

# МОДЕЛ ЗА ПОВИШАВАНЕ НА ДОВЕРИЕТО В МАШИННОТО ГЛАСУВАНЕ

Алекс Радев

Университет по библиотекознание и информационни технологии

**Резюме:** В тази разработка се предлага модел за повишаване на доверието в машинното гласуване чрез приложение на блокчейн технологии и други технически способи за валидация, удостоверение и осигуряване на легитимността на изборния процес, процедури и добри практики за провеждане на изборния процес в съответствие на националните и европейските стандарти и текущите технологични тенденции и приложения на използваните технологии в процеса на машинното гласуване, като не е изключено да е приложимо и за дистанционно електронно гласуване чрез интернет връзка.

**Ключови думи:** блокчейн; валидация; изборен процес; криптография; машинно гласуване

## ВЪВЕДЕНИЕ

Изборният процес е един от най-важните процеси в една демократична държава. Именно този процес на власт на народа е ключов за развитието на държавата, институциите, определянето на държавната политика чрез референдуми и най-вече – изразяване на нагласите на обществото (Gancheva 2024). В Република България правото на провеждане на избори и референдуми и участието в тях са защитени от чл. 10 и чл. 42 на Конституцията на Република България (КРБ) и уредени в Изборния кодекс (ИК).

С развитието на цифровите технологии все по-често се обсъжда идеята за електронно гласуване с машини или чрез интернет свързаност. През 2014 г. Централната избирателна комисия (ЦИК) провежда експериментално изборите за членове на Европейския парламент от Република България чрез машинен вот (Tsareva 2014). През 2016 и 2020 г. се въвеждат значителни промени в ИК (Tsareva 2014), които допускат машинния вот на практика, а през 2021 г. се приема Закон за допълнение и изменение на ИК (ИК, изм. и доп., ДВ, бр. 36 от 2021 г., в сила от 1.05.2021 г.<sup>1</sup>), с който се предвижда провеждане на 100% машинен вот, но той среща сериозен обществен отпор, свързан с притеснения за честността и доверието в софтуера на машинните. На 27.10.2023 г. Държавна агенция „Национална сигурност“ (ДАНС) изпраща доклад до ЦИК за подозрения за манипулиране на машинния вот. ЦИК издава Решение<sup>2</sup> за отмяна на машинното гласуване, на базата на доклада на ДАНС и непълна документация от страна на Министерството на електронното управление (МЕУ). Докладът на ДАНС за недоверието в машинния вот предизвиква несигурност в обществото и политическите формации относно честността на машинното гласуване и в общественото пространство възникват множество въпроси: „Компроментирани ли са машините?“, „Има ли опит за саботаж на машинното гласуване“.

не?“, „Защо някои политически формации са категорично против машинното гласуване?“ и пр.

Въпреки сериозните съмнения в надеждността на машинното гласуване, то може да бъде сериозен инструмент за гарантиране на автентичността и честността на изборния процес, но са необходими адекватни мерки, за да може да служи като такъв гарант. За да бъде една система за машинно гласуване честна и прозрачна и същевременно да спазва духа на тайното гласуване, е необходимо тя да отговаря на следните критерии:

- ▷анонимност на гласа;
- ▷проверимост на гласа;
- ▷прозрачност;
- ▷сигурност.

В тази разработка ще се предложи модел на система за машинно гласуване, която да осигури горепосочените критерии, да отговаря на необходимите изисквания в ИК, както и на европейските регламенти, но и съвременен подход към удостоверяването на гласоподавателите и процедури за провеждане на изборния процес в предложената система. Част от предложенията и мерките, изложени тук, се припокриват фундаментално, но не напълно с блог пост на бившия министър на МЕРУ Божидар Божанов<sup>4</sup>, като тази корелация се установява в процеса на разработка на настоящия текст.

## **МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО**

Методологията на изследването се състои в анализ на научни публикации, книги, нормативноправни документи и публични източници, проучване на стандарти и добри практики за целите на изследването, синтез на знания и създаване на собствена концептуална разработка с интердисциплинарен подход и теоретико-приложен характер.

## **РЕЗУЛТАТИ**

В модела са включени множество мерки и предложения на ниво софтуер и хардуер, с които да се гарантира честен изборен процес и да се отговори на изискванията по чл. 212, чл. 213, чл. 213а и чл. 213б на ИК. Предложените в модела мерки и промени ще се разделят на две категории – софтуер и хардуер. Софтуерните мерки и предложения касаят само софтуерните системи за машинно гласуване, както и всичко необходимо за тяхното обезпечение. Хардуерните мерки и предложения засягат само техническите средства, устройствата за провеждане на машинното гласуване, също наричани „терминали за гласуване“ или „машини за гласуване“, и инфраструктурата за целите на реализация на този модел.

Техническите устройства за машинно гласуване е необходимо да отговарят на изискванията на ЦИК, съгласно чл. 213 и чл. 213а от ИК. Тяхната функционалност в предложенния модел не се засяга, но се предлагат следните изменения в техническите изисквания, целящи повишаването на сигурността на всяко крайно устройство (endpoint):

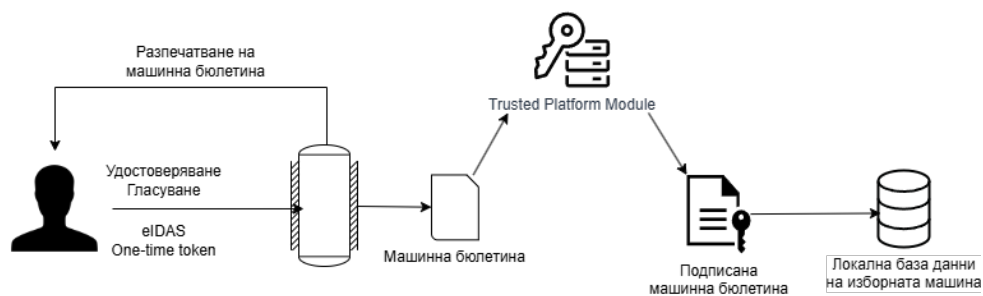
- ▷система, поддържаща Unified Extensible Firmware Interface(UEFI);
- ▷централен процесор и операционна система (ОС), базирани на 64-битови инструкции;
- ▷имплементиране на Trusted Platform Module 2.0 (TPM 2.0) или по-нов;
- ▷задължителна поддръжка на UEFI Secure boot с възможност за настройване на базата с цифрови сертификати на операционните системи (custom Secure boot);
- ▷ограничен брой портове за входно-изходни устройства;
- ▷поставяне на контролна пломба за сигурност върху шасито на техническото устройство;
- ▷задаване на параметри на Secure boot и конфигуриране за работа само с цифрови сертификати на ЦИК и ОС, подписани от ЦИК;
- ▷четец на цифрово подписани електронни карти и квалифицирани електронни подписи (КЕП);
- ▷липса на вградена безжична мрежова карта, с цел ограничаване на външно влияние;
- ▷предоставяне на модем за свързаност с мобилна мрежа.

От съществено значение за сигурността на всеки endpoint е имплементацията на UEFI Secure boot. UEFI Secure boot осигурява, че всички модули и програми при първоначалното пускане на ОС и ядрото на ОС се изпълняват без външни модификации от трети лица (Wilkins 2013).

Повратен момент в сигурността на техническите устройства за електронно гласуване е цифровото подписване на ОС. Цифровото подписване на операционната система гарантира, че ОС, която се изпълнява на машината за гласуване, е удостоверена и подписана от ЦИК. Предлага се следният механизъм за проверка на интегритета на ОС – сравнение на цифровия подпис на ОС и сравняване на целостта на ОС и нейните компоненти посредством контролен хеш, наречен checksum. Необходимо е също създаването на уникален цифров подпис на всяка машина за гласуване и на криптографски ключове за критични и чувствителни компоненти от софтуера за машинно гласуване, които се подписват от ЦИК и съхраняват в TPM модула на терминала за гласуване.

Софтуерът за машинно гласуване е разделен на две основни части – система за гласуване и ОС. В този раздел ще разгледаме в частност системата за гласуване, тъй като тя е независима от ОС.

Софтуерът за машинно гласуване трябва да отговаря на изискванията на ЦИК, съгласно чл. 213 от ИК. Функционалността на софтуера за машинно гласуване не е засегната в потребителския софтуер, но се изменя архитектурно, особено процесите на заден план, където гласоподавателят не взаимодейства с тях по никакъв начин, както е показано на фиг. 1.



Фиг. 1. Схема на процес на гласуване с техническо устройство за машинно гласуване

При инициализацията на софтуера за гласуване всички тайни и криптографски ключове се достъпват еднократно в паметта чрез ТРМ модула, където са съхранени. Предлагат се изменение и допълнение на чл. 213 от ИК, като се добавят следните предложения:

- ▷ задължително постоянно присъствие на версията и контролен хеш код на електронната система в потребителския софтуер на видимо място;
- ▷ задължително изпечатване на хеш кода на машинната бюлетина в края на машинната бюлетина.

Тези изменения и допълнения подобряват значително проверимостта на системата за машинно гласуване, защото позволяват на всеки гласоподавател, застъпник или член на избирателна комисия да контролира и следи изборния процес. Чрез хеша на машинната бюлетина гласоподавателят може да провери автентичността на гласа си в блокчейн регистъра на ЦИК след обявяването на изборните резултати.

Преди началото на изборния ден член на СИК в присъствието на техническо лице привежда устройството за гласуване в работен режим и сравнява контролния хеш код на електронната система за гласуване с хеш кода, предоставен от ЦИК.

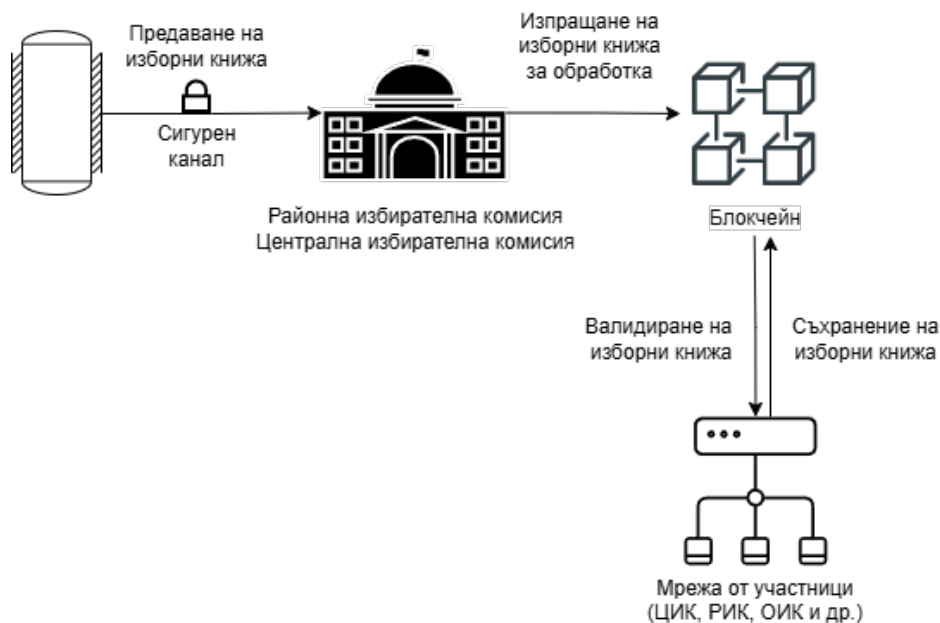
Краят на изборния ден се обявява от председателя на СИК по следната процедура:

- ▷ след последния гласоподавател председателят на СИК се идентифицира чрез електронната си карта, предоставена преди изборния ден;
- ▷ устройството за гласуване прекратява изборния процес;
- ▷ председателят на СИК вкарва модема за свързаност с мобилна мрежа в изборния терминал;
- ▷ машината за гласуване обработва събраните гласове и генерира машинния протокол в електронен формат;
- ▷ машината за гласуване разпечатва машинния протокол на хартиен носител;
- ▷ операционната система на машината за гласуване разрешава изходящия трафик от машината след установяване на сигурна връзка с ЦИК.

Предлага се и публичен регистър на проверените гласове и машинните протоколи, базиран на блокчейн технология като алтернатива на сегашните отчети в машинно четим формат (.csv). Блокчейн технологията има множество разнообразни дефиниции, но за целите на разработката ще приемем, че блокчейн представлява децентрализирана разпределена система, в която недоверяващи страни участват и сътрудничат без доверен посредник (Tabatabaei, Vitenberg, Veeraragavan 2023). Участници в блокчейн мрежата са всички избирателни комисии без СИК, като тяхната роля е верифициране и валидиране на получените машинни бюлетини и протоколи и вписването им в регистъра.

Този регистър би функционирал по следния начин, както е показано на фиг. 2:

- ▷ получава гласове и машинни протоколи от машините за гласуване;
- ▷ верифицира получените гласове и протоколи;
- ▷ валидира получените гласове и протоколи;
- ▷ въвежда валидираните гласове и протоколи в регистъра, ако има консенсус на над 75% от участниците в блокчейн мрежата.



Фиг. 2. Схема на механизъм за предаване и обработка на изборните книжа с помощта на блокчейн

След края на изборния ден машината за гласуване предава до РИК или ЦИК събраните гласове и протокола по сигурен канал, например вътрешна виртуална частна мрежа, и заключва системата. Освен ползите от повишената сигурност, предаването на машинните протоколи по сигурен канал предоставя възможност за моментално паралелно предварително преброяване по райони,

области или секции, с което може да се проследят и контролират високорисковите секции в страната.

Важен аспект от системата в модела, който се различава от текущия вариант на машинно гласуване в страната, е промененият механизъм за автентикация на гласоподавателя при терминала за гласуване. Всеки гласоподавател, след като бъде вписан в избирателните списъци, има две възможности за автентикация при терминала за гласуване – чрез цифрово подписана електронна карта с еднократен токен, издадена от член на СИК, или чрез цифрова самоличност под формата на квалифициран идентификационен документ или КЕП, включително мобилен такъв, в съответствие с Регламент (ЕС) 2024/1183 (eIDAS<sup>3</sup>). При удостоверяване с КЕП по eIDAS<sup>3</sup> е необходимо да се имплементира проверка за потвърждение, че подписът е удостоверен от български доставчик на електронни удостоверяващи услуги, отговарящи на изискванията на Регламента. Ако подписът не е удостоверен от българска страна, лицето, използващо eIDAS услугата, няма да бъде допуснато до изборите, освен в случаите, определени в чл. 396 от ИК. За да се запази анонимността на гласоподавателя, механизмът за автентикация не трябва да съхранява никакви чувствителни данни или данни, които могат да го идентифицират по някакъв начин, а ако обстоятелствата задължават тяхното съхранение, тези лични данни задължително трябва да бъдат криптирани с част от криптографския ключ на конкретната машина за гласуване преди съхраняването им, за да се гарантира анонимността на гласоподавателя в съответствие с Регламент (ЕС) 2016/679. Изборният процес след това протича обикновено – гласоподавателят избира, потвърждава избора си и машината изпечатва бюлетина.

Заради въведените промени и мерки за сигурност в софтуера и хардуера на машините за гласуване бюлетината се подписва цифрово с публичния ключ, предоставен от ЦИК, и след това повторно се подписва с публичния ключ на машината за гласуване, подписан от ЦИК и съхранен в TPM модула.

Прозрачността на системите за машинно гласуване е жизненоважна за повишаване и поддържане на доверието в изборния процес. Съществен принос в осигуряването на прозрачността на предложения модел има парадигмата на софтуера с отворен код. Предложението за публикуване на изходния код и документацията на системата за машинно гласуване в публичното пространство значително би повишило доверието на гражданското общество и би стимулирало активното участие в осигуряването на сигурността и одитирането на софтуера за машинно гласуване. Освен техническото обезпечение и предложението в този модел, необходимо е да се предприемат и законодателни промени в Изборния кодекс, конкретно чл. 213б, ал. 1. В настоящия си вид чл. 213б от ИК не осигурява достатъчно прозрачност на гражданите, тъй като те нямат достъп до горепосочения софтуер и документация и не могат да участват активно в осигуряването на прозрачността и честността на изборния процес, проведен чрез машинно гласуване, освен ако не са посочени от някоя политическа формация, и би направил предложението за отворен код практически невъзможно.

## ИЗВОДИ/ДИСКУСИЯ

Предложеният модел за повишаване на доверието в машинното гласуване показва възможността за справяне с проблемите чрез интегриране на модерни технологии. Предлагат се подробно описани мерки и предложения на ниво софтуер и хардуер, с които значително се подобрява сигурността на крайните устройства и ключовата инфраструктура. Освен предложените мерки се предлагат и нововъведения, като блокчейн базиран регистър на изборните книжа, механизъм за сигурно предаване на изборните книжа и автоматизирано паралелно преброяване на гласовете.

Освен предложените технически промени и нововъведения е необходимо да се направят законодателни промени на Изборния кодекс, за да се повишат прозрачността и отчетността на техническите средства и системи, като се насърчава активното участие на гражданското общество в контрола на изборния процес. Повишаването на доверието в машинното гласуване е ключов фактор за цялостното повишаване на доверието в изборния процес.

## ЗАКЛЮЧЕНИЕ

Изборният процес е един от най-важните процеси в една демократична правова държава. Въвеждането на машинното гласуване може значително да улесни и ускори провеждането на избори, като същевременно гарантира легитимността на изборния процес. Както всяка технология, машинното гласуване не е съвършено и изникват опасения за честността на изборите, проведени чрез подобна технология, което представлява сериозен риск за демокрацията. Създаването на прозрачна и сигурна инфраструктура, определянето и прилагането на добри практики и стандарти в изборния процес, проведен с машинно гласуване, са повече от необходимост – те са абсолютно задължително условие за изграждането на доверие към машинното гласуване и стъпка напред към гарантирането на нормални демократични процеси в една правова държава. В този доклад е предложен модел за повишаване на доверието в машинното гласуване, като се предприемат конкретни мерки и се въведат технически изисквания, касаещи устройствата и електронните системи за машинно гласуване, и се предлагат определени процедури за провеждане на машинното гласуване. Този модел не се ограничава само до употребата му в контекста на машинното гласуване, а като цяло може да бъде приложен и надграждан за различни системи за електронно гласуване, следвайки подобни насоки в процеса на проектиране на системи за електронно гласуване, включително дистанционно електронно гласуване.

## БЕЛЕЖКИ

1. Допълнение и изменение – Държавен вестник, бр. 36 от 2021 г., в сила от 1.05.2021 г. [viewed 2 May 2025]. Available from: <https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=158029>.
2. РЕШЕНИЕ на ЦИК от 27.10.2023 г. [viewed 2 May 2025]. Available from:

<https://www.cik.bg/bg/decisions/2819/2023-10-27>.

3. eIDAS – Electronic Identification, Authentication and Trust Services.

4. БОЖАНОВ, Б., 2021. *Рискове и мерки за защита на машинното гласуване*. [viewed 7 May 2025]. Available from: <https://blog.bozho.net/blog/3868>.

## ЛИТЕРАТУРА

ГАНЧЕВА, Й., 2024. По някои въпроси за девиационите рискове в изборния процес. *Юридически сборник на БСУ*. Бургас: Бургаски свободен университет, с. 209 – 216. [viewed 28 April 2025]. Available from: <http://research.bfu.bg:8080/server/api/core/bitstreams/42a961ca-43a9-4567-a588-dea64e310743/content>.

ЦАРЕВА, Д., 2020. Електронното гласуване в България и Германия. *Политика и Сигурност*, год. IV, бр. 1. Пловдив: Висше училище по сигурност и икономика, с. 87 – 109. [viewed 1 May 2025]. Available from: <https://politics-security.net/index.php/ojsdata/article/view/117/126>.

WILKINS, R.; RICHARDSON, B., 2013. UEFI secure boot in modern computer security solutions. *UEFI forum*, pp. 1 – 10. [viewed 2 May 2025]. Available from: [https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2014/06/21032725/UEFI\\_Secure\\_Boot\\_in\\_Modern\\_Computer\\_Security\\_Solutions\\_2013.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2014/06/21032725/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf).

TABATABAEI, M.; VITENBERG, R.; VEERARAGAVAN, N., 2023. Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review*, 50, p. 100575. [viewed 6 May 2025]. Available from: <https://arxiv.org/pdf/2207.02264>.

## REFERENCES

GANCHEVA, Y., 2024. About some questions, about deviation risks in the election process. *Yuridicheski sbornik na BSU*. Burgas: Burgaski svobodnen universitet, pp. 209 – 216. [viewed 28 April 2025]. Available from: <http://research.bfu.bg:8080/server/api/core/bitstreams/42a961ca-43a9-4567-a588-dea64e310743/content>.

TSAREVA, D., 2020. Elektronното glasuvane v Bulgaria i Germania. *Politika i Sigurnost*, god. IV, br. 1. Plovdiv: Visshe uchilishte po sigurnost i ikonomika, s. 87 – 109. [viewed 1 May 2025]. Available from: <https://politics-security.net/index.php/ojsdata/article/view/117/126>

WILKINS, R.; RICHARDSON, B., 2013. UEFI secure boot in modern computer security solutions. *UEFI forum*, pp. 1 – 10. [viewed 2 May 2025]. Available from: [https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2014/06/21032725/UEFI\\_Secure\\_Boot\\_in\\_Modern\\_Computer\\_Security\\_Solutions\\_2013.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2014/06/21032725/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf).

TABATABAEI, M.; VITENBERG, R.; VEERARAGAVAN, N., 2023. Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review*, 50, p. 100575. [viewed 6 May 2025]. Available from: <https://arxiv.org/pdf/2207.02264>.

## MODEL OF IMPROVING TRUST IN E-VOTING

**Abstract:** *This study proposes a model of improving trust in e-voting systems through the application of blockchain technology and other technical methods for validation, verification and ensuring the legitimacy of the electoral process, as well as procedures and good practices for conducting elections, according to the national and European standards and current technological trends and their application for the purpose of e-voting and potentially remote e-voting via Internet.*

**Keywords:** *blockchain; cryptography; election process; e-voting; validation*

**Alex Radev, Student**

Scientific Advisor: Prof. Magdalena Garvanova, PhD  
University of Library Studies and Information Technologies  
Sofia, Bulgaria  
E-mail: 301sr@unibit.bg