроз имплементацију предложене архитектуре СЕГ показати како овакав систем изгледа у пракси.

Кључне ријечи: е-демократија, е-влада, е-гласање, системи за е-гласање, шеме е-гласања, особине е-гласања, сигурност, анализа ризика, неизмјењиви уређаји.

will be paid to the safety of EVS and types of attacks against them. The most important chapter in the dissertation will propose a new EVS architecture with multivector, multimodal, and multiprofile properties. We designed and implemented software system as a case study to show how this system is proved to the practice of e-government.

Key words: e-democracy, e-government, e-voting systems, e-voting schemes, e-voting properties, security, risk analysis, anti-tamper devices.

САДРЖАЈ

Списак слика у монографији	9
Списак табела у монографији	11
Акроними и скраћенице	12
1. Предговор	17
2. Увод у електронско гласање	20
2.1 Примјери електронских гласања у свијету	21
2.2 Појам електронског гласања	25
2.3 Предмет и циљ истраживања монографије	27
2.4 Ставови младих према е-гласању	29
2.5 Организација научне монографије	43
3. Е-демократија и е-влада	45
3.1. Електронска демократија	47
3.1.1 Мобилна демократија	54
3.2. Е-елементи е-демократије	54
3.2.1 Електронска партиципација	55
3.2.2 Е-конгрегација	62
3.2.3. Електронска влада	63
3.2.3.1 Мобилна влада	76
3.3 Мјесто и улога е-елемената	78

CONTENT

List of pictures in the monograph	9
List of tables in monograph	11
Acronyms and abbreviations	12
1. Preface	17
2. Introduction to electronic voting	20
2.1 Examples of electronic voting in the 21st century	
2.2 The concept of electronic voting	25
2.3 The subject and aim of research of monograph	27
2.4 Attitudes of young people towards e-voting	29
2.5 Organization of scientific monograph	43
3. E-democracy and e-government	45
3.1. Electronic democracy	47
3.1.1 Mobile democracy	54
3.2. E-elements of e-democracy	54
3.2.1 Electronic participation	55
3.2.2 E-congregation	62
3.2.3. Electronic government	63
3.2.3.1 Mobile government	76
3.3 Place and role of e-elements	78

3.4 Организација е-избора	84	3.4 Organization of e-elections	84
3.4.1 Одабир врсте и система за е-изборе (framework)	87	3.4.1 Choosing the type and system for e-elections (framework)	87
3.4.2 Развој и увођење е-избора	90	3.4.2 Development and introduction of e-elections	90
3.4.2.1 Реинжењеинг е-избора	93	3.4.2.1 Reengineering of e-elections	93
3.4.3 Реализација е-избора	96	3.4.3 Realization of e-elections	96
3.4.3.1 Тестирање е-избора	97	3.4.3.1 Testing of e-elections	97
3.4.4 Надгледање процеса е-избора	100	3.4.4 Monitoring the e-elections process	100
3.4.4.1 Дигитална форензика е-избора	101	3.4.4.1 Digital forensics of e-elections	101
3.4.5 E-trust код е-избора	102	3.4.5 E-trust in e-elections	102
4. Класификација електронског гласања	107	4. Classification of electronic voting	107
4.1 Машине за биљежење гласова (DRE)	108	4.1 Vote recording machines (DRE)	108
4.2 Удаљено е-гласање	111	4.2 Remote e-voting	111
4.2.1 Интернет гласање	112	4.2.1 Internet voting	112
4.2.2 Мобилно гласање	112	4.2.2 Mobile voting	112
4.3 Употреба е-гласања у другим областима	113	4.3 Use of e-voting in other areas	113
4.3.1 Колаборација, системи за подршку одлучивању (СПО) и е-гласање	113	4.3.1 Collaboration, decision support systems (DSS) and e-voting	113
4.3.2 Е-гласање у образовању	115	4.3.2 E-voting in education	115
4.3.3 Е-гласање и е-аукције	117	4.3.3 E-voting and e-auctions	117
4.3.4 Е-гласање и игре на срећу	118	4.3.4 E-voting and games of chance	118
5. Захтјеви и стандардизација електронског гласања	119	5. Requirements and standardization of electronic voting	119
5.1 Општи друштвено-правни захтјеви за е-гласање	120	5.1 General socio-legal requirements for e-voting	120
5.2 Системске особине и захтјеви	122	5.2 System features and requirements	122
5.3 Технички захтјеви у вези доступности и перформанси	125	5.3 Technical requirements regarding availability and performance	125
5.4 Остали захтјеви и особине	127	5.4 Other requirements and features	127
5.5 Стандарди и препоруке за е-гласање	128	5.5 Standards and recommendations for e-voting	128
5.5.1 OASIS EML	128	5.5.1 OASIS EML	128
5.5.2 ISO/IEC 15408 (CC – Common Criteria)	130	5.5.2 ISO/IEC 15408 (CC – Common Criteria)	130
5.5.3 Rec CoE (2004) 11	131	5.5.3 Rec CoE (2004) 11	131
5.5.4 FEC VSS	132	5.5.4 FEC VSS	132
5.5.5 EAC VVSG	133	5.5.5 EAC VVSG	133
5.5.6 KORA	134	5.5.6 BARK	134
5.5.7 CORE	134	5.5.7 CORE	134
5.6 Супростављени захтјеви код е-гласања	135	5.6 Opposing requirements in e-voting	135
5.7 Електронски новац у функцији електронског гласа	136	5.7 Electronic money in the function of electronic voice	136
5.7.1 Е-новац у централизованомј топологији	136	5.7.1 E-money in a centralized topology	136

5.7.2 Е-новац у топологији без централе	138	5.7.2 E-money in a topology without a switchboard	138
5.8 Интеракција човјек-рачунар (HCI) код е-гласања	142	5.8 Human-computer interaction (HCI) in e-voting	142
6. Системи за електронско гласање	149	6. Systems for electronic voting	149
6.1 Општа архитектура е-гласања	150	6.1 General architecture of e-voting	150
6.2 Анализа шема за е-гласање	152	6.2 Analysis of e-voting schemes	152
6.2.1 Микс-нет шеме	155	6.2.1 Mix-net schemes	155
6.2.1.1 Примјер конкретне микс-нет шеме	158	6.2.1.1 Example of a concrete mix-net scheme	158
6.2.2 Шеме са хомоморфним криптовањем	159	6.2.2 Schemes with homomorphic encryption	159
6.2.2.1 Примјер конкретне шеме са хомоморфним криптовањем	161	6.2.2.1 Example of a concrete scheme with homomorphic encryption	161
6.2.3 Шеме засноване на потпису наслијепо	162	6.2.3 Blind signature-based schemes	162
6.2.3.1 Примјер конкретне шеме засноване на потпису наслијепо	163	6.2.3.1 Example of a concrete scheme based on blind signature	163
6.2.4 Шеме засноване на биометрији	164	6.2.4 Biometrics-based schemes	164
6.2.4.1 Примјер конкретне шеме засноване на биометрији	166	6.2.4.1 Example of a concrete scheme based on biometrics	166
6.2.5 Шеме засноване на РКИ и смарт картицама	168	6.2.5 Schemes based on PKI and smart cards	168
6.2.5.1 Примјер конкретне шеме засноване на смарт картицама	169	6.2.5.1 Example of a concrete scheme based on smart cards	169
6.2.6 Шеме засноване на визуелној криптографији	170	6.2.6 Schemes based on visual cryptography	170
6.2.6.1 Примјер конкретне шеме засноване на визуелној криптографији	170	6.2.6.1 Example of a concrete scheme based on visual cryptography	170
6.2.7 Шеме са слањем кóдова	171	6.2.7 Schemes with sending codes	171
6.2.7.1 Примјер конкретне шеме са слањем кóдова	172	6.2.7.1 Example of a concrete scheme with sending codes	172
6.2.8 Остале шеме	172	6.2.8 Other schemes	172
6.2.8.1 Prêt-à-Vote шема	173	6.2.8.1 Prêt-à-Vote scheme	173
6.2.8.2 ThreeBallot шема	174	6.2.8.2 ThreeBallot Scheme	174
6.2.8.3 Хелиос шема	174	6.2.8.3 Helios scheme	174
6.3 Поређење шема за е-гласање	175	6.3 Comparison of e-voting schemes	175
7. Сигурност и идентификација код е-гласања	189	7. Security and identification in e-voting	189
7.1 Анализа ризика	190	7.1 Risk analysis	190
7.1.1 Формализовани приступ анализи ризика преко π процесног рачуна	198	7.1.1 Formalized approach to risk analysis through π process calculus	198
7.2 Напади на систем и процес е-гласања	203	7.2 Attacks on the e-voting system and process	203
7.3 Проблем и постојање неизмјењивог (anti-tamper) уређаја	212	7.3 The problem and the existence of an unchangeable (anti-tamper) device	212
7.3.1 Отворени софтвер	221	7.3.1 Open software	221
7.3.1.1 Лиценце за отворени софтвер	221	7.3.1.1 Open Software Licenses	221
7.3.1.2 Методологије развоја отвореног софтвера	223	7.3.1.2 Open software development methodologies	223
7.3.1.3 Отворени компајлери и развојна окружења	224	7.3.1.3 Open compilers and development environments	224

7.3.1.4 Отворени стандарди за софтвер	226
7.3.1.5 Отворени оперативни системи	227
7.3.2 Отворени хардвер	228
7.3.2.1 Готов отворени хардвер	228
7.3.2.2 Отворене хардверске компоненте	230
7.3.2.3 Отворене хардверске архитектуре и сопствени развој хардвера	232
8. Пројектовање и имплементација MMM-VOTE система за е-гласање	233
8.1 Енвизија система за гласање са MMM функционалношћу	234
8.1.1 Осмишљавање вишевекторности	237
8.1.2 Осмишљавање вишемодалности	243
8.1.3 Осмишљавање вишепрофилности	254
8.2 Случајеви коришћења	258
8.3 Фаза анализе	260
8.4 Фаза пројектовања	265
8.5 Имплементациона фаза	268
8.6 Анализа предложеног рјешења и дискусија	270
9. Закључак	283
10. Литература	287
ДОДАТАК А: СТИЛ РЕФЕРЕНЦИРАЊА	301
ДОДАТАК Б: ИЗГЛЕД АНКЕТНОГ ЛИСТИЋА	304
ДОДАТАК В: SQL УПИТИ ЗА ОПИСНУ СТАТИСТИКУ УЗОРКА	305

7.3.1.4 Open Software Standards	226
7.3.1.5 Open operating systems	227
7.3.2 Open hardware	228
7.3.2.1 Ready Open Hardware	228
7.3.2.2 Open hardware components	230
7.3.2.3 Open hardware architectures and proprietary hardware development	232
8. Design and implementation of the MMM-VOTE system for e-voting	233
8.1 Envisioning a voting system with MMM functionality	234
8.1.1 Conceptualizing multi-vectority	237
8.1.2 Designing multimodality	243
8.1.3 Designing multi-profile	254
8.2 Use cases	258
8.3 Analysis phase	260
8.4 Design phase	265
8.5 Implementation phase	268
8.6 Analysis of the proposed solution and discussion	270
9. Conclusion	283
10. Literature	287
APPENDIX A: REFERENCE STYLE	301
APPENDIX B: LAYOUT OF THE QUESTIONNAIRE	304
APPENDIX V: SQL QUERIES FOR DESCRIPTIVE SAMPLE STATISTICS	305