ՀՏԴ 004.738.1

Ս.Վ. ԲԱԲԱՅԱՆ

ԷԼԵԿՏՐՈՆԱՅԻՆ ԸՆՏՐԱԿԱՆ ՀԱՄԱԿԱՐԳԻ ՎԵԲ ՄՈԴԵԼԻ ՀԵՏԱԶՈՏՈՒՄԸ

Դիտարկվում են էլեկտրոնային ընտրական համակարգի (ԷԸՀ) վեբ մոդել և դրա անվտանգությունը: Համակարգի անվտանգությունն ապահովվում է կառավարման բաշխված մարմինների սկզբունքի և բաց կոդով ծրագրակազմի օգտագործմամբ:

Առանցքային բառեր. էլեկտրոնային ընտրական համակարգ, ծրագրերի անվտանգություն, բաց կոդով ծրագրային ապահովում, անվտանգ աշխատապրոցեսի մոդելավորում:

Ներածություն: Ընտրական համակարգերը մեծ դեր ունեն ժողովրդավարության գոյատևման գործում ամբողջ աշխարհում: Մի քանի երկրներ քննարկում են էլեկտրոնային քվեարկությունը՝ որպես քվեարկության ավանդական մեթոդներին այլընտրանք կամ փոխարինում [1]: Էլեկտրոնային քվեարկությունը կարող է մեծացնել ընտրողների ներգրավվածությունը և ամրապնդել ժողովրդավարությունը, քանի որ էլեկտրոնային քվեարկությունը կբարձրացնի մատչելիությունը բնակչության մեծ շերտերի համար, մասնավորապես՝ այն խմբերի, որոնք նախկինում դժվարություններ էին ունենում քվեարկության ավանդական տարբերակի դեպքում:

Էլեկտրոնային եղանակով քվեարկությունը շատ ավելի շահավետ կարող է լինել: Ընտրողները կգնահատեն ցանկացած տեղից քվեարկելու հնարավորությունը: Ընկերությունը, որն ունի իր գրասենյակները տարբեր վայրերում, կարող է ինտերնետ քվեարկություններ անցկացնել, քանի որ բոլոր աշխատակիցները ընտրություններին կմասնակցեն իրենց գրասենյակներից: Էլեկտրոնային քվեարկությունը, ինչպես անունն է ենթադրում, էլեկտրոնային սարքավորումների օգտագործմամբ անցկացվող քվեարկության գործընթացն է: Ընդհանուր առմամբ, ինտերնետային քվեարկության համակարգերը պետք է բավարարեն հետևյալ պահանջները. ճշգրտություն, պարզություն, ժողովրդավարություն, ստուգելիություն, գաղտնիություն, անվտանգություն:

Քվեարկության ինտերնետային համակարգի հիմնական խնդիրն է ընտրությունների անվտանգությունն ու գաղտնիությունը: Այդ տեսանկյունից փակ ինտերնետ քվեարկության համակարգի ներդրումը, կարծես, գաղտնագրման և ցանցային անվտանգության մեկ այլ կիրառություն է: Վերջին քսան տարիների ընթացքում ինտենսիվորեն ուսումնասիրվում է էլեկտրոնային քվեարկությունը: Հետևաբար, վերջին մի քանի տասնամյակների ընթացքում առաջարկվել են

էլեկտրոնային քվեարկության շատ համակարգեր, և բարելավվել են ինչպես անվտանգությունը, այնպես էլ արդյունավետությունը:

Այս մոտեցումն առաջարկում է առկա գաղտնագրային սխեմաների գործնական կիրառում և թվային ստորագրություն, որն ապահովում է ընտրողների կողմից տրված քվեների ամբողջականությունը և ընտրողների իսկությունը: Ցանցով ապահով էլեկտրոնային քվեարկության համակարգի ձևավորումը իսկապես շատ բարդ խնդիր է, քանի որ քվեարկության համակարգի բոլոր պահանջները պետք է բավարարվեն: Նույնիսկ բնութագրերից որևէ մեկը չապահովելը կարող է հանգեցնել բացերի և անսարքությունների, որոնք կարող են օգտագործվել երրորդ անձի կողմից՝ տվյալները կեղծելու կամ շահարկելու համար: Հետևաբար, ընտրության արդյունքը հաշվարկվում է այն ձայների հանրագումարից, որը հաջողությամբ վերծանվում է համակարգի միջոցով: Քվեարկության սխեման պետք է ապահովի, որ ընտրողը կարողանա իր ձայնը գաղտնի պահել [2]:

Էլեկտրոնային քվեարկության համակարգերի անվտանգության չափանիշներ: Էլեկտրոնային քվեարկության նպատակը ընտրողների ձայների գրանցման հուսալիությունն ու ճշգրտությունն է՝ քվեարկության գործընթացը արդար և թափանցիկ դարձնելու համար: Էլեկտրոնային քվեարկության համակարգերը պետք է հետևեն որոշ կարևոր պահանջների՝ ընտրական գործընթացի ամբողջականությունն ապահովելու համար:

Առաջին չափանիշն այն է, որ յուրաքանչյուր ընտրության ժամանակ ընտրողը պետք է քվեարկի միայն մեկ անգամ:

Երկրորդն այն է, որ քվեարկության էլեկտրոնային համակարգերը պետք է գրանցեն քվեարկության գրառումներ՝ սխալներն ու փոփոխությունները հայտնաբերելու համար:

Երրորդ չափանիշն այն է, որ ընտրողների նախընտրությունները պետք է լինեն գաղտնի: Քվեարկության համակարգը պետք է լինի նաև աշխատունակ՝ ընտրությունների ողջ ընթացքում միաժամանակ կատարելու առաջադրանքները:

Չորրորդ չափանիշն այն է, որ քվեարկության համակարգերը պետք է պաշտպանված լինեն խարդախությունից և հարձակումներից:

Վերջին չափանիշն այն է, որ քվեարկության արդյունքները պետք է ճշգրիտ գրանցվեն և լինեն հասանելի [3]:

Գաղտնագրման գործիքներ: Առաջարկվող համակարգում օգտագործվել են պարզ, լավ հայտնի և լայնորեն օգտագործվող գաղտնագրման գործիքներ՝ RSA-ում օգտագործվող բացահայտ բանալիով գաղտնագրումը և գաղտնագրման հեշ ֆունկցիաները՝ SHA ալգորիթմների [4] օգտագործմամբ:

Բաց բանալիով գաղտնահամակարգը մեծապես կախված է հաշվողական բարդության և թվերի տեսություններից: RSA-ը առավել հայտնի և ամենատարած-

ված գաղտնագրային համակարգն է այսօրվա թվային աշխարհում: Այն հաճախ օգտագործվում է կոդավորման այլ սխեմաների հետ միասին կամ թվային ստորագրությունների համար, որոնք կարող են ապացուցել հաղորդագրության իսկությունը և ամբողջականությունը:

RSA գաղտնագրման սխեման.

գաղտնագրման ֆունկցիան՝ ξ_{enc}, ciphertext, $c = \xi_{enc}(K_{pub}, m)$,

վերծանման ֆունկցիան՝ ξ_{dec}, plaintext, $m = \xi_{dec}(K_{prv}, c)$.

RSA ստորագրության սխեման.

ստորագրում՝ ζ_{sig}, signature, $s = \zeta_{sig}(K_{prv}, m)$,

հաստատում՝ ζ_{ver}, verify, $v = \zeta_{ver}(K_{pub}, s)$.

RSA կույր ստորագրության սխեման.

blind՝ λ_{blind}, blind, $b = \lambda_{blind}(K_{pub}, \psi, m)$,

ստորագրում՝ ζ_{sig}, signature, $bs = \zeta_{sig}(K_{prv}, b)$,

unblind՝ $\lambda_{unblind}$, unblind, $s = \lambda_{unblind}(K_{pub}, \psi, bs)$,

հաստատում՝ ζ_{ver}, verify, $v = \zeta_{ver}(K_{pub}, s)$:

Գաղտնագրման հեշ ֆունկցիաները վերադարձնում են մուտքային արժեքների համար ֆիքսված չափի արժեք, որը կոչվում է դրանց հեշ արժեք կամ հեշ:

Ծրագրային ապահովում: Քվեարկության էլեկտրոնային համակարգերի օգտագործման հիմնական թերություններից մեկն այն է, որ այդպիսի համակարգերում օգտագործվող ծրագրակազմի տեսակը փակ կոդով է, ինչը հիմնականում քննադատվում է անբավարար անվտանգության և հուսալիության համար: Բաց կոդով ծրագրակազմի օգտագործումը կարող է բարելավել էլեկտրոնային քվեարկության համակարգերի անվտանգության որոշ սահմանափակումներ: Բաց կոդի օգտագործման նպատակը էլեկտրոնային քվեարկության ծրագրային ապահովման մեջ անվտանգության և հուսալիության կառուցումն ու զարգացումն է, քանի որ բաց կոդը հնարավորություն է տալիս մշակողներին և փորձագետներին հայտնաբերել սխալներ և փոփոխություններ, որոնք կարող են շահարկել քվեարկության արդյունքները: Բաց աղբյուրի ծրագրակազմը ոչ միայն բարելավում է էլեկտրոնային քվեարկության համակարգերի օգտագործման անվտանգությունն ու հուսալիությունը, այլ նաև խրախուսում է հասարակությանը՝ կախված լինելու էլեկտրոնային քվեարկության համակարգերից և ընտրողների վստահությունը նորից զարգացնելու ընտրական գործընթացների նկատմամբ:

Համակարգը պետք է իրականացվի որպես բազմամակարդակ վեբ ծրագիր, որը կառուցվելու է ազատ և բաց աղբյուրի ծրագրակազմի միջոցով: Օգտագործողի ինտերֆեյսը կառուցվելու է Angular-ով, որը Google-ի կողմից TypeScript-ի վրա հիմնված բաց կոդով ծրագրային ապահովում է:

Օգտագործողների և սերվերի հաղորդակցումն ապահովելու համար օգտագործվելու է Apache HTTP Server-ը, որն ապահովում է վեբ տվյալների անվտանգ փոխանցումը:

Սերվերի կոդը և միջանկյալ ծրագրային ապահովումները կգրվեն Python ծրագրավորման լեզվով: Pyhton լեզվի շեշտը դրված է կոդի ընթեռնելիության և օգտագործողի հարմարավետության վրա: Բացի այդ, Python-ը ամենաարագ զարգացող լեզուն է Back-End ծրագրավորման համար:

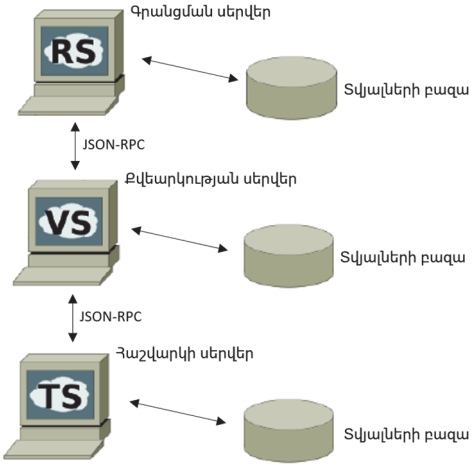
Որպես տվյալների բազա կօգտագործվի PostgreSQL-ը: Այն թույլ է տալիս անվտանգ պահել բարդ և մեծ քանակի տվյալները: Այն օգնում է մշակողներին՝ կառուցելու ամենաբարդ ծրագրերը, գործարկելու ադմինիստրատիվ առաջադրանքներ և ստեղծելու ինտեգրալ միջավայր:

Համակարգի ճարտարապետությունը: Առաջարկվելիք համակարգը հիմնված է մի քանի սերվերների, կառավարման բաշխված մարմինների և ծրագրերի բազմամակարդակ ճարտարապետության վրա: Համակարգը բաժանվելու է գրանցման, քվեարկության և հաշվարկի սերվերների, որոնք ընտրության տարբեր փուլերում կատարելու են տարբեր գործառույթներ (նկ.): Յուրաքանչյուր սերվեր ունենալու է առնվազն երկու նույնական պատճեն այնպես, որ եթե սերվերներից որևէ մեկը ձախողվի, տվյալները չեն կորչի, և պատճեններից մեկը կփոխարինի հիմնական սերվերին: Տվյալների բազաները նույնպես կունենան առնվազն երկու կրկնօրինակ.

RS - գրանցման սերվեր (Registration server),

VS - քվեարկության սերվեր (Voting server),

TS - հաշվարկի սերվեր (Tallying server):



Նկ. Համակարգի ճարտարապետությունը

Եզրակացություն: Քննարկվել է առցանց քվեարկության համակարգի բարդությունը՝ կապված հակասական պահանջների հետ: Լուծումը հիմնված է միմյանց նկատմամբ սահմանափակ վարչական իշխանություն ունեցող լիազորությունների բաշխման վրա: Անվտանգությունը մոդելավորվում է սերվերներից և միայն նրանց միջև փոխազդեցությունից: Օգտագործվել են պարզ և լավ հայտնի գաղտնագրման գործիքներ:

Պահպանվում է անանունությունը, և միևնույն ժամանակ խթանվում ստուգելիությունն ու կապելիությունը՝ օգտագործելով գրանցման և քվեարկության երկփուլանի գործընթացներ: Օգտագործողին անհրաժեշտ է միայն աջակցել HTML-ը և էջի վերահղումը՝ առանց Javascript-ը աջակցելու, քանի որ օգտագործողի կողմից script-եր գործարկելը նվազեցնում է համակարգի անվտանգությունը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. i-Voting - e-Estonia. https://e-estonia.com/solutions/e-governance/i-voting/.- 2021 (last accessed)
2. **Neumann S.**, **Volkamer M.** A Holistic Framework for the Evaluation of Internet Voting Systems // In D. Zissis & D. Lekkas (eds) // Design, Development, and Use of Secure Electronic Voting Systems.- 2014.- P. 76-91.
3. **Adeel M. J.** Electronic Voting System Security // SSRN Electronic Journal.- 2014.- 18 P.
4. National Institute of Standards and Technology (October 2008) SECURE HASH STANDARD (SHS) // Federal Information Processing Standards Publications (FIB PUBS) 180-3.- 2008.

С.В. БАБАЯН

ИССЛЕДОВАНИЕ ВЕБ-МОДЕЛИ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Рассматриваются веб-модель избирательной системы и ее безопасность. Безопасность системы обеспечивается принципом распределения ответственности и с использованием программного обеспечения с открытым исходным кодом.

Ключевые слова: система электронного голосования, безопасность программ, программное обеспечение с открытым исходным кодом, моделирование безопасного рабочего процесса.

S.V. BABAYAN

INVESTIGATING THE WEB-MODEL OF THE ELECTRONIC VOTING SYSTEM

This paper discusses the web-model of the electoral system and its security. The system security is ensured by the principle of distribution of responsibility, and using open-source software.

Keywords: e-voting system, program security, open-source software, secure workflow modeling.

ՀՏԴ 681.51/54

Է.Ա. ԱԼԵՔՍԱՆՅԱՆ

ՎԻՐՏՈՒԱԼ ԻՐԱԿԱՆՈՒԹՅԱՆ ՄԻՋԱՎԱՅՐՈՒՄ ԷԼԵԿՏՐԱԿԱՆ ԵՐԵՎՈՒՅԹՆԵՐԻ ՈՒՍՈՒՄՆԱՍԻՐՄԱՆ ԵՎ ՀԵՏԱԶՈՏՄԱՆ ՄՈԴԵԼԻ ՆԱԽԱՏԻՊԸ

Դիտարկվում է մոդելի նախատիպ, որը հնարավորություն կտա օգտագործողին վիրտուալ իրականության մեջ կատարել այնպիսի հետազոտություններ և լաբորատոր փորձեր, որոնք ինչ-ինչ պատճառներով անհնար են իրականացնել իրական միջավայրում, վտանգավոր են կամ՝ շատ թանկարժեք: Ներկայացված մոդելը նախատեսվում է օգտագործել և՛ որպես կրթական գործիք ուսանողների համար, և՛ որպես վիրտուալ էլեկտրական միջավայր լայն հասարակության համար:

Առանցքային բառեր. էլեկտրական շղթաներ, վիրտուալ իրականություն, լաբորատոր հետազոտություն, էլեկտրական միջավայր:

Ներածություն: Էլեկտրական ծառայությունների մատուցման համար էլեկտրականությունը և դրա իրական միջավայրում օգտագործման հետ կապված բնորոշ ռիսկերը վաղուց առաջնահերթություն են դարձել հասարակության լայն զանգվածների համար, որոնք պետք է ապրեն և աշխատեն այս միջավայրում:

Վիրտուալ իրականությունը կարող է նկարագրվել որպես մի տեխնոլոգիա, որը հնարավորություն է տալիս իրական ժամանակում ուսումնասիրել և շահարկել համակարգչով գեներացվող եռաչափ միջավայրեր [1]: Չնայած սկզբնական շրջանում այն դիտվում էր թանկարժեք գործիք, ինչը ենթադրում էր հսկայական ներդրումներ, ներկայումս հեշտորեն հնարավոր է ստանալ ավելի բարդ և թանկարժեք համակարգեր [2]: Իր բնույթով վիրտուալ իրականությունն(VR) ունի առավելություն՝ լինել անվտանգ ինչպես օգտագործողի, այնպես էլ սարքավորումների համար: Բացի այդ, այն օգտվողին հնարավորություն է տալիս լինել տվյալ