



**ВЫБАРЧАЯ
КАМІСІЯ**

**РАШЭННЕ ВЫБАРЧАЙ КАМІСІІ
“Аб зацвярджэнні Тэхнічнага задання
па стварэнні і функцыянаванні электроннай плятформы
для галасавання на выбарах у Каардынацыйную Раду 2026”**

5 сакавіка 2026 года

г. Варшава

На падставе падпунктаў 4.9.1 і 4.10 пункта 4, падпункта 9.1 пункта 9 Палажэння аб выбарах у Каардынацыйную раду, прынятага 20 студзеня 2026 года, у мэтах вызначэння формы і сродкаў правядзення галасавання і далейшага заключэння дамовы з выканаўцам паслуг па стварэнні і функцыянаванні лічбавай плятформы для галасавання, зацвярджаецца:

**ТЭХНІЧНАЕ ЗАДАНЬНЕ
па стварэнні й функцыянаванні электроннай плятформы
для галасавання на выбарах у Каардынацыйную Раду 2026**

1. Агляд

Гэты дакумент апісвае тэхнічныя патрабаванні да электроннай плятформы для правядзення выбараў у Каардынацыйную Раду Беларусі IV склікання. Плятформа забяспечвае вэрыфікацыю асобы выбаршчыкаў, дэдуплікацыю галасоў і ананімнае галасаваньне.

1.1. Тэрміналогія.

Паняцці	Азначэнні
Выбаршчык	Грамадзянін Беларусі, які жадае прагаласаваць
Тэхнічны правайдэр	Суб’ект, які распрацоўвае электронную плятформу для галасавання ў адпаведнасці з Тэхнічным заданьнем, і забяспечвае яе функцыянаваньне.
Камісія	Выбарчая камісія, абраная Каардынацыйнай радай Беларусі, у асобах Яраслава Бекіша, Алены Жылачкінай (Жываглад), Пятра Маркелава, Алены Прыходзька, Дзьмітрыя Фурманава, якая дзейнічае на падставе Ўстаноўчай дамовы ад 6 лютага 2026 года і Палажэння аб выбарах у Каардынацыйную раду.
КУС-правайдэр	Зьнешні сэрвіс вэрыфікацыі асобы.

Сыстэма Пашпарта Новай Беларусі	Зьнешняя сыстэма для вэрыфікацыі ўладальнікаў Пашпарта Новай Беларусі
Электронная плятформа	Электронная сыстэма, якая дазваляе беларускім грамадзянам прагаласаваць за выбарчыя суб'екты.
РaaS-правайдэр	Зьнешні воблачны сэрвіс (Platform as a Service), які забяспечвае хостынг, аўтаматычнае разгортваньне з CI/CD пайплайна, вядзеньне логаў разгортваньня і адсутнасьць прамога доступу (SSH) да сэрвэра, а таксама audit trail для дзеяньняў адміна (Cloud Audit Logs або аналяг) і выкарыстаньнем гранулярнага доступу да сэрвісаў
Блокчэйн-правайдэр (Vocdoni)	Зьнешняя дэцэнтралізаваная плятформа для галасаваньня на аснове блокчэйна, якая забяспечвае ананімнае і вэрыфікаванае галасаваньне. Vocdoni прымае зашыфраваныя галасы, запісвае іх у блокчэйн і дазваляе выбаршчыку правярць свой голас па унікальным ідэнтыфікатары галасаваньня.
Зьнешнія назіральнікі	Незалежныя спэцыялісты або арганізацыі, прызначаныя Камісіяй для правэркі карэктнасьці функцыянаваньня электроннай плятформы. Маюць права на прагляд логаў разгортваньня РaaS-правайдэра, логаў зборкі GitHub Actions, audit trail КҮС-правайдэра і логаў API-запытаў, лог дзеяньняў адмінаў РaaS-правайдэра) без магчымасьці іх зьмяняць або выдаляць. Не маюць доступу да пэрсанальных даных выбаршчыкаў.

1.2. Мэты

- Выключэньне магчымасьці доступу да пэрсанальных дадзеных выбаршчыкаў
- Магчымасьць выбаршчыкаў прагаласаваць з выкарыстаньнем розных тыпаў дакумэнтаў
- Гарантыя таго, што кожны выбаршчык можа прагаласаваць толькі адзін раз
- Забесьпячэньне празрыстасьці працэсу

2. Дакумэнты, якія прымаюцца электроннай плятформай

2.1. Аўтаматычная вэрыфікацыя праз КҮС-правайдэра

Наступныя дакумэнты прымаюцца праз аўтаматычную сыстэму КҮС-правайдэра:

Тып дакумэнта	Наяўнасьць нацыянальнага ID	Нататкі
Беларускі пашпарт (у тым ліку пратэрмінаваны)	Так	Пратэрмінаваныя пашпарты прымаюцца, бо грамадзянства не залежыць ад тэрміну дзеяньня пашпарта

2.2. Вэрыфікацыя праз сыстэму Пашпарта Новай Беларусі

Тып дакумэнта	Наяўнасьць нацыянальнага ID	Нататкі
Пашпарт Новай Беларусі	Так	Вэрыфікацыя праз інтэграцыю з сыстэмай Пашпарта Новай Беларусі.

3. Архітэктурна дэдуплікацыі

3.1. Агульны прынцып

Дэдуплікацыя адбываецца на двух узроўнях:

1. **Узровень КҮС-правайдара** — дэдуплікацыя па фатаграфіі, імя й прозьвішчу й даце нараджэньня (правайдэр выяўляе падазроныя супадзеньні паміж вэрыфікацыямі ў працэсе галасаваньня, Тэхнічным правайдэрам разам з Камісіяй вызначаюцца межы падабенства, калі запісы пазначаюцца як патрабуючы дадатковай правэркі)
2. **Узровень электроннай плятформы** — дэдуплікацыя па хэшу ўнікальнага ідэнтыфікатара грамадзяніна (асабістым нумары)

3.2. Дэдуплікацыя на ўзроўні КҮС-правайдара

- Запісы вэрыфікацый захоўваюцца ў КҮС-правайдара на працягу ўсяго тэрміну галасаваньня, вызначанага Камісіяй, цягам сямі дзён (не выдаляюцца адразу пасля вэрыфікацыі)
- КҮС-правайдэр выяўляе падазроныя выпадкі (падабенства твару, пры наяўнасьці іншага ймя або даты нараджэньня і г.д.)
- Пры выяўленьні падазронага дубліката сыстэма можа аўтаматычна адмовіць у вэрыфікацыі выбаршчыка
- Тэхнічны правайдэр прадастаўляе справаздачу па кожным выпадку з указаньнем прычыны адхіленьня спробы вэрыфікацыі
- Межы падабенства вызначаюцца паводле ўзгадненьня з Камісіяй да пачатку ці на працягу пэрыяду галасаваньня.

4. Бясьпека і кантроль доступу да даных

4.1. Прынцып мінімальнага захоўваньня

- Пэрсанальныя дадзеныя выбаршчыкаў не захоўваюцца на сэрверах сыстэмы для галасаваньня, акрамя хэшаванага асабістага нумару грамадзяніна каб зафіксаваць факт выдачы бюлетэня.

4.2. Лагаваньне API-запытаў

Усе звароты да КҮС-правайдара павінны лагавацца

4.2.1. Лагаваньне запытаў да КҮС-правайдара

- Кожны АРІ-запыт да КҮС-правайдара (стварэньне сэсыі, атрыманьне вынікаў, выдаленьне запісаў) запісваецца ў лог
- Лог утрымлівае: часовую пазнаку, тып запыту, ідэнтыфікатар сэсыі, вынік (без пэрсанальных даных)
- КҮС-правайдэр павінен мець audit trail для дзеяньняў у адмінцы

4.2.3. Аўдыт доступу

- Логі захоўваюцца на працягу ўсяго пэрыяду галасаваньня і захоўваюцца па сканчэньні галасаваньня Камісіяй разам з Каардынацыйнай Радай.
- Камісія мае магчымасьць прааналізаваць усе логі пасля заканчэньня выбараў для пацьверджаньня, што доступ да даных быў толькі ў абгрунтаваных выпадках
- Пасля заканчэньня галасаваньня й абвяшчэньня канчатковыхі вынікаў галасаваньня, акаўнт у КҮС-правайдэры выдаляецца

4.4. Выдаленьне даных пасля абвяшчэньня вынікаў выбараў

Кампанэнт	Дзеяньне
База хэшаў ID выбаршчыкаў	Поўнае выдаленьне Тэхнічным правайдэрам
Акаўнт КҮС-правайдэра	Захаваньне ўсіх неабходных логаў, потым выдаленьне акаўнта (Камісія і Каардынацыйная Рада)

4.5. Працэдура рэагаваньня на здарэньні ў сфэры бясьпекі

4.5.1. Вызначэньне

Здарэньнем у сфэры бясьпекі лічыцца любая падзея, якая ўяўляе пагрозу цэласнасьці, канфідэнцыяльнасьці або даступнасьці электроннай плятформы, у тым ліку:

- несанкцыянаваны доступ да сэрвэраў, баз даных або адмінпанэляў;
- несанкцыянаванае разгортваньне коду, мінуючы ўстаноўленую працэдуру;
- каардынаваныя спробы падтасоўкі галасоў;
- няштатнае зьмяненьне або выдаленьне запісаў у базе хэшаў;
- уцечка пэрсанальных дадзеных выбаршчыкаў.

4.5.2. Парадак рэагаваньня

1. **Апавяшчэньне.** Бок, які выявіў здарэньне, неадкладна апавяшчае другі бок пра здарэньне
2. **Лакалізацыя.** Тэхнічны правайдэр прымае неадкладныя меры для лакалізацыі здарэньня.
3. **Расьследаваньне.** Тэхнічны правайдэр сумесна з Камісіяй праводзіць расьследаваньне з выкарыстаньнем логаў АРІ-запытаў (п. 4.2), логаў разгортваньня (п. 5.2) і audit trail КҮС-правайдэра. Меры рэагаваньня зацьвярджаюцца Камісіяй.

4. **Дакумэнтаваньне.** Тэхнічны правайдэр рыхтуе справаздачу (храналогія, прычыны, ужытыя меры, ацэнка ўплыву на вынікі) і перадае яе Камісіі на працягу 48 гадзін пасля ліквідацыі здарэньня.

5. Вэрыфікацыя разгорнутага коду

5.1. Праблема

Неабходна гарантаваць, што менавіта пэўная вэрсія коду задэплойна ў прадакшане, каб Камісія і грамадзкасьць маглі пераканацца, што сыстэма працуе так, як заяўлена.

5.2. Рашэньне

5.2.1. Публічны рэпазіторы

- Зыходны код сыстэмы публікуецца ў адкрытым рэпазіторы перад пачаткам галасаваньня
- Кожны рэліз пазначаецца git-тэгам з подпісам (signed tag)

5.2.2. Вэрыфікацыя разгорнутай вэрсіі

- Пры разгортваньні сыстэма запісвае хэш свайго коду/зборкі ў публічна даступны лог
- Камісія мае магчымасьць у любы момант запытаць хэш бягучай разгорнутай вэрсіі й параўнаць яго з апублікаваным (вэрыфікуецца праз выкарыстаньне Github Actions)

5.2.3. Кантроль разгортваньня

Для забесьпячэньня незалежнага кантролю над разгортваньнем выкарыстоўваецца мадэль падзеленага доступу з удзелам даверанага трэцяга боку (PaaS-правайдэра). Ні Тэхнічны правайдэр, ні Камісія паасобку не маюць магчымасьці разгарнуць код у прадакшн-асяродзьдзі без кантролю другога боку.

Кампанэнты інфраструктуры разгортваньня

- **Публічны рэпазіторы (GitHub)** — утрымлівае зыходны код сыстэмы, канфігурацыю CI/CD пайплайна і гісторыю ўсіх зьменаў. Кожны рэліз пазначаецца signed git tag.
- **CI/CD пайплайн (GitHub Actions)** — аўтаматычна запускаяецца пры зьмене коду ў галоўнай галіне рэпазіторыя. Выконвае зборку Docker-вобразу, запуск тэстаў і вылічэньне хэшу зборкі.
- **РaaS-правайдэр** — акаўнт у PaaS-правайдэры ствараецца Камісіяй. Тэхнічны правайдэр і зьнешнія назіральнікі атрымоўваюць аўдыраскія правы ў акаўнце з магчымасьцю бачыць Cloud Audit Logs (або аналяг), а таксама правы настройкі аплаты воблачных паслуг, калі неабходна.

Працэс разгортвання

- Разгортваньне ажыццяўляецца выключна праз CI/CD пайплайн (GitHub Actions). Прамое разгортваньне на прадакшн-сэрвэры, мінуючы пайплайн, тэхнічна немагчымае.
- Пры зьяўленьні новай вэрсіі коду ў галоўнай галіне, пайплайн аўтаматычна разгортвае зборку на PaaS-правайдэры з дапамогай API-ключа, які захоўваецца ў зашыфраваным сховішчы GitHub Secrets.

Падзел правоў доступу

- **Камісія:** мае доступ да панэлі кіраваньня PaaS-правайдэра
- **Камісія і Каардынацыйная Рада:** маюць доступ да адмінкі KYC-правайдэра
- **Тэхнічны правайдэр:** мае права на запіс коду ў рэпазіторыі, мае доступ да панэлі кіраваньня PaaS-правайдэра
- **Зьнешнія назіральнікі:** маюць права на прагляд логаў доступу да базы дадзеных і логаў разгортвання
- **Сакрэты PaaS-правайдэра:** захоўваюцца ў зашыфраваным сховішчы GitHub Secrets. Пасьля ўнясення ключы ня могуць быць прачытаны ніводным удзельнікам (уключаючы адміністратараў рэпазіторыя) і выкарыстоўваюцца толькі аўтаматычна падчас разгортвання. Хэшы ключоў даступны ў логах дэплоймэнту з частковым маскаваньнем.

Лагаваньне разгортванняў

- Логі разгортвання ствараюцца аўтаматычна двума незалежнымі сыстэмамі: GitHub Actions (лог зборкі і зацьверджаньня) і PaaS-правайдэрам (лог разгортвання на сэрвэры).
- Логі ўключаюць: часовую пазнаку, хэш каміта, хэш зборкі (Docker image digest)
- Ніводны бок не мае магчымасьці зьмяніць або выдаліць логі разгортвання, паколькі яны захоўваюцца трэцімі бакамі (GitHub і PaaS-правайдэр).
- Прамы доступ да прадакшн-сэрвэра (SSH) адсутнічае — PaaS-правайдэр не прадастаўляе такой магчымасьці.

6. Парадак вэрыфікацыі і галасаваньня

1. Камісія атрымоўвае ад Тэхнічнага правайдэра унікальны ідэнтыфікатар выбарчай кампаніі і публікуе яго ў афіцыйных каналах
2. Выбаршчык усталёўвае мабільны дадатак або выкарыстоўвае вэб-вэрсыю Электроннае плятформы. Выбаршчыкі з IP-адрасамі з Беларусі не маюць магчымасьці ўсталяваць мабільны дадатак. Выбаршчыкі з IP-адрасамі з Беларусі не маюць магчымасьці прагаласаваць праз вэб-вэрсыю без выкарыстаньня VPN.
3. Выбаршчык праходзіць вэрыфікацыю асобы (адзін з варыянтаў):
 - а) Аўтаматычная вэрыфікацыя празь KYC-правайдэра (пашпарт)
 - б) Вэрыфікацыя праз сыстэму Пашпарта Новай Беларусі
4. Правайдэр вяртае personId (унікальны асабісты нумар грамадзяніна) і вынік вэрыфікацыі
5. Issuer-сэрвэр:
 - Хэшуе personId
 - Правярае хэш на дублікат у базе
 - Калі дублікат — адхіляе
 - Калі ўнікальны — выдае крэдэнцыял выбаршчыка і выдае яго з памяці

6. Выбаршчык выкарыстоўвае крэдэнцыял для ананімнага галасавання праз Vocdoni.
7. Выбаршчык мае магчымасць праверыць, ці сапраўды ягоны голас аддадзены за абраны ім выбарчы суб'ект, праз наяўнасць унікальнага ключа, выкарыстоўваючы Vocdoni Explorer (<https://explorer.vote/verify>).

7. Патрабаванні да КҮС-правайдара

Патрабаваньне	Апісаньне
Падтрымка пашпарта Рэспублікі Беларусь	У тым ліку пратэрмінаваных
Дэдуплікацыя па фатаграфіі	Выяўленьне аднаго твару на розных дакумэнтах
Захоўваньне запісаў на працягу пэрыяду галасавання й да абвяшчэньня канчатковых вынікаў выбараў	Для забесьпячэньня дэдуплікацыі
Audit trail	Лагаваньне ўсіх дзеяньняў у адмінцы або праз API
Выдаленьне запісаў пасля кампаніі	Выдаленьне ўсяго акаўнта

8. Рызыкі і абмежаванні

Рызыка	Апісаньне	Мітыгацыя
Недавер да Пашпарта Новай Беларусі	Сыстэма не правяраецца КҮС-правайдэрам	Прыняцьце рызыкі; даверы да каманды Пашпарта НБ
Доступ да персанальных даных з боку Тэхнічнага правайдэра	Тэхнічны правайдэр мае патэнцыйны доступ праз API-ключ КҮС-правайдэра, а таксама панэль кіраванья PaaS правайдэра	Лагаваньне ўсіх API-запытаў (audit trail з боку правайдэра). Выкарыстаньне Cloud Audit Logs або аналяга, выдача правоў на прагляд Зьнешнім назіральнікам.
Доступ да персанальных даных з боку Камісіі	Камісія мае доступ да панэлі кіраванья PaaS правайдэрам, а таксама адмінкі КҮС-правайдэра	Выкарыстаньне Cloud Audit Logs або аналяга, выдача правоў на прагляд Зьнешнім назіральнікам. Падзяленьне права доступу да адмінкі КҮС-правайдэра паміж Камісіяй і ўпаўнаважаным ад Каардынацыйнай рады з дапамогай двухфактарнай аўтэнтыфікацыі для выключэньня доступу толькі адным з бакоў.

Старшыня Выбарчай Камісіі



Алена Прыходзька