



# Apskritojų stalo diskusija: Blokuojamųjų domėnų valdymo informacinės sistemos kūrimas

2022 m. vasario 2 d.



Projekto „Kenkėjiškų interneto svetainių grėsmių suvaldymo priemonių kūrimas“ dalis

# Viešoji konsultacija-apskritojų stalo diskusija

Tikslas – suteikti galimybę suinteresuotosioms šalims išreikšti poreikį ir pateikti pastabas dėl pagrindinių Blokuojamųjų domenų valdymo informacinės sistemos (BDVIS) veikimo principų.

Data ir laikas: 2022 m. vasario 2 d. 9.00-11.00 val. (nuotoliniu būdu)

## Tikslinės grupės:

domenų blokavimą galinčios inicijuoti valstybinės institucijos:

Lietuvos policija, Lietuvos bankas, Lošimų priežiūros tarnyba, Lietuvos radijo ir televizijos komisija, Valstybinė vartotojų teisių apsaugos tarnyba, (NTAKD);

interneto prieigos paslaugų tiekėjai:

Telia, Bitė, Tele2, INIT, Balticum, KVTC;

kitos valstybinės institucijos:

NKSC, RRT;

nepriklausomi kibernetinio saugumo specialistai:

INFOBALT, Vilnius Legal Hackers.



# Projekto gairės

Atlikta esamos situacijos  
analizė dėl interneto  
svetainių saugumo būklės  
Lietuvoje  
2021 m. lapkritis



Atlikta gerosios užsienio  
praktikos analizė dėl  
priemonių, apribojančių  
kenkėjiškų svetainių prieigą  
2021 m. gruodis



Atlikta viešoji konsultacija  
dėl siūlomų priemonių  
kenkėjiškų svetainių prieigos  
apribojimui  
2022 m. vasaris

Parengtas Blokuojamų  
domenų valdymo  
informacinės sistemos  
modelis  
2022 m. vasaris

Pateiktos rekomendacijos  
dėl BDVIS įgyvendinimo  
ir tolimesnių žingsnių  
2022 m. kovas

# Diskusijos planas

Ižanga (20 min)

BDVIS poreikis (20 min)

BDVIS veikimo principai (60 min)

BDVIS įgyvendinimas (15 min)

Apibendrinimas (5 min)



# Kokią problemą sprendžiame?



1

## **Policija**

Nusikaltimo elektroninėje erdvėje atvejais su teismo sankcija arba blokuoti 48 val. ir kreiptis į teismą dėl tokio veiksmo teisėtumo.

2

## **Lošimų priežiūros tarnyba**

Nelegalios lošimų veiklos internetu atvejais su teismo sankcija.

3

## **Valstybinė vartotojų teisių apsaugos tarnyba**

Esant sistemingiems Civilinio kodekso, Vartotojų teisių apsaugos, Nesąžiningos komercinės veiklos vartotojams draudimo ar Produktų saugos įstatymų pažeidimams su teismo sankcija.

4

## **Lietuvos radijo ir televizijos komisija**

Interneto svetainių, kuriose neteisėtai viešai paskelbtas autorių teisių saugomas turinys atvejais su teismo sankcija.

5

## **Lietuvos bankas**

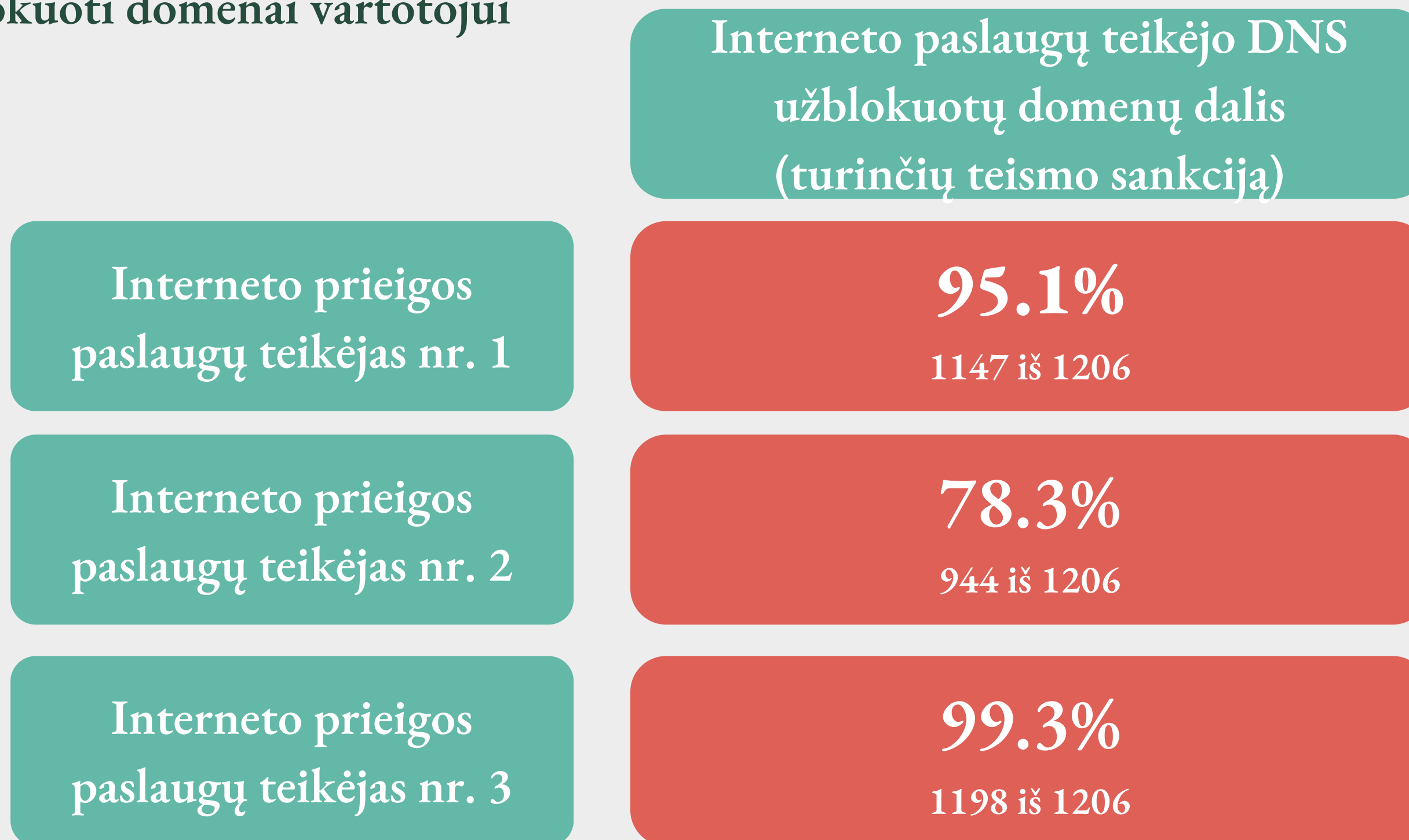
Nelegalias finansines paslaugas siūlančių interneto svetainių atvejais su teismo sankcija.

## **Kitos institucijos aktyviai siekiančios blokavimo galimybės**

Ateityje institucijų galinčių inicijuoti domenų blokavimą per IPT skaičius didės (pvz., Narkotikų, tabako ir alkoholio kontrolės departamentas)

# Įvykdytos teismo skirtos sankcijos

Realiai užblokuoti domenai vartotojui



Vertintos trys blokavimą inicijuoti galinčios institucijos ir tikrinti su teismo sankcija užblokuoti domenai viešai paskelbti institucijų interneto svetainėse. Visi eksperimente vertinti interneto paslaugų teikėjai yra TOP 5 interneto paslaugų teikėjai pagal pajamas ([RRT](#)). Duomenys surinkti 2021-11-29.

# Tobulintinas blokavimo sankcijų įgyvendinimas

## Procesas

5 skirtingos valstybinės institucijos  
siunčia nurodymus el. laiškais

90 interneto prieigos paslaugų teikėjų  
rankiniu būdu apdoroja tą pačią  
užklausą

## Problemos

Procesas imlus žmogiškosioms klaidoms

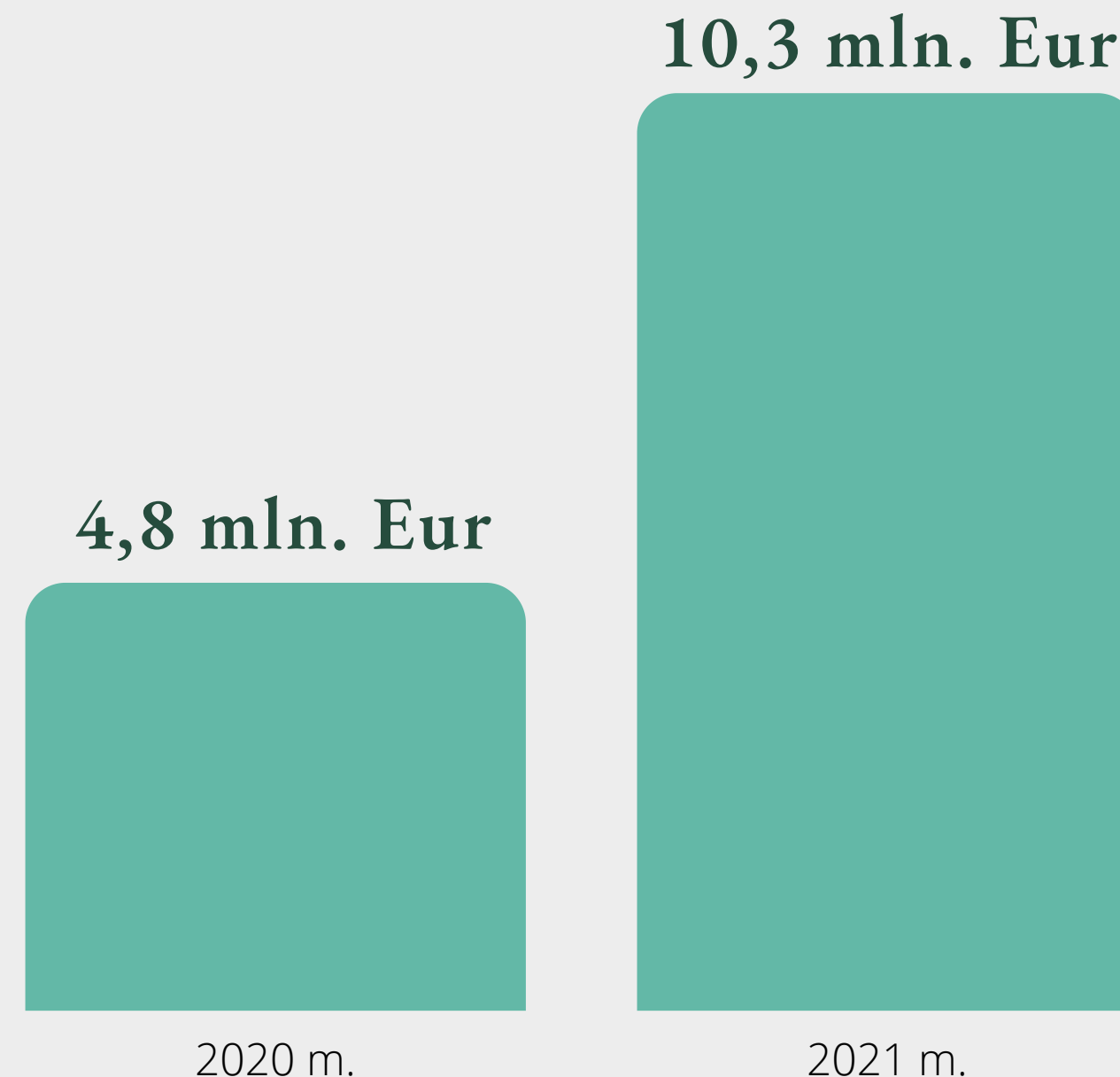
Nėra galimybės patikrinti, ar tikrai yra įvykdomos teismo sankcijos

Įgyvendinimas gali užtrukti iki 5 d.d.



# 2021 m. Lietuvos gyventojams ir verslui finansinių sukčių padaryta žala išaugo dvigubai

Pasaulinės tendencijos rodo, kad nusikaltimų elektroninėje erdvėje daroma žala ir toliau augs eksponentiškai.



Lietuvos bankų asociacijos duomenys, 2022 m. Šioje statistikoje nėra išskiriama, kokią dalį žalos padaro konkrečiai kenkėjiškos interneto svetainės. Kita vertūs realūs skaičiai yra didesni, nes gyventojai ir verslas ne visada informuoja apie patirtą žalą.

# Diskusija: koks yra poreikis tobulinti blokavimo sankcijos įgyvendinimą?

Kokie yra pagrindiniai iššūkiai įgyvendinant sankciją blokuoti interneto svetainę?

Kokie sprendimai pasiteisino/nepasiteisino užtikrinant sankcijos įgyvendinimą?



# Kokią sprendimą svarstome?





# Blokuojamų domenų valdymo informacinė sistema (toliau – BDVIS)

Tikslas: pagreitinti jau egzistuojantį sankcionuotą interneto svetainių blokavimo vykdymo procesą, suteikti stebėjimo mechanizmą blokuojančioms institucijoms ir išvengti teismo sankcijos neįvykdymo.

# Įprastas interneto svetainės blokavimo inicijavimo ir įvykdymo procesas

Taikant BDVIS, būtų pasiektas maksimalus greitis vykdant teismo sankcijas, t.y. paskutiniame etape. Siekiant pasiekti geriausią galimą BDVIS poveikį, ateityje reikėtų peržiūrėti ir kitas proceso dalis.



\*Taip pat policijos pareigūnai taikydami 48 val. blokavimą arba institucijos, blokuojančios veidrodines svetaines pagal ankstesnes teismo nutartis.

# Policijos 48 val. kenkėjiškų internetu svetainių blokavimo proceso paspartinimas su BDVIS

Pagal Lietuvos Respublikos kibernetinio saugumo  
įstatymo 10 straipsnio 3 dalį.

Identifikuojama kenkėjiška  
internetu svetainė, kelianti didelę  
žalą lankytojams ir naudojama  
nusikaltimams elektroninėje erdvėje



Policija atlieka tyrimą ir  
paruošia dokumentus dėl  
svetainės blokavimo



Policija inicijuoja 48 val.  
blokavimą ir kreipiasi į  
teismą



Internetu paslaugų teikėjai per  
kelias val. apriboja prieigą prie  
kenkėjiškos internetu svetainės  
naudojant BDVIS

# BDVIS iš skirtingų naudotojų perspektyvos

## **Blokavimą inicijuojanti institucija**

Įveda domeną į BDVIS ir blokavimo teisėtumą pagrindžiančius dokumentus.

Gali automatinio būdu sužinoti ar interneto paslaugų teikėjas vykdo domeno blokavimo sankciją.

## **Interneto prieigos paslaugų teikėjas**

Automatiškai ir periodiškai pasiima blokuojamų domenų sąrašą.

Užblokuotas domenas tampa nebepasiekiamas klientams per mažiau nei 2 valandas.

# Sankcijos įgyvendinimo procesas per BDVIS

1. Blokavimą inicijuojanti institucija prideda blokuojamą domeną (ir subdomenus) bei sankciją pagrindžiančius dokumentus į BDVIS.



2. BDVIS tvarkytojas patikrina blokavimo atvejį ir jį patvirtina / atmeta.



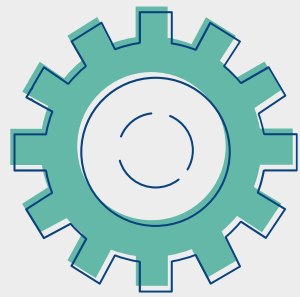
3. Interneto prieigos paslaugų teikėjas periodiškai pasiima patvirtintus blokuojamus domenus (ir subdomenus).



4. Blokavimą inicijavusi insitucija gali patikrinti, ar sankcija yra įgyvendinta.

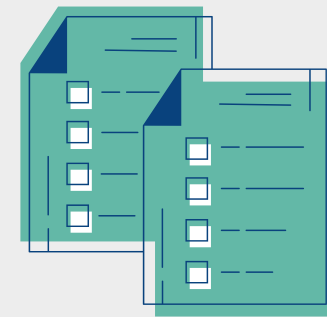


# BDVIS sudedamosios dalys



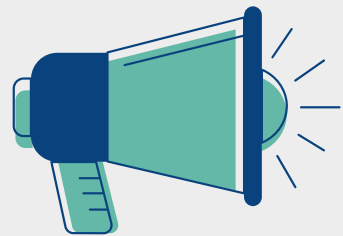
## 1. Valdymas

Blokavimą inicijuojančioms institucijoms pridėda blokuojamus domenus ir tokio blokavimo teisėtumą pagrindžiančius dokumentus. BDVIS tvarkytojuas patvirtina lokuojamus domenus.



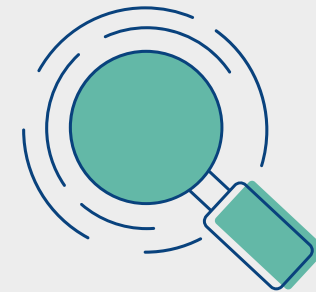
## 2. Perdavimas

Automatinis su sankcija blokuojamų domenų ir baltųjų domenų sąrašų perdavimas visiems interneto prieigos paslaugų teikėjams.



## 3. Informavimas

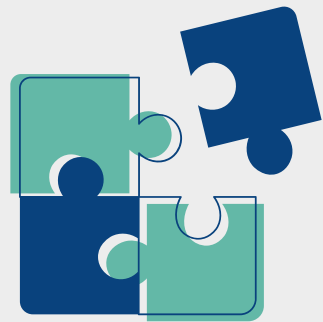
Informacinių puslapių su blokavimo priežastimi skirtų blokuojamų svetainių lankytojams generavimas bei visų blokuojamų domenų viešai pasiekiamo sąrašo generavimas.



## 4. Stebėseną

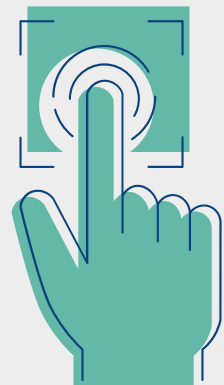
Periodiškai ir automatiškai tikrina ar interneto paslaugų teikėjai įvykdė domenų blokavimo sankcijas.

# BDVIS pagrindiniai principai



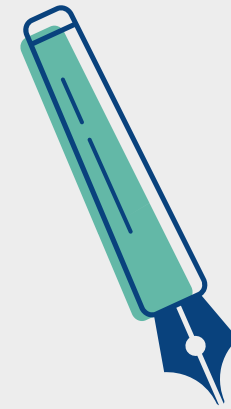
## 1. Naudojamumas

Visi Lietuvos interneto prieigos paslaugų teikėjai ir visos sankcionuotą domenų blokavimą inicijuojančios institucijos naudoja BDVIS.



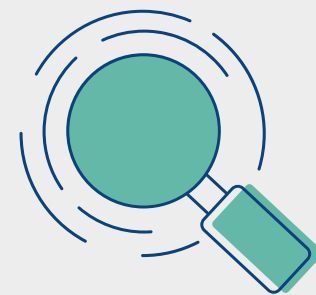
## 3. Greitis

BDVIS sistemoje patvirtintas blokuojamas domenas tampa nepasiekiamas visiems interneto prieigos paslaugų teikėjų DNS naudotojams per mažiau nei 2 valandas.



## 2. Atsakomybė

Interneto paslaugų teikėjai iš BDVIS gauna tik su sankcija blokuojamus domenus, kurių blokavimo faktas yra patvirtintas BDVIS tvarkytojo.



## 4. Skaidrumas

Galimybė automatiniu būdu sužinoti ar visi interneto prieigos paslaugų teikėjai vykdo domeno blokavimo sankciją. Taip pat blokuotos svetainės lankytojui pateikiama detali informacija apie svetainės blokavimo priežastį.

# Pagrindiniai teisiniai aspektai

## Privalomas BDVIS naudojimas

Atitinkamuose įstatymuose ir poįstatymiuose aktuose turėtų būti numatyta, kad visos interneto svetainės blokavimą galinčios inicijuoti valstybinės institucijos ir visi Lietuvoje veikiantys interneto prieigos paslaugų teikėjai turi naudotis šia informacine sistema. Taip pat bus numatomas pereinamasis laikotarpis.

## Atsakomybės numatymas dėl tinkamo BDVIS veikimo

Klaidingai, per aplaidumą ar dėl kibernetinės atakos neteisėtai užblokavus interneto svetainę, atsakomybę dėl padarytos žalos prisiima informacinės sistemos tvarkytojas arba neteisingai informaciją pateikusi valstybės institucija.

## Sankcija dėl neprisijungimo prie BDVIS

Interneto prieigos paslaugų tiekėjai, kurie nesinaudos BDVIS, bus baudžiami pagal Administracinių nusižengimų kodekse numatytas sankcijas.



# Pagrindiniai rizikų valdymo mechanizmai



## Domenų blokavimo fakto patikrinimas

BDVIS tvarkytojas patikrina domeno blokavimo atvejį ir jį patvirtina / atmeta.

## Domenų baltieji sąrašai

Interneto paslaugų teikėjai gautų baltųjų domenų sąrašus, kurie susidėtų iš populiariausių lietuviškų ir užsienietiškų interneto svetainių, kurių BDVIS pagalba nebūtų galima užblokuoti.

## Sistemos veiksmų stebėseną ir monitoringas

Visi BDVIS atliekami veiksmai yra registruojami, o pagrindiniai sistemos parametrai yra stebimi.

## Aukščiausi saugumo standartai ir ypatingos svarbos informacinės infrastruktūros statusas

Tiek domenų perdavimui, tiek sistemos veikimui keliami ypač aukšti saugumo reikalavimai.

# Tiesioginė BDVIS nauda

1

## **Greitesnis sankcijos įgyvendinimas**

Sankcijos įgyvendinimo laikas sutrumpėja nuo 5 d.d. (priklausomai nuo institucijos) iki **mažiau nei 2 val.**, sankcija vykdoma **24/7**.

3

## **Konkurencijos užtikrinimas**

Visi interneto prieigos paslaugų teikėjai sankcionuoti blokuoja tas pačias interneto svetaines dėl to užtikrinama konkurencija.

2

## **Sankcijų įgyvendinimo garantavimas**

BDVIS užtikrina sankcijos įgyvendinimo stebėseną dėl to nebelieka galimybės, kad interneto paslaugų teikėjai neužblokuos domeno ar vėluos tą padaryti.

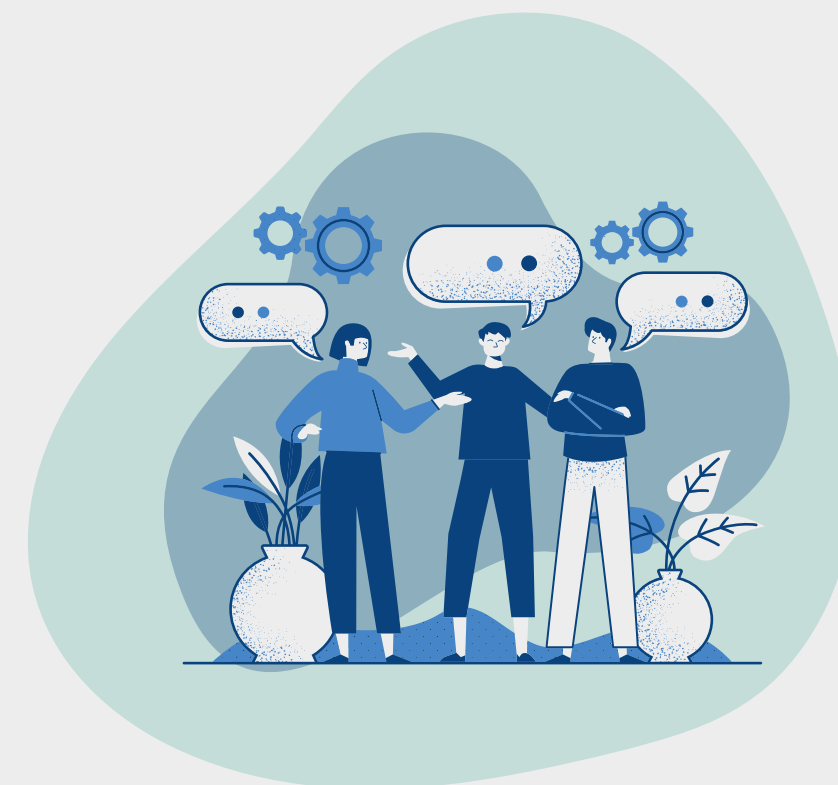
4

## **Administracinės naštos sumažinimas**

Visiems besinaudojantiems BDVIS sumažinama administracinė našta.

# Greitis itin svarbus užkardant nusikaltimuose elektroninėje erdvėje dalyvaujančias kenkėjiškas interneto svetaines

Igyvendinus BDVIS, Policija galės efektyviau naudoti 48 val. blokavimą iki teismo sprendimo, nes atsiras galimybė reaguoti realiu laiku į iškilusią grėsmę, pavyzdžiui, didžiulio masto duomenų viliojimo ataką (anlg. *phishing*).



# Svarstomos techninės BDVIS įgyvendinimo galimybės interneto prieigos paslaugų teikėjams (toliau IPPT)

Interneto prieigos paslaugų teikėjai kviečiami teikti  
motyvuotus pasiūlymus ir pastebėjimus.



# Blokuojamų domenu perdavimo IPPT įgyvendinimo galimybės

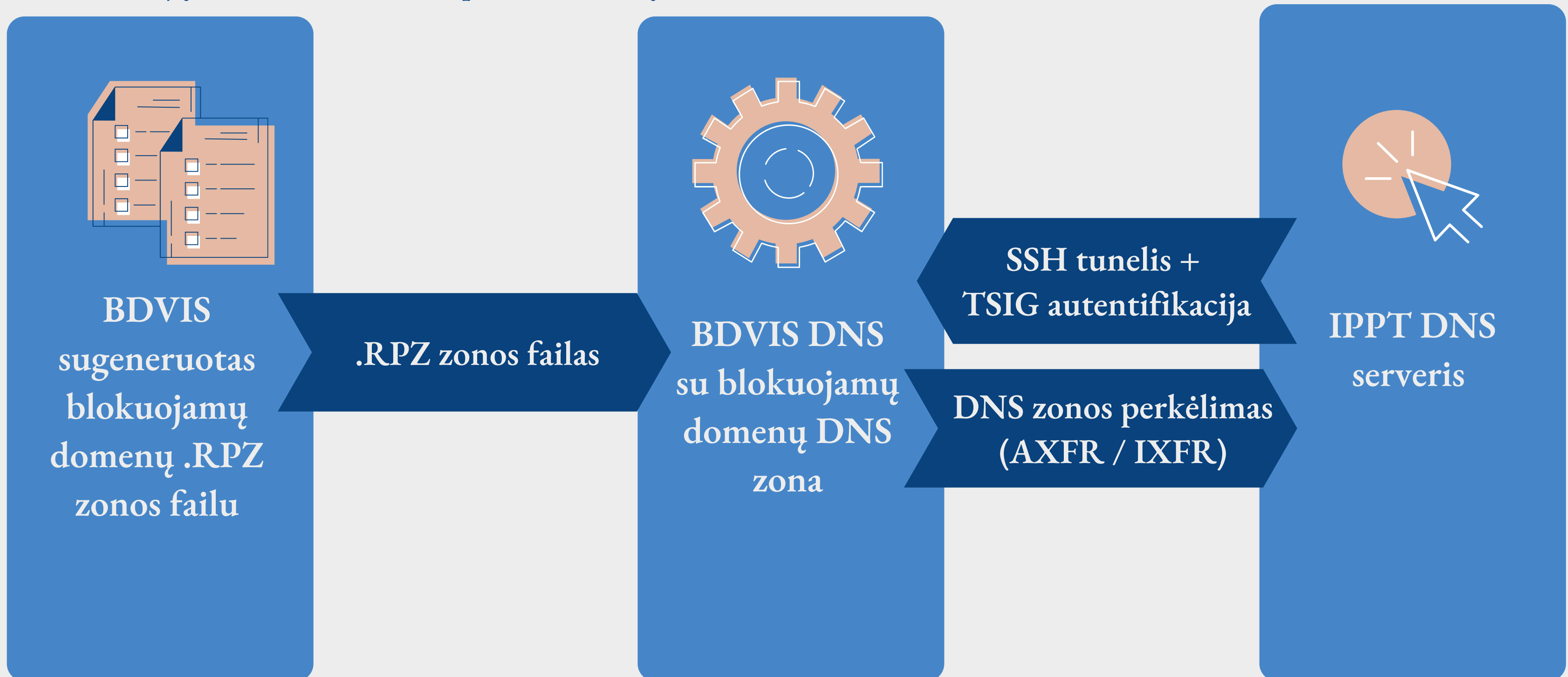
Su sankcija blokuojamų domenu perdavimas visiems interneto prieigos paslaugų teikėjams.





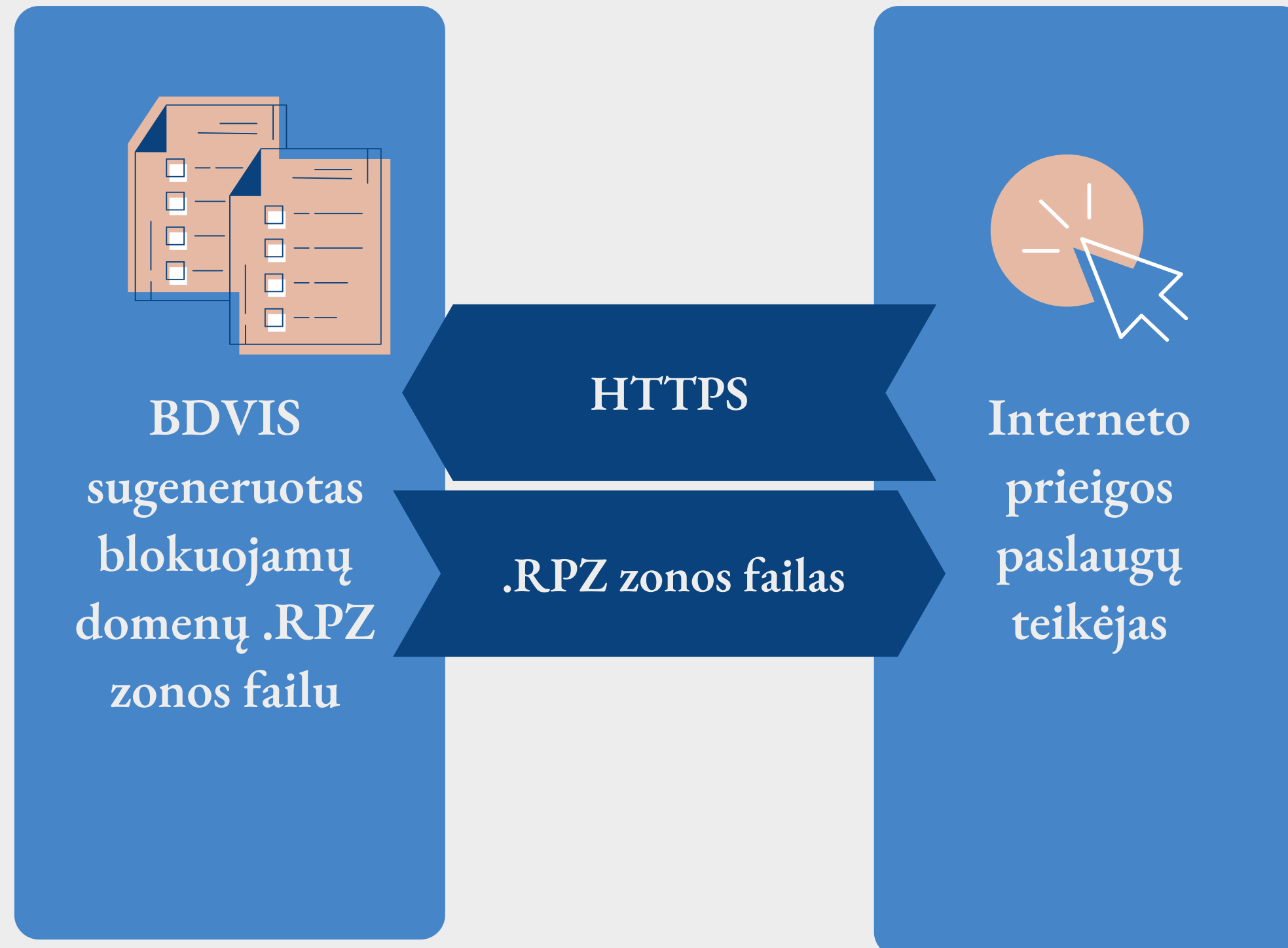
# 1 būdas: DNS zonos perkėlimas

IPPT atlieka DNS zonos perkėlimą iš BDVIS DNS į savo DNS serverius per AXFR/IXFR naudodami TSIG autentifikaciją (HMAC-SHA512) per SSH tunelį.



## 2 būdas: .RPZ failo atsisiuntimas

IPPT atsisiunčia .RPZ failą su blokuojamais domenais per HTTPS (ne rečiau nei kas 10 min) ir įkelia į savo DNS serverius. Prieiga prie atsisiuntimo serverio suteikiama iš konkrečių IPPT IP adresų.



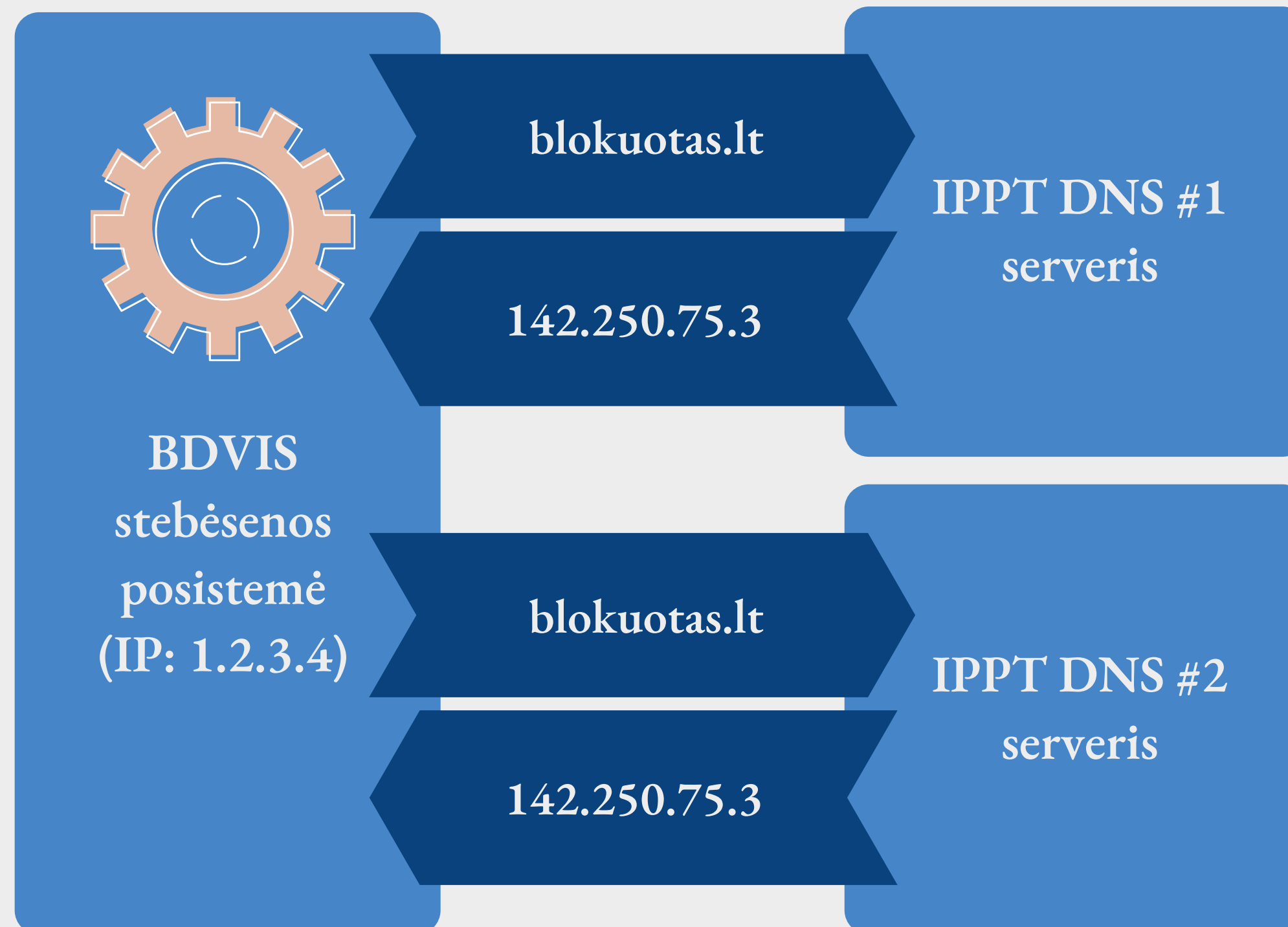
# IPPT Blokuojamų domenų stebėsenos įgyvendinimo galimybės

Galimybė patikrinti ar interneto prieigos paslaugų teikėjai vykdo domenų blokavimo sankcijas.



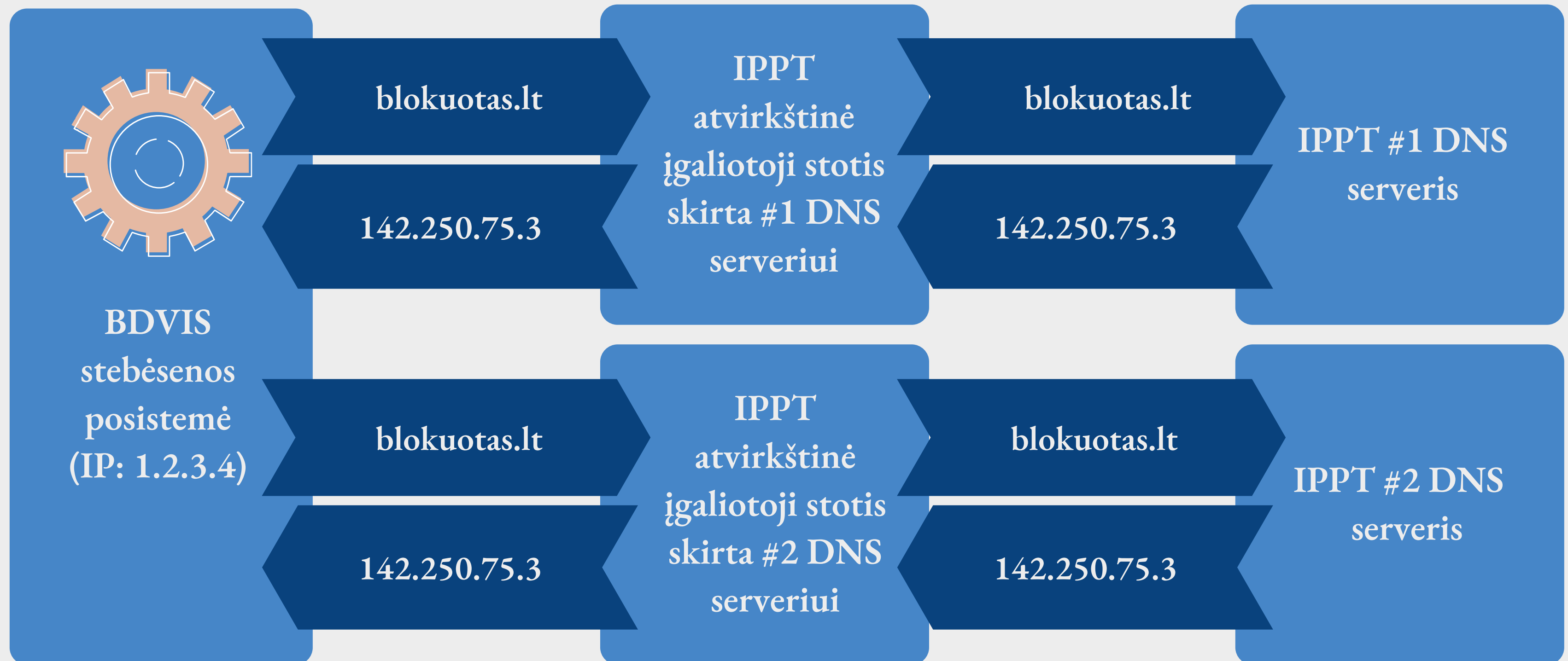
# 1 būdas: tiesioginė IPPT blokuojamų domenu stebėseną

IPT suteikia tiesioginę prieigą prie IPPT DNS iš BDVIS stebėsenos posistemės IP adreso (1.2.3.4) per 53 portą.



## 2 būdas: IPPT blokuojamų domenų stebėseną per atvirkštinę įgaliotoją stotį (angl. *reverse proxy*)

IPPT suteikia prieigą prie savo DNS serverių iš BDVIS stebėsenos IP adreso (1.2.3.4) per atvirkštines įgaliotąsias stotis ir 54 portą su SOCKS5 protokolu.



# Diskusija: koks BDVIS modelis būtų patogiausiai, efektyviausiai ir saugiausiai?

Kokie funkcionalumai yra būtini BDVIS?

Kokias rizikas yra būtina įvertinti  
įgyvendinant BDVIS?

Kokie techniniai/teisiniai reikalavimai turi  
būti užtikrinti įgyvendinant BDVIS?



# Kas toliau?



# Kaip bus panaudoti diskusijos rezultatai?

Apskritojo stalo diskusijos metu išsakyti pasiūlymai ir komentarai

Pasiūlymai ir komentarai pateikti raštu iki 2022 m. vasario 9 d.

Apskritojo stalo diskusijos ataskaita

BDVIS modelis

Rekomendacijų paketas



# BDVIS modelis

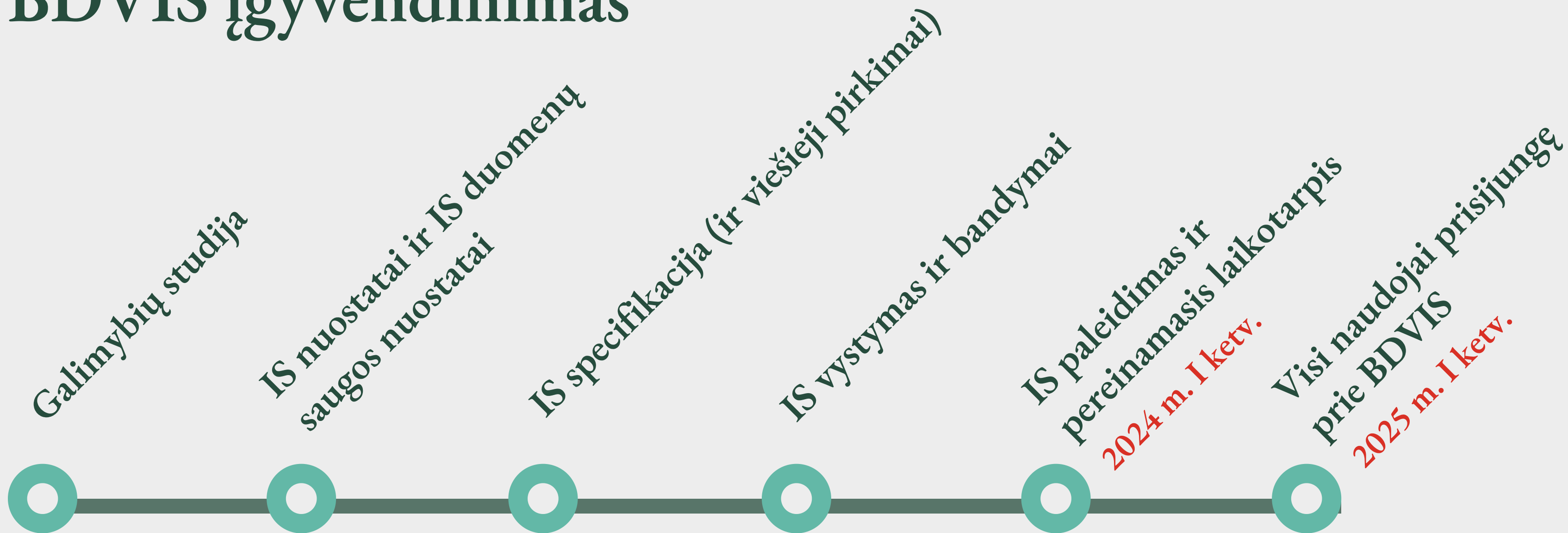
Tikslas – pagreitinti jau egzistuojantį sankcionuotą interneto svetainių blokavimo procesą, suteikti stebėjimo mechanizmą blokuojančioms institucijoms ir išvengti teismo sankcijos neįvykdymo.

Pagrindiniai uždaviniai:

- apibrėžti pagrindinius IS veikimo principus;
- numatyti IS valdytoją ir tvarkytoją;
- numatyti IS finansavimo šaltinį;
- numatyti, kokius reikės atlikti teisės aktų pakeitimus;
- pateikti rekomendacijas dėl tolimesnių žingsnių.



# BDVIS įgyvendinimas



Teisės aktų pakeitimai



# Diskusija: BDVIS įgyvendinimas

Kokius iššūkius matytumėte pereinant prie  
BDVIS naudojimo iš Jūsų institucijos  
perspektyvos?

Preliminariai vertinant, koks būtų reikalingas  
pereinamasis laikotarpis?



Renata Donauskytė

renata.donauskyte@kurklt.lt

[kurklt.lt](http://kurklt.lt)

Karolis Vyčius

karolis.vycius@kurklt.lt

[kurklt.lt](http://kurklt.lt)