Modelis

# Blokuojamų domenų valdymo informacinė sistema

Programos „Kurk Lietuvai“ projekto „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“ dalis

**Parengė Renata Donauskytė ir Karolis Vyčius**

**2022 m. vasaris**

Kurk Lietuvai

KRAŠTO APSAUGOS MINISTERIJA

# Turinys

# Įžanga

„Kurk Lietuvai“ projekto „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“ metu buvo iškeltas tikslas – numatyti papildomas priemones, skirtas saugoti gyventojus ir verslą nuo kenkėjiškų interneto svetainių sumažinant tokių svetainių pasiekiamumą ir laiko tarpą, reikalingą prieigai apriboti. Šiame dokumente bus apžvelgiama viena priemonė, kurios vystymui buvo skiriama daugiausia dėmesio projekto metu.

Pagal šiuo metu esantį teisinį reguliavimą, siekiant apsaugoti Lietuvos gyventojus nuo grėsmių elektroninėje erdvėje, 5 valstybinės institucijos pagal savo kompetenciją, tarp jų ir Lietuvos policijos, kaip kraštutinę priemonę gali inicijuoti interneto svetainės blokavimą. Įprastas interneto svetainės blokavimo procesas susideda iš keturių pagrindinių etapų: identifikavimo, tyrimo, sprendimo priėmimo ir vykdymo (žr. pav. 1). Atlikus procesų analizę, nustatyta, kad būtent blokavimo vykdymas, įgyvendinamas per Lietuvoje veikiančius interneto prieigos paslaugų teikėjus (toliau – IPPT), yra silpnoji dalis ir gali būti tobulinama pasitelkiant technines priemones.

Projekto metu išvystytas **Blokuojamų domenų valdymo informacinės sistemos** (toliau – BDVIS) modelis, centralizuodamas ir automatizuodamas interneto svetainės blokavimą, sudarys sąlygas greičiau ir efektyviau užkardyti ne tik kenkėjiškas, bet ir kitas interneto svetaines, naudojamas nusikalstamai bei nelegaliai veikai internete vykdyti. BDVIS tikslas – centralizuoti visų valstybinių institucijų, kurios įstatymu numatyta tvarka gali duoti privalomus nurodymus blokuoti interneto svetainę per IPPT, interneto svetainių blokavimo vykdymas procesą ir automatizuoti privalomų nurodymų vykdymą per Lietuvoje veikiančius IPPT.

BDVIS keliami uždaviniai: 1) sutrumpinti blokavimo vykdymą iki mažiau nei 2 val.; 2) užtikrinti blokavimo galimybę 24/7 režimu; 3) suteikti valstybinėms institucijoms įrankį stebėti, ar faktiškai yra įvykdomas blokavimas; 4) sumažinti administracinę naštą BDVIS naudotojams.

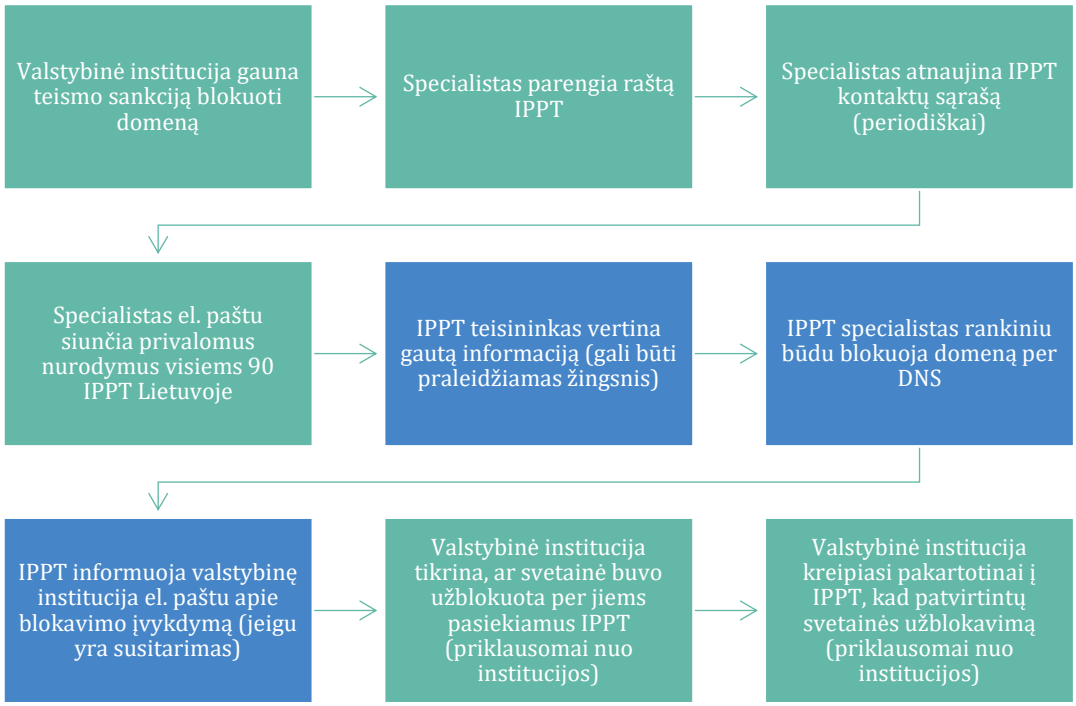
Atsižvelgiant į kitų šalių taikomas praktikas bei atliktų viešųjų konsultacijų rezultatus, šiame dokumente bus aptariami pagrindiniai BDVIS veikimo principai, sudedamosios dalys, reikalingi teisės aktų pakeitimai, kylančių rizikų valdymas, numatoma tokios informacinės sistemos nauda bei įgyvendinimo etapai. Šis modelis skirtas informacinės sistemos valdytojui bei tvarkytojui(-ams), kurie toliau vystys šį įrankį ir vertins galimas alternatyvas.


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

Pav. 1. Įprastas interneto svetainės blokavimo procesas.

# I. Poreikis

Šiuo metu interneto svetainių blokavimo vykdymas yra paremtas rankiniu darbu atliekant pasikartojančias užduotis ir neturint jokių patikimų įrankių patikrinti, ar realiai yra įvykdomas blokavimas (žr. pav. 2. Negana to, kiek IPPT užtruks įvykdyti privalomus nurodymus priklauso nuo jų vidaus tvarkos: vieni į procesą įtraukia teisininkus, kiti sutikrina gauto rašto informaciją su viešai institucijų puslapiuose skelbiama informacija, kai kurie IPPT visai netaiko papildomų kontrolės mechanizmų ir iškart blokuoja domeną. Abi proceso pusės – valstybinės institucijos ir IPPT – susiduria su tam tikrais iššūkiais vykdant blokavimo sankciją.




Pav. 2. Interneto svetainių blokavimo sankcijos vykdymo procesas.

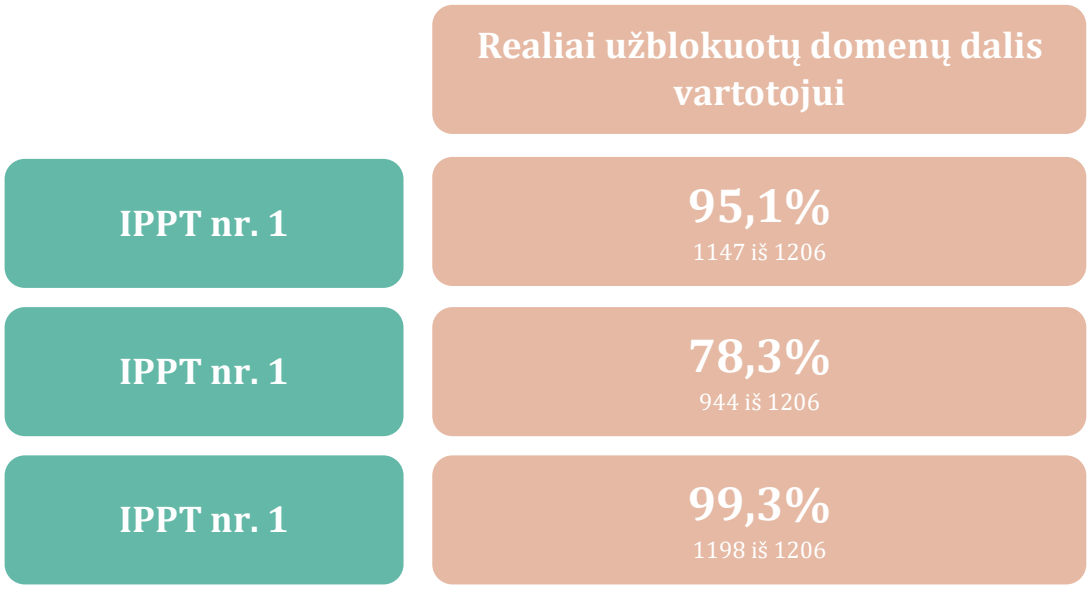
**Valstybinių institucijų patiriami iššūkiai:**

- ribotos galimybės patikrinti, ar tikrai domenas užblokuotas visų IPPT:
  - dažnai IPPT prašoma raštu patvirtinti, kad domenas yra užblokuotas, o tai reikalauja daug žmogiškųjų resursų, bet negarantuoja, kad nebus piktnaudžiaujama;
  - vienintelė galimybė įsitikinti, ar domenas tikrai buvo užblokuotas, yra naudojantis IPPT paslaugomis, t.y. esant klientu, tačiau tai reiškia, kad 5 valstybinės institucijos turi būti visų 90 IPPT klientais, todėl praktiškai yra labai sunku įgyvendinti. Vis dėlto kai kurios institucijos

tikrina tik didžiuosius IPPT, nes jie padengia didžiąją interneto vartotojų dalį Lietuvoje;
    - nėra techninių būdų patikrinti regioninius IPPT, nes paslauga teikiama tik konkrečioje teritorijoje.
- periodiškai reikia atnaujinti IPPT kontaktų sąrašą, todėl nauji IPPT nebūtinai iškart gaus nurodymus dėl privalomo blokavimo arba negaus ankstesnių sąrašų.

**Interneto prieigos paslaugų teikėjų patiriami iššūkiai:**

- kiekviena institucija teikia privalomus nurodymus skirtingu formatu, kuris ne visada yra patogus apdoroti, pasitaiko nesutapimų su viešai skelbiamais sąrašais, skiriasi įvykdymo terminai, todėl yra sunku optimizuoti darbą, sukuriama papildoma administracinė našta;
- nėra vieno bendro visų blokuojamų interneto svetainių sąrašo, kuris padėtų užtikrinti, kad visos interneto svetainės yra blokuojamos, pavyzdžiui, po atliktų IPPT DNS priežiūros darbų;
- ne visi IPPT gauna privalomus nurodymus el. paštu;
- viešai skelbiamų sąrašų IPPT nenaudoja dėl kelių priežasčių:
    - piktavaliai gali lengvai patalpinti netikrą informaciją į interneto svetainę, t.y. papildyti sąrašą neblokuotinais domenais;
    - nėra numatyti jokie saugumo mechanzimai;
    - sąrašai pateikiami skirtingais formatais ir ne visus galima nuskaityti automatiniu būdu;
    - nepateikiama visa reikalinga informacija (DNS CNAME įrašas), o sąrašas turi būti transformuojamas į IPPT DNS reikalingą formatą (DNS zoną reikalingą RPZ (angl. *response policy zone*) veikimui).




Pav. 3. Rezultatai patikrinus, kokią dalį domenų blokuoja 3 iš 5 didžiausių IPPT Lietuvoje 2021 m. lapkričio 29 d.

Taigi, dėl sąlyginai chaotiško proceso ir patiriamų iššūkių kyla **dvi pagrindinės problemos – kenkėjiškų interneto svetainių atveju blokavimas vykdomas per ilgai, o dalis domenų lieka neužblokuoti** (žr. pav. 3).

Kad būtų atliepti valstybinių institucijų, IPPT ir visuomenės poreikiai, BDVIS yra keliami šie pagrindiniai uždaviniai:

- sutrumpinti blokavimo vykdymą iki mažiau nei 2 val.;
- užtikrinti blokavimo galimybę 24/7 režimu;
- suteikti valstybinėms institucijoms įrankį stebėti, ar faktiškai yra įvykdomas blokavimas;
- sumažinti administracinę naštą BDVIS naudotojams.

# II. Įgyvendinimo ir veikimo principai

Atsižvelgiant į tai, kad interneto svetainių blokavimas yra jautrus klausimas žodžio ir saviraiškos laisvės bei laisvės veikti atžvilgiu, tokia priemonė turėtų būti taikoma tik kraštutiniais atvejais siekiant apsaugoti visuomeninį interesą. Kita vertus, norint užtikrinti gyventojų ir verslo saugumą užkardant kenkėjiškos veikos poveikį, yra būtina turėti efektyvias ir greitas priemones veikti, kai tai yra būtina. Taigi, galima teigti, kad kalbant apie interneto svetainių blokavimą susidaro įtampa tarp dviejų vertybių – žmogaus teisių ir saugumo. Siekiant subalansuoti šias dvi vertybes bei įgyvendinti BDVIS keliamus uždavinius, įgyvendinant BDVIS būtina atsižvelgti į šiuos principus: efektyvumas, atsakomybė, patikimumas, naudojamumas, atskaitomybė bei skaidrumas.

**Efektyvumas**

Užtikrintas didžiausias įmanomas greitis atsižvelgiant į būtinus saugumo elementus ir galimas rizikas

**Atsakomybė**

BDVIS naudojama blokuoti tik toms interneto svetainėms, kurias galima blokuoti pagal esantį teisinį reguliavimą

**Patikimumas**

BDVIS atitinka aukščiausius kibernetinio saugumo reikalavimus, užtikrinami saugikliai, kurie sumažintų žmogiškosios klaidos ar incidento poveikį

**Naudojamumas**

BDVIS privalo naudotis visi blokavimo procese dalyvaujantys subjektai, kad būtų sumažinta administracinė našta suvienodinant blokavimo procesą

**Atskaitomybė**

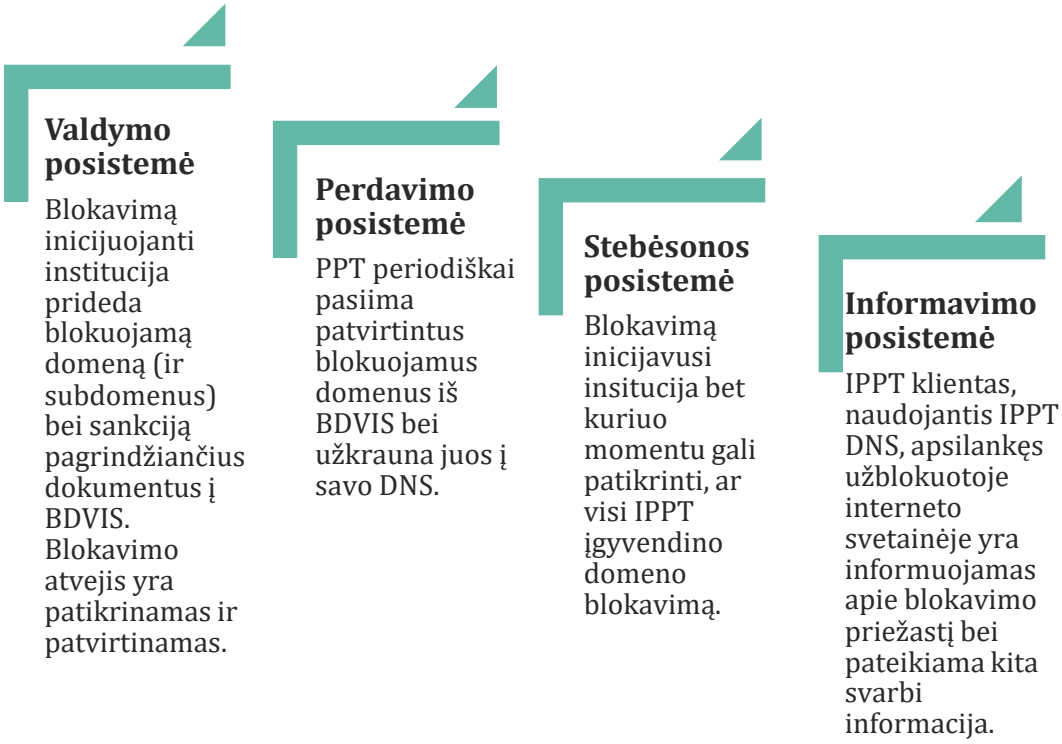
BDVIS užtikrina blokuojamų svetainių stebėsenos funkciją bei registruoja naudotojų atliekamus veiksmus, kad būtų užtikrinamas sąžiningas sistemos naudojimas

**Skaidrumas**

Palengvintas informacijos prieinamumą visuomenei apie tai, kokios ir kokiais atvejais yra blokuojamos interneto svetainės, informacija turi būti pateikiama viešai ir patogia forma

# III. Sudedamosios dalys

Šioje dalyje aptarsime pagrindines BDVIS sudedamąsias dalis: valdymo, perdavimo, informavimo, stebėsenos posistemes (žr. pav. 4). Verta pastebėti, kad BDVIS naudotojų autentifikavimo posistemė čia nebus aptarta ir rekomenduojama jos veikimą detalizuoti įgyvendinimo stadijoje.




Pav. 4. BDVIS veikimas ir sudedamosios dalys.

## a. Valdymo posistemė

Valdymo posistemės paskirtis yra centralizuoti blokavimą inicijuojančių institucijų domenų blokavimo atvejų valdymą.

**Blokavimą inicijuojančios institucijos specialistas į BDVIS įveda:**

- Domeno pavadinimas bei su juo susijusius subdomenus;
- Blokavimo priežastis ir teisės aktas, kurio pagrindu svetainė buvo užblokuota (pasirenkant iš sąrašo);
- Teismo nutarties numeris bei datą (jei blokuojama su teismo sankcija);
- Datą iki kada galioja blokavimas (jei data neįvedama, domenas blokuojamas neterminuotai);
- Pažymi, jeigu domeno blokavimo atvejis nėra viešinamas (tam tikrais atvejais gali būti sudaroma galimybė neviešinti blokuojamo domeno, pvz., policijai atliekant ikiteisminį tyrimą) ir nurodoma priežastis (pasirenkant iš sąrašo);
- Blokavimo teisėtumą pagrindžiančius dokumentus.

Šioje posistemėje blokavimą inicijuojančios institucijos specialistai mato savo institucijos pridėtus blokavimo atvejus. Gali sąrašą rikiuoti pagal teismo nutarties datą, blokavimo atvejo pridėjimo datą. Taip pat gali filtruoti pagal tai ar domeno blokavimo atvejis yra matomas viešai prieiname sąraše, ar domeno blokavimas nėra pasibaigęs.

BDVIS administratorius gali matyti visų blokavimą iniciuojančių institucijų blokuojamus domenus ir teisėtumą pagrindžiančius dokumentus. Taip pat galima numatyti domenų blokavimo atvejo papildomą patikrinimo funkciją (plačiau žr. V skyrius „Rizikų valdymas“).

Galiausiai yra suformuojamas bendras ir aktualus visų blokavimą inicijuoti galinčių institucijų blokuojamų domenų sąrašas ir parengiamas perdavimui IPPT.

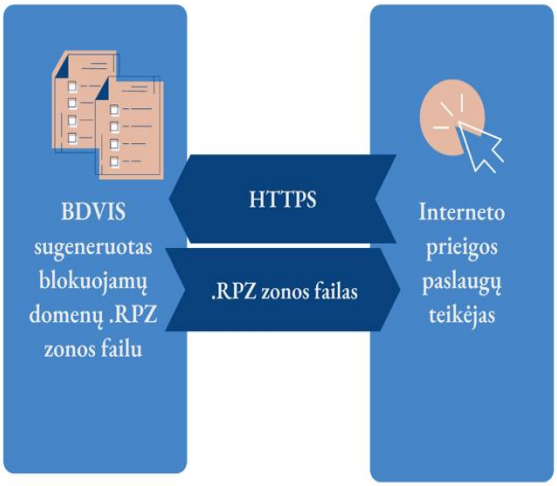
## b. Perdavimo posistemė

Perdavimo posistemės paskirtis yra automatiškai perduoti blokuojamų domenų ir baltųjų domenų sąrašus (daugiau apie baltuosius domenų sąrašus žr. V skyrius „Rizikų valdymas“ rizikų) visiems Lietuvoje veikiantiems IPPT. Perdavimo funkciją galima įgyvendinti keliais būdais ar suteikti IPPT galimybę pasirinkti priimtiniausią variantą.

### *Perdavimo įgyvendinimo būdai*

**1 būdas: .RPZ failo atsiuntimas per HTTPS**

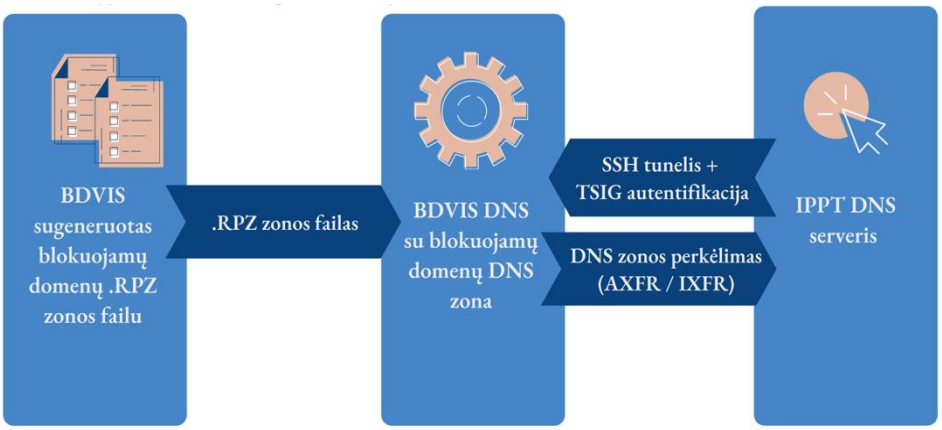
Pirmasis perdavimo būdas suteikia galimybę IPPT atsiųsti .RPZ failą su visų blokavimą inicijuojančių institucijų blokuojamais domenais per HTTPS ir patiems jį įkelti į savo DNS serverius (žr. pav. 5). Rekomenduojama failą atsisiųsti ir į IPPT DNS įkelti ne rečiau nei kas 10 min. Prieigai valdyti prie serverio su BDVIS sugeneruotu .RPZ failu būtų galima prisijungti tik iš konkrečių IPPT IP adresų.




Pav. 5: Blokuojamų domenų perdavimas per HTTPS veikimas

**2 būdas: DNS zonos perkėlimas**

Siekiant maksimizuoti blokuojamų domenų perdavimo procesą galima naudoti DNS zonos perkėlimo (angl. *DNS Zone Transfer, AXFR*) arba inkrementinio DNS zonos perkėlimo (angl. *Incremental Zone Transfer, IXFR*) mechanizmus (žr. pav. 6). *IXFR* kartu su pranešimu apie zonos pakeitimą (angl. *DNS NOTIFY*) naudojimas leistų pasiekti blokuojamų IPPT domenų atnaujinimą vos per kelias sekundes. Siekiant šifruoti perduodamus duomenis bei užtikrinti, kad DNS serveris nebūtų pasiekiamas iš išorės rekomenduojama apsvarstyti SSH tunelio būtinybę. Priklausomai nuo kitų pasirinktų mechanizmų, autentifikavimui gali būtų naudojamas DNS slaptasis raktas operacijos autentifikavimui (angl. *Transaction Signature, TSIG*) su HMAC-SHA512 šifravimu.




Pav. 6. Blokuojamų domenų perdavimas per DNS zonos perkėlimą

## *Perdavimo įgyvendinimo būdų vertinimas*

Remiantis viešųjų konsultacijų metu surinkta informacija bei perdavimo būdų vertinimu (žr. pav. 7), negalima vienareikšmiškai teigti, kuris įgyvendinimo būdas yra geresnis. Nors pirmasis perdavimo būdas (.RPZ failo atsiuntimas per HTTPS) pasižymi mažesniu perdavimo greičiu, tačiau IPPT suteikia didesnę kontrolę ir BDVIS įgyvendintojui yra paprastesnis lyginant su antruoju būdu (DNS zonos perkėlimas). Priimant galutinį sprendimą dėl perdavimo įgyvendinimo rekomenduojama atsižvelgti į reikalingą perdavimo greitį bei galimybę IPPT diegti papildomas automatines rizikos valdymo priemones.

| | Perdavimo būdas | Vertinimas | |
|---|---|---|---|
| Domenų perdavimo būdai | **1. .RPZ failo atsiuntimas per HTTPS** | **Perdavimo greitis:** apie 10 minučių; | ◑ |
| | | **Įgyvendinimo lengvumas IPPT pusėje:** reikalinga programa, kuri periodiškai gautų .RPZ failą per HTTPS ir įkeltų į DNS; | ◑ |
| | | **Įgyvendinimo lengvumas BDVIS pusėje**: žiniatinklio serveris (pvz., su Nginx ar Apache HTTP); | ● |
| | | **Palaikymo kaštai BDVIS pusėje**: IPPT IP adresų prieigai administravimas ir žiniatinklio serverio priežiūra; | ● |
| | | **Rizikų valdymo mechanizmai IPPT pusėje:** baltieji domenų sąrašai taip pat IPPT gali integruoti papildomus automatinius rizikų valdymo mechanizmus. | ● |
| | **2. DNS zonos perkėlimas** | **Perdavimo greitis:** per kelias sekundes (IXFR kartu su pranešimu apie zonos pakeitimą atveju); | ● |
| | | **Įgyvendinimo lengvumas IPPT pusėje**: SSH tunelis ir DNS zonos pridėjimas; | ● |
| | | **Įgyvendinimo lengvumas BDVIS pusėje**: bent du DNS serveriai, DNS serverio programinė įranga (pvz., BIND) ir sertifikatų valdymo sistema; | ◑ |
| | | **Palaikymo kaštai BDVIS pusėje**: sertifikatų valdymas, DNS infrastruktūros priežiūra; | ◑ |
| | | **Rizikų valdymo mechanizmai IPPT pusėje**: tik baltieji domenų sąrašai. | ◑ |

● Atitinka ◑ Iš dalies atitinka

Pav. 7. Domenų perdavimo IPPT būdų vertinimas.

## c. Informavimo posistemė

Informavimo posistemės paskirtis yra blokuojamos svetainės lankytojui generuoti aiškius, detalius, suprantamus informacinius blokavimo puslapius. Taip pat automatiškai pateikti blokuojamų domenų sąrašą.

### *Informacinis blokavimo puslapis*

Šiuo metu kiekviena blokavimą inicijuojanti institucija skirtingai pateikia informaciją apie užblokuotą interneto svetainę lankytojui. BDVIS informavimo posistemė suvienodintų informacijos pateikimą ir visų blokavimą inicijuojančių institucijų informacinius blokavimo puslapius.

Į informacinį blokavimo puslapį lankytojai patenka IPPT DNS gražinus šio puslapio DNS įrašą, vietoje originalaus DNS įrašo. Rekomenduojama, kad blokavimo puslapis būtų prieinamas keliomis kalbomis (lietuvių, anglų, rusų). Kalba parenkama automatiškai pagal *Accept-Language* HTTP headerį, tačiau sudaroma galimybė kalbą pasikeisti. Taip pat puslapis turi būti pritaikytas asmenims su negalia.

**Informaciniame blokavimo puslapyje turėtų pateikiama tokia informacija:**

- Domeno pavadinimas
- Blokavimo priežastis ir teisės aktas, kurio pagrindu svetainė buvo užblokuota;
- Teismo nutarties numeris ir data;
- Domeno užblokavimo data;
- Blokavimą inicijavusios institucijos pavadinimas, nuoroda į institucijos puslapį, atsakingo asmens el. paštas ir kontaktai;
- Instrukcija, ką daryti, jeigu manoma, kad svetainė yra per klaidą užblokuota (nurodoma kreiptis į blokavimą inicijavusią instituciją);
- Nuoroda į bendrą blokuojamų domenų sąrašą.

### *Viešai prieinamas blokuojamų domenų sąrašas*

Šiuo metu blokavimą iniciuojančios institucijos atskirai skelbia blokuojamų domenų sąrašus bei juose pateikia skirtingą informaciją. Lietuvos gyventojai negali patogia forma vienoje vietoje gauti informaciją apie visas blokuojamas interneto svetaines. Siekiant skaidrumo ir norint sudaryti galimybę analizuoti duomenis, yra reikalingas bendras, viešai prieinamas blokuojamų domenų sąrašas. BDVIS informavimo posistemės generuojamas viešai prieinamas blokuojamų domenų sąrašas suvienodintų informacijos pateikimą.

**Viešai skelbiami blokuojamų domenų sąrašų nuorodos:**

- Lietuvos bankas
- Lietuvos radijo ir televizijos komisija
- Lošimų priežiūros tarnyba prie Lietuvos Respublikos finansų ministerijos
- Valstybinė vartotojų teisių apsaugos tarnyba
- Lietuvos policija neskelbia tokių sąrašų

Viešai prieinamas blokuojamų domenų sąrašas būtų rodomi visi patvirtinti užblokuoti domenai, kurie yra viešai skelbiami. Sąrašas būtų surikiuotas pagal domeno užblokavimo data mažėjančiai. Taip pat sąrašas palaikytų filtravimo funkciją bei sudaroma galimybė sąrašą atsisiųsti .csv formatu, kuris leistų patogiai analizuoti duomenis.

**Bendrame blokuojamų domenų sąraše pateikiama informacija:**

- Domeno pavadinimas;
- Blokavimo priežastis ir teisės aktas, kurio pagrindu svetainė buvo užblokuota;
- Teismo nutarties kodą bei datą;
- Blokavimą inicijavusios institucijos pavadinimas;
- Domeno užblokavimo data ir laikas;
- Domeno atblokavimo data ir laikas (jei blokuojama terminuotai).

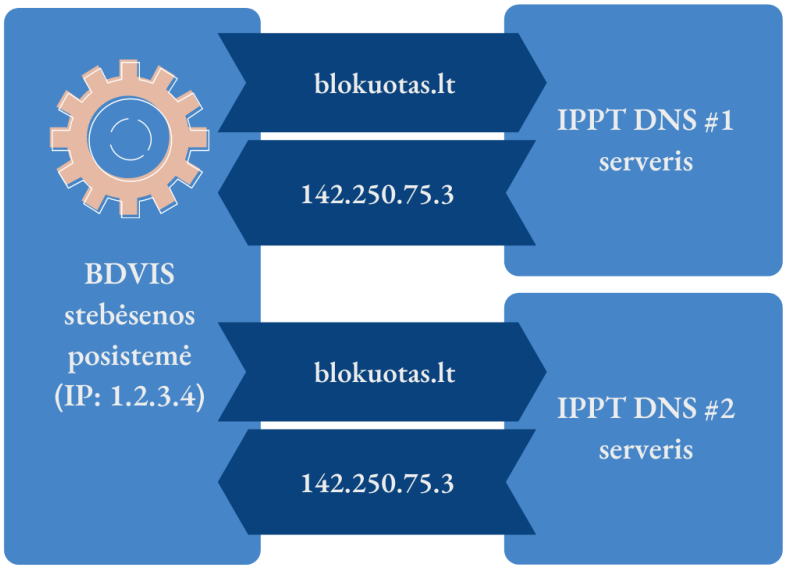
## d. Stebėsenos posistemė

Stebėsenos posistemės paskirtis yra automatiškai ir periodiškai tikrinti IPPT domenų blokavimo vykdymą. BDVIS tvarkytojas administruotų IPPT DNS IP adresus, kuriuos tikrintų stebėsenos posistemė. Taigi, naudojant šią posistemę, blokavimą inicijuojančios institucijos gali patikrinti, ar IPPT realiai užblokavo domeną.

### *Stebėsenos įgyvendinimo būdai*

**1 būdas: tiesioginė blokuojamų domenų stebėsena per IPPT DNS**

Tiesioginei IPPT blokuojamų domenų stebėsenai įgyvendinti reikalinga susitarimas su IPPT dėl prie IPPT DNS iš BDVIS stebėsenos posistemės. Turint tokią prieigą BDVIS stebėsenos posistemė su kiekvienu blokuojamu domenu periodiškai per 53 prievadą kreiptųsi į visus IPPT DNS, kurie gražintų domeno IP adresą. Pagal tai, ar gražintas IP adresas yra informacinio blokavimo puslapio IP adresas, BDVIS stebėsenos posistemė nustatytu, ar domenas buvo užblokuotas (žr. pav. 8).

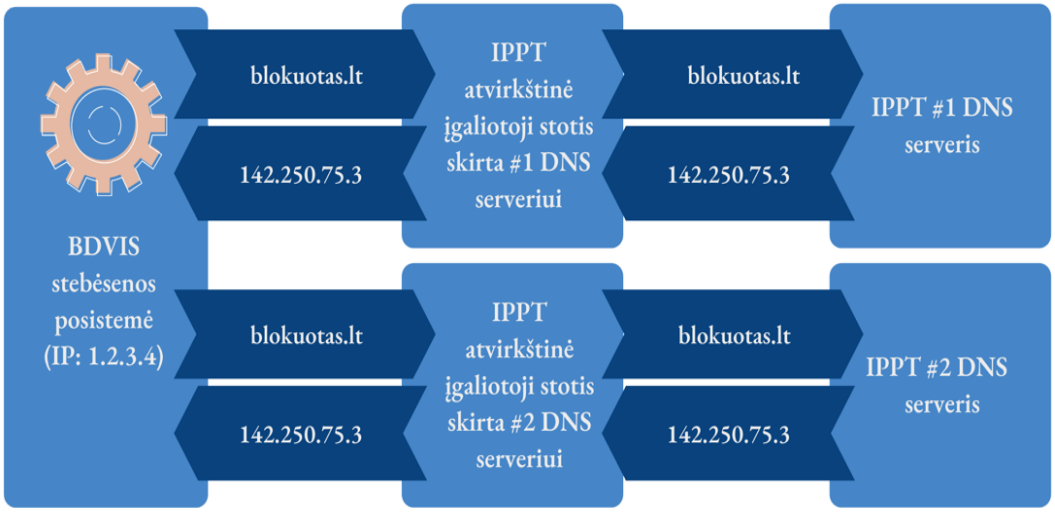



Pav. 8. Tiesioginė blokuojamų domenų stebėsena per IPPT DNS.

Suteikti prieigą prie IPPT DNS galima skirtingais techniniais būdais. Viešųjų konsultacijų metu pagrindinis vertintas būdas buvo prieigos prie IPPT DNS atvėrimas iš BDVIS stebėsenos posistemės IP adreso. Vystymo metu rekomenduojama įvertinti ir kitas prieigos suteikimo alternatyvas bei tikrinimo periodiškumą.

**2 būdas: blokuojamų domenų stebėsena per IPPT DNS su atvirkštine įgaliotoja stotimi**

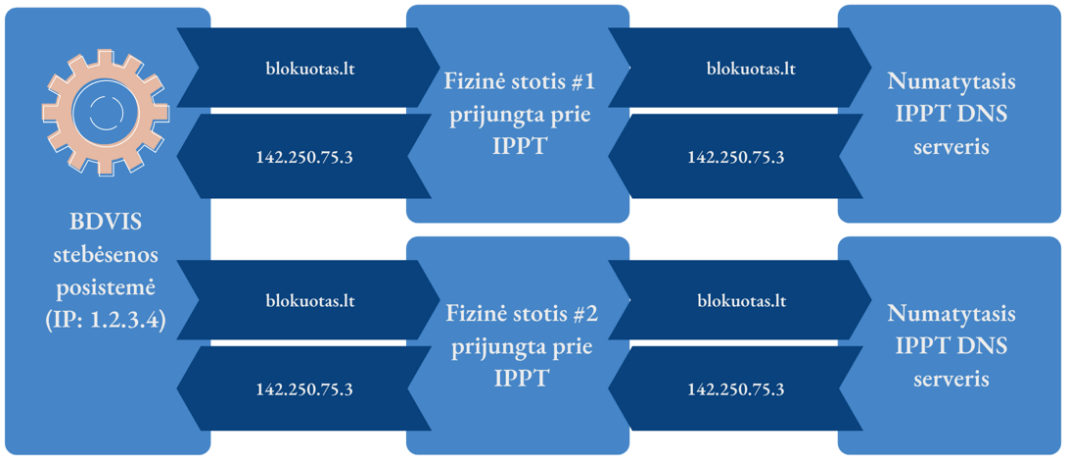
Antrasis blokuojamų domenų stebėsenos būdas yra labai panašus į pirmąjį stebėsenos įgyvendinimo būdą, tačiau vietoj jungimosi prie IPPT DNS serverio tiesiogiai yra naudojama IPPT sukurta atvirkštinė įgaliotoji stotis (angl. *reverse proxy*) veikianti pagal SOCKS5 protokolą (žr. pav. 9).




Pav. 9. Blokuojamų domenų stebėsena per IPPT DNS su atvirkštine įgaliotoja stotimi.

**3 būdas: Blokuojamų domenų stebėsena imituojant IPPT klientą**

Abu prieš tai aptarti stebėsenos būdai reikalauja pakeitimų iš IPPT pusės. Atliekant blokuojamų domenų patikrinimą taip pat galima imituoti IPPT klientą t.y. per fizines stotis prisijungus prie IPPT paslaugų, su domenu kreiptis į numatytąjį IPPT DNS serverį ir pagal gražintą IP adresą patikrinti ar šis domenas yra užblokuotas (žr. pav. 10).

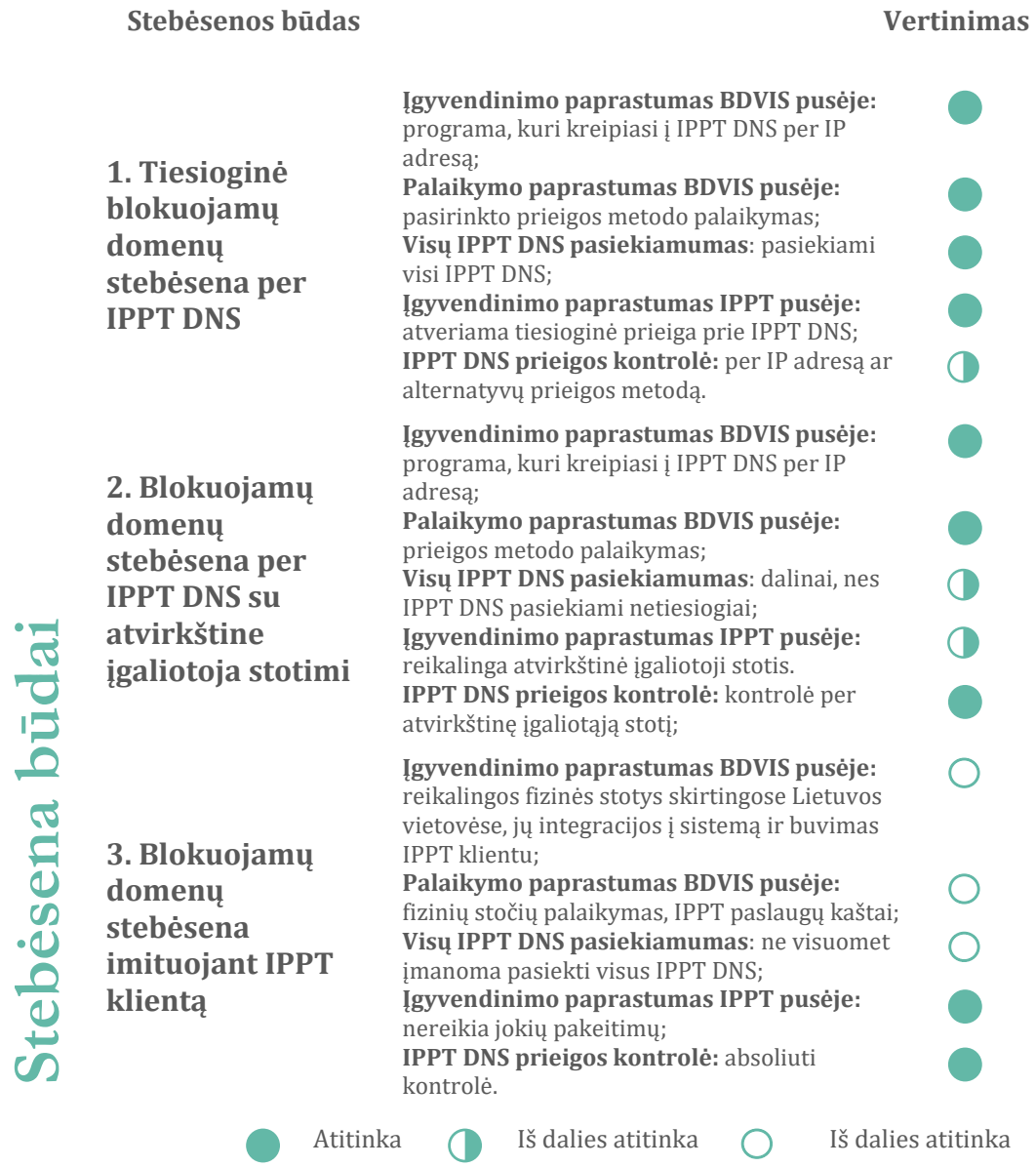



Pav. 10. Blokuojamų domenų stebėsena per IPPT DNS su atvirkštine įgaliotoja stotimi

## *Stebėsenos įgyvendinimo būdų vertinimas*

Remiantis viešųjų konsultacijų metu surinkta informacija bei IPPT blokuojamų domenų stebėsenos būdų vertinimu (žr. pav. 11), rekomenduojama pasirinkti 1 būdą (tiesioginė blokuojamų domenų stebėsena per IPPT DNS). Šis būdas yra sąlyginai paprastai įgyvendinamas kuriant BDVIS bei garantuoja visų IPPT DNS pasiekiamumą.

Taip pat rekomenduojama argumentuotu IPPT prašymu (pvz., IPPT infrastrūktos ypatybių) sudaryti galimybę naudoti ir 2 būdą (blokuojamų domenų stebėsena per IPPT DNS su atvirkštine įgaliotoja stotimi). Šis būdas suteikia didesnę kontrolę IPPT, tačiau sudaro mažą galimybę, kad ne visi IPPT DNS bus pasiekiami.




Pav. 11. IPPT blokuojamų domenų stebėsenos būdų vertinimas.

Verta pastebėti, kad siekiant įgyvendinti 3 būdą (blokuojamų domenų stebėsena imituojant IPPT klientą) būtų reikalingas fizinis prisijungimas prie kiekvieno Lietuvoje veikiančio IPPT iš skirtingų Lietuvos vietų (dėl DNS apkrovos balansavimo, kuris dažnai vykdomas pagal kliento vietą). Vis dėlto, šis sprendimas neatiktų BDVIS skaidrumo principo t.y. net turint fizinę prieigą prie IPPT ne visuomet būtų įmanoma pasiekti visus IPPT DNS, o tik numatytuosius. Dėl šios priežasties šis būdas nėra tinkamas realaus laiko stebėsenai vykdyti ir rekomenduojama rinktis prieš tai aptartus metodus. Vis dėlto, esant poreikiui, tokį stebėsenos būdą galima taikyti periodiniams blokuojamų domenų patikrinimas. Periodiškai (pvz., kas pusę metų) būtų prisijungiama prie IPPT tinklo ir imituojant galutinį klientą patikrinama, kurie domenai yra blokuojami. Tokia priemonė galėtų būti taikoma blokuojamų domenų patikrai jau dabar.

# IV. Teisiniai aspektai

Siekiant, kad BDVIS galėtų pilnavertiškai funkcionuoti bei būtų užtikrinti išsikelti veikimo principai – naudojamumas, atsakomybė, greitis ir skaidrumas – bus reikalingi teisės aktų pakeitimai, kurie užtikrintų šių principų įgyvendinimą.

## a. Dabartinio teisinio reguliavimo vertinimas

BDVIS yra viena iš priemonių, skirtų užkardyti nusikaltimus elektroninėje erdvėje bei šalinti jų poveikį. Šia priemone pagal savo kompetenciją naudosis skirtingos valstybinės institucijos, kurios turi įgaliojimus duoti privalomus nurodymus dėl interneto svetainių blokavimo per interneto prieigos paslaugų teikėjus. Šie įgaliojimai yra suteikti pagal skirtingus įstatymus[1], institucijos nėra tarpusavyje susijusios tiesioginiu pavaldumu, o ateityje gali būti ir daugiau institucijų, kurioms bus suteikti tokie pat įgaliojimai. Visa tai kelia papildomų iššūkių siekiant apibrėžti BDVIS steigimo teisinį pagrindą bei nustatyti kitas reikalingas teisines nuostatas.

Vienas iš iššūkių – didelis skaičius įstatymų ir poįstatyminių aktų, kuriuos reikėtų atnaujinti. Kitas iššūkis susijęs su tuo, kad nebūtinai užtektų atnaujinti tik dabartinius teisės aktus, kuriuose yra reguliuojami atvejai, kada gali būti duodami privalomi nurodymai blokuoti interneto svetainę. Pavyzdžiui, norint įtvirtinti nuostatą, kad visos institucijos, turinčios įgaliojimus duoti nurodymus blokuoti, privalo tai vykdyti per BDVIS, reikalingas bendras teisės aktas, kuriame būtų reguliuojamas visas nusikaltimų elektroninėje erdvėje užkardymo procesas.

## b. Reikalingos teisinės nuostatos

### *Privalomas naudojimasis BDVIS*

Norint užtikrinti, kad **BDVIS** būtų veiksminga ir realiai sumažintų administracinę naštą visiems proceso dalyviams, ji **turi būti naudojama visų Lietuvoje veikiančių IPPT ir valstybinių institucijų, kurios duoda privalomus nurodymus blokuoti domeną**. Jeigu liks neprisijungusių IPPT prie šios sistemos, tada nebus pasiektas veiksmingumo tikslas, kad visi domenai būtų vienodai blokuojami visų IPPT. Jeigu liks valstybinės institucijos, kurios neprisijungs prie bendros sistemos ir toliau siųs nurodymus el. laiškais, tokiu atveju nesumažės administracinė našta IPPT ir verslo subjektai turės mažiau paskatų naudotis IPPT. Apibendrinant, privalomas BDVIS naudojimas yra kertinis elementas norint užtikrinti sistemos pilnavertišką funkcionavimą.

Atsižvelgiant į tai, kaip svarbu, kad visi proceso dalyviai naudotųsi BDVIS, yra reikalingi tokie teisės aktų pakeitimai, kad būtų numatyta, jog visos institucijos tiek šiuo metu inicijuojančios blokavimą, tiek ateityje gausiančios tokią teisę, naudotųsi BDVIS. Siekiant užtikrinti visų IPPT prisijungimą prie informacinės sistemos, Administracinių nusižengimų kodekse turi būti nustatytos sankcijos dėl šio reikalavimo nevykdymo.

[1] Lietuvos Respublikos Lietuvos banko įstatymas, Lietuvos Respublikos azartinių lošimų įstatymas, Lietuvos Respublikos švietimo įstatymas, Lietuvos Respublikos vartotojų teisių apsaugos įstatymas, Lietuvos Respublikos autorinių teisių ir gretutinių teisių įstatymas.

### *Atsakomybė dėl klaidos ar įvykusio incidento*

Net ir skiriant itin daug dėmesio kibernetinio saugumo užtikrinimui įgyvendinant BDVIS, visada lieka tikimybė, kad bus padaryta žmogiškoji klaida ar įvykdyta kibernetinė ataka prieš informacinę sistemą. Kadangi BDVIS veiks centralizuotai ir automatiškai, klaidos ar incidento atveju gali būti padaryta didelė žala tiek viešojo, tiek privataus sektoriaus subjektams. Atsižvelgiant į tai, yra būtina sudėti tiek techninius saugiklius (daugiau žr. „Rizikų valdymo priemonės“), tiek teisines garantijas.

Keičiant teisės aktus yra būtina numatyti, **kad atsakomybę dėl padarytos žalos prisiimtų institucija ar asmuo, dėl kurio klaidos ar aplaidumo buvo padaryta žala.** Pavyzdžiui, jeigu valstybinės institucijos specialistas padaro klaidą įvesdamas duomenis į BDVIS, tada valstybinė institucija atsako už padaryta žalą, o ne IPPT, kurie įgyvendino gautą nurodytą per BDVIS. Tam, kad būtų galima atsekti padarytą klaidą arba incidentą, BDVIS bus registruojami visi veiksmai ir prireikus bus galima peržiūrėti įrašus.

# V. Rizikų valdymas

BDVIS įgyvendinimas centralizuotų ir automatizuotų blokavimo procesą t.y. IPPT iš vienos vietos pasiimtų visą blokuojamų interneto svetainių sąrašą ir automatiški visas sąraše esančias svetaines padarytų nebepasiekiamas jų klientams. Visada egzistuoja tikimybė, kad domenas bus užblokuotas per klaidą arba bus įvykdyta kibernetinė ataka nukreipta prieš BDVIS. Dėl centralizuoto ir automatizuoto blokavimo, **įvykęs incidentas paveiktų visus Lietuvoje veikiančius IPPT ir jų klientus, todėl būtina labai atsakingai vertinti rizikas** ir ieškoti sprendimų, kurie leistų jas minimizuoti. Toliau pateikiamos kelios galimos rizikų valdymo priemonės siekiant minimizuoti BDVIS keliamas rizikas.

### *Blokavimo atvejo papildomas patikrinimas*

Blokavimą inicijuojančiai institucijai, kuriant naują blokavimo atvejį ar keičiant jau egzistuojantį blokavimo atvejį, gali būti padaryta žmogiškoji klaida, pavyzdžiui, įvestas neteisingas domeno vardas, nepateikti visi reikalingi blokavimo teisėtumą pagrindžiantys dokumentai. Siekiant minimizuoti žmogiškosios klaidos riziką, susijusią su blokavimo atvejų kūrimu ar atnaujinimu, rekomenduojama įgyvendinti papildomą blokavimo atvejo patikrinimo mechanizmą.

Papildomas blokavimo atvejo patikrinimas galėtų būti atliekamas po to, kai blokavimo atvejis buvo sukurtas ar atnaujintas. Tai galėtų atlikti BDVIS administratorius arba antras asmuo blokavimą inicijuojančioje institucijoje, pavyzdžiui, specialisto tiesioginis vadovas arba įstaigos vadovas (žr. pav. 12).

Palyginimas

| BDVIS administratorius | Antras asmuo institucijoje |
|---|---|
| Užtikrinamas nešališkumas, nes patikrinimą vykdo trečioji, nesuinteresuotoji šalis. | Paliekama daugiau galimybių piktnaudžiauti sistema institucijos lygmeniu. |
| Reikalingas papildomas specialistas, kuris gebėtų įvertinti, ar tinkamai pateikta informacija sistemoje ir atvejį pagrindžiantys dokumentai. | Tikimybė, kad patikrinimas bus atliekamas formaliai. |
| Papildomi kaštais užtikrinant darbą 24/7 režimu. | Daugiau laisvės institucijoms optimizuojant procesą. |
| Užklausos būtų vykdomos eilės, o ne prioriteto tvarka, todėl galėtų išsitęsti procesas. | Institucija gali apsispręsti suteikti didesnį prioritetą ir koordinuoti tarpusavyje veiksmus, todėl procesas gali sąlyginai greičiau vykti. |

Pav. 12. Blokavimo atvejo papildomo patikrinimo alternatyvų palyginimas.

Papildomas patikrinimas suteiktų daugiau garantijų IPPT, kad į sistemą pateks tik įstatymo nustatyta tvarka blokuojami domenai, būtų sumažinta žmogiškosios klaidos tikimybė, tačiau papildomas žingsnis sulėtintų visą procesą ir sukurtų daugiau administracinės naštos ir finansinių kaštų. Papildomas patikrinimas kaip rizikų valdymo priemonė turėtų būti vertinama bendrame rizikų valdymo kontekste bei susitarus tarp suinteresuotųjų šalių, koks rizikos lygis yra toleruotinas neprarandant BDVIS efektyvumo.

### *Pripažinimas ypatingos svarbos informacine infrastruktūra*

Įvykus didelio mąsto sutrikimui, BDVIS galėtų turėti poveikį visų Lietuvoje veikiančių IPPT veiklai ir jų klientams, gali sutrikdyti kitas valstybines informacines sistemas, turėti ekonominių padarinių ar pakenkti gyventojų pasitikėjimu valstybe, todėl BDVIS turėtų būti pripažinta ypatingos svarbos informacine infrastruktūra.

Šis statusas lemtų, kad būtų atliekami kasmetiniai auditai, išbandomas kibernetinių incidentų valdymo priemonių veikimas, rengiami kibernetinių incidentų valdymo planai, atliekama detali sistemos veiksmų stebėsena bei monitoringas ir t.t. Tai leistų geriau pasiruošti kibernetinėms atakoms, operatyviau reaguoti į kylančias rizikas, užtikrintų BDVIS atliktų veiksmų atsekamumą ir leistų sumažinti kibernetinio incidento poveikį.

### *Baltieji domenų sąrašai*

Įvykus didelio mąsto kibernetinei atakai ir nulaužus BDVIS egzistuoja tikimybė, kad IPPT iš BDVIS gaus domenus, kurie neturėtų būti blokuojami. Siekiant sumažinti šios rizikos poveikį rekomenduojama įgyvendinti baltųjų domenų sąrašų mechanizmą.

Baltųjų domenų sąraše esančių domenų per BDVIS nebūtų įmanoma užblokuoti. Šis sąrašas susidėtų iš populiariausių lietuviškų ir užsienietiškų interneto svetainių domenų (pvz., valstybės institucijų, komercinių bankų, socialinių tinklų ir kt. domenų) ir būtų atnaujinamas BDVIS administratoriaus.

Baltųjų domenų sąrašą IPPT periodiškai, rankiniu būdu įkeltu į savo DNS. Rekomenduojama IPPT sąrašą atnaujinti ne rečiau nei kas tris mėnesius. Analogiškai, kaip ir su blokuojamų domenų perdavimu IPPT, rekomenduojama baltųjų domenų sąrašo perdavimui IPPT naudoti pirmąjį perdavimo būdą per HTTPS (žr. *perdavimo posistemė*).

# VI. Nauda ir ribotumai

### *Tiesioginė nauda*

Įgyvendinus BDVIS bus centralizuotas ir automatizuotas interneto svetainių blokavimo per IPPT DNS procesas, todėl:

- maksimalus interneto svetainių blokavimo vykdymo laikas sutrumpės nuo 5 d.d. iki mažiau nei 2 val.;
- blokavimas bus įmanomas 24/7 režimu;
- sumažės žmogiškosios klaidos galimybė;
- sumažės administracinė našta BDVIS naudotojams;
- neliks galimybės, kad blokavimo sankcija būtų neįvykdyta.

Pagrindinė numatoma nauda yra tai, kad toks **proceso optimizavimas sudarys technines galimybes Lietuvos Policijai realiu laiku reaguoti į iškilusią grėsmę** pritaikant 48 val. blokavimo iki teismo sprendimo mechanizmą, o tai yra itin svarbu vykstant didžiulio masto duomenų viliojimo atakoms (angl. *phishing*).

### *Papildoma nauda*

BDVIS taip pat gali turėti netiesioginį teigiamą poveikį:

- suvienodinamos konkurencijos sąlygos tarp IPPT, nes visi Lietuvoje veikiantys IPPT bus įpareigoti naudotis BDVIS, kuri nesuteikia galimybės neįvykdyti interneto svetainės blokavimo;
- privalomas BDVIS taikymas sudarys sąlygas suvienodinti teisinę bazę, reglamentuojančią, kaip turėtų būti vykdomas interneto svetainės blokavimas, todėl atsiras daugiau aiškumo tiek IPPT, tiek institucijoms, galvojančioms apie tokios sankcijos taikymo galimybę ateityje;
- BDVIS centralizuotai viešinant visų blokuojamų domenų sąrašą, visuomenė ir galės lengviau galės kontroliuoti, kokiais atvejais yra blokuojamos interneto svetainės ir ar nėra piktnaudžiaujama įgaliojimais;
- Viešai ir patogiu formatu skelbiami blokuojamų domenų sąrašai sudarys palankias sąlygas jų analizei ir tolimesniems tyrimams.

### *Ribotumai*

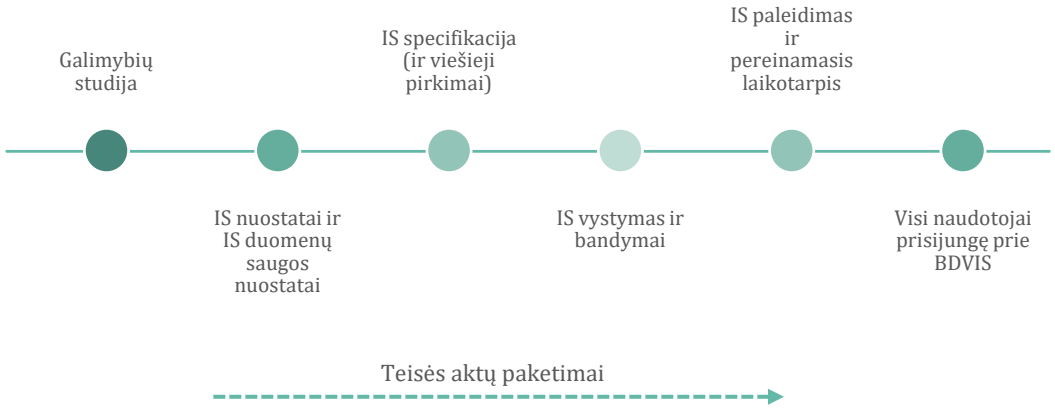
Nepaisant to, kad BDVIS žymiai paspartina kenkėjiškų svetainių blokavimo procesą, tačiau lieka keletas techninių trūkumų:

- Lietuvos IPPT klientai, pasikeitę kompiuterio DNS nustatymus į atvirus DNS serverius (pvz., Google Public DNS, Cloudflare Public DNS) ar naudojantys VPN, turės prieigą prie Lietuvoje užblokuotų interneto svetainių;
- Išliks galimybė blokuoti tik domeno ar subdomeno lygmenyje ir nebus įmanoma užblokuoti tik konkrečių interneto svetainės puslapių;
- Gyventojai, apsilankę blokuojamose svetainėse, kurios naudoja HTTPS, vietoj detalios informacijos apie svetainės blokavimo priežastį matys SSL sertifikato klaidą.

Atsižvelgiant į tai, kad BDVIS tik paspartina blokavimo vykdymą, siekiant efektyviai kovoti su kenkėjiškomis interneto svetainėmis yra būtina peržiūrėti visą procesą pradedant tuo, kaip greičiau atpažinti tokias svetaines, bei taikant kitas tikslines priemones. Daugiau apie rekomenduojamus žingsnius žr. kurklt.lt .

# VII. Įgyvendinimas

Numatomas BDVIS valdytojas yra Krašto apsaugos ministerija, kuri inicijuos galimybių studijos rengimą, paskirs būsimąjį pagrindinį informacinės sistemos tvarkytoją, užtikrins informacinės sistemos kūrimo finansavimą bei koordinuos teisės aktų pakeitimų inicijavimą. BDVIS tvarkytojas(-ai) rengs informacinės sistemos bei duomenų saugos nuostatus, parengs ir suderins IS specifikaciją (bei vykdys viešuosius pirkimus), koordinuos IS vystymą ir bandymus bei administruos pačią sistemą (žr. pav. 13). Anksčiausiai numatoma data, kada BDVIS galėtų pradėti naudotis visi vartotojai, yra 2025 m. I ketv.




Pav. 13. BDVIS sukūrimo ir įgyvendinimo žingsniai.

### *Informacinės sistemos tvarkytojas*

BDVIS nėra tipinė informacinė sistema, nes ji skirta optimizuoti procesui, kuriame dalyvauja daug tarpusavyje nepavaldžių institucijų ir privačių subjektų bei nėra vieno proceso šeimininko. Dėl šios priežasties ieškoma galimo BDVIS tvarkytojo, kuris būtų pavaldus Krašto apsaugos ministerijai kaip BDVIS valdytojui bei turėtų aukštas technines kompetencijas bei atitiktų kitus keliamus kriterijus.

Parenkant BDVIS tvarkytoją yra būtina atsižvelgti į šiuos kriterijus:

- Pagrindinė institucija, tvarkanti BDVIS, turėtų būti pavaldi BDVIS valdytojui;
- Institucijos funkcijos ir tikslai bent iš dalies turi atitikti BDVIS kūrimo tikslus;
- Institucijoje turi būti specialistų su aukštomis techninėmis kompetencijomis ypač kibernetinio saugumo klausimais;
- Patirtis kuriant informacines sistemas ir/arba darbas su ypatingos svarbos informacine infrastruktūra.

Pagal aukščiau nurodytus kriterijus įvertintos keturios institucijos, kurios buvo dažniausiai minimos individualių konsultacijų su suinteresuotosiomis šalimis metu (žr. pav. 14). Atlikus vertinimą galima teigti, kad nėra vienos institucijos, kuri atitiktų visus keliamus kriterijus ir natūraliai galėtų būti BDVIS tvarkytoja, tačiau toliau rekomenduojama toliau vertinti ir tęsti konsultacijas su NKSC ir KVTC dėl galimybės būti BDVIS tvarkytoju.

BDVIS tvarkytojai

| Institucija | Vertinimas | |
|---|---|---|
| **Nacionalinis kibernetinio saugumo centras** | **Pavaldumas:** Krašto apsaugos ministerija;<br>**Funkcijos ir tikslai:** kibernetinio saugumo užtikrinimas yra pagrindinė NKSC funkcija, todėl NKSC specialistai gali anksti identifikuoti kenkėjiškas interneto svetaines, tačiau jų užkardymo funkciją vykdo Lietuvos Policija. Taigi, NKSC funkcijos tik netiesiogiai dera su BDVIS tikslais;<br>**Techninės kompetencijos**: aukštos kompetencijos kibernetinio saugumo srityje;<br>**Patirtis su IS ir YSII:** yra;<br>**Kita**: sukauptos kompetencijos ir patirtis įgyvendinant DNS ugniasienės sprendimą galėtų būti pritaikyta vystant BDVIS; taip pat NKSC pagal savo funkcijas ir turimus žmogiškuosius išteklius gali generuoti reikalingus „baltuosius sąrašus“. | ●<br>◑<br>●<br>●<br>● |
| **Ryšių reguliavimo tarnyba** | **Pavaldumas:** nepriklausoma institucija;<br>**Funkcijos ir tikslai**: RRT yra institucija, kuri reguliuoja elektroninių ryšių paslaugos teikimo veiklą, tačiau pagrindiniai tikslai yra užtikrinti veiksmingą konkurenciją ir skatinti infrastruktūros plėtrą. Taigi, RRT funkcijos ir tikslai neatitinta BDVIS tikslų;<br>**Techninės kompetencijos**: aukštos teisinės kompetencijos, tačiau nėra kibernetinio saugumo kompetencijų;<br>**Patirtis su IS ir YSII**: yra;<br>**Kita**: RRT valdo aktualius IPPT sąrašus, kurie bus reikalingi BDVIS tvarkytojui. | ○<br>◑<br>○<br>●<br>◑ |
| **Kertinis valstybės telekomu-nikacijų centras** | **Pavaldumas**: Krašto apsaugos ministerija;<br>**Funkcijos ir tikslai**: tvarko Saugųjį valstybinių duomenų perdavimo tinklą ir teikia valstybės duomenų centro paslaugas. Kadangi KVTC siekia užtikrinti tinklo saugumą viešajam tinklui, KVTC tikslai iš dalies dera su BDVIS kūrimo tikslais;<br>**Techninės kompetencijos**: aukštos kompetencijos kibernetinio saugumo srityje;<br>**Patirtis su IS ir YSII**: yra;<br>**Kita**: KVTC veikia kaip valstybinis IPPT, todėl yra rizika, kad kiltų klausimų dėl konkurencijos užtikrinimo tarp visų Lietuvoje veikiančių IPPT. | ●<br>◑<br>●<br>●<br>○ |
| **Informacinės visuomenės plėtros komitetas** | **Pavaldumas**: Ekonomikos ir inovacijų ministerija;<br>**Funkcijos ir tikslai**: IVPK yra Valstybės informacinių išteklių sąveikumo platformos (VIISP) tvarkytojas. Preliminariu vertinimu dalį BDVIS funkcionalumų būtų galima įgyvendinti per VIISP, tačiau įgyvendinimas gali būti sudėtingas, nes reikėtų sukurti daug naujų elementų;<br>**Techninės kompetencijos**: aukštos kompetencijos kibernetinio saugumo srityje;<br>**Patirtis su IS ir YSII**: yra;<br>**Kita**: VIISP neturi DNS, kuris yra reikalingas BDVIS įgyvendinimui. | ○<br>◑<br>●<br>●<br>○ |

● Atitinka ◑ Iš dalies atitinka ○ Iš dalies atitinka

Pav.14. Institucijų, galinčių būti BDVIS tvarkytoju vertinimas.

Atliekant galimybių studiją taip pat yra rekomenduojama svarstyti ir konsultuotis dėl alternatyvių BDVIS tvarkytojų:

- Tvarkytojais gali būti paskirtos visos BDVIS naudosiančios valstybinės institucijos, kai viena iš jų yra išrenkama ar savanoriškai apsisprendžia būti pagrindine BDVIS tvarkytoja. Tokiu atveju yra būtina įvertinti, ar Krašto apsaugos ministerija galėtų būti BDVIS valdytoja;
- Nacionalinė teismų administracija taip pat galėtų būti įvertinta kaip potenciali BDVIS tvarkytoja. Tokiu atveju būtų reikalinga peržiūrėti atsakomybes tarp interneto svetainės blokavimą inicijuoti galinčių valstybinių institucijų, teismų ir teismų administracijos.

### *Informacinės sistemos finansavimas*

Būtina numatyti lėšas ne tik BDVIS sukūrimui, bet taip pat administravimui bei priežiūrai. Atsižvelgiant į IS komponentų skaičių ir kibernetinio saugumo reikalavimus, preliminariu vertinimu BDVIS sukūrimas gali kainuoti apie 100 tūkst. eurų. Kad BDVIS tvarkytojas galėtų administruoti ir prižiūrėti sistemą, bus reikalingas finansavimas žmogiškiesiems ištekliams (nuo 0,5 iki 1 papildomo darbuotojo etato) bei lėšų kibernetinio saugumo reikalavimams užtikrinti (sertifikatai, auditai ir kt.).

### *Informacinės sistemos alternatyvos*

Atliekant galimybių studiją, reikia įvertinti galimybę įgyvendinti BDVIS tikslus per Valstybės informacinių išteklių sąveikumo platformą (VIISP). Svarbu įvertinti ne tik galimus kaštus, bet ir tai, kad būtų įgyvendinti visi keliami tikslai BDVIS.

# VIII. Papildomos funkcijos

### *IP adresų blokavimas per BDVIS*

IPPT interneto svetaines gali blokuoti ne tik DNS būdu domeno lygmenyje, tačiau ir per IP adresą. Lietuvoje kartu su domeno blokavimu naudojama ir IP adreso blokavimo praktika. Šis mechanizmas ypač dažnai taikomas Lietuvos policijos siekiant užtardyti nusikaltimus elektroninėje erdvėje.

Nors interneto svetainės serverio IP adreso blokavimas negali būti apeinamas pakeičiant kompiuterio DNS nustatymus, tačiau IP adreso blokavimo galimybė negali būti naudojama, kai svetainė naudoja turinio pristatymo tinklus (angl. *content delivery network*) veikiančius atvirkštinės įgaliotosios stoties principu, pavyzdžiui, CloudFlare. Dėl šios priežasties IP adreso blokavimas tik papildo, o ne pakeičia domeno blokavimą.

BDVIS įgyvendinimo metu rekomenduojama apsvarstyti galimybę ir reikalingus pakeitimus siekiant išplėsti BDVIS funkcionalumą blokuoti ne tik domeno lygmenyje, tačiau ir serverio IP adreso lygmenyje.

### *Integracija su Lietuvos teismų informacine sistema LITEKO*

Lietuvoje nutarimas blokuoti interneto svetainę gali būti priimamas trimis skirtingais būdais:

1. Teismui skyrus blokavimo sankciją;
2. Lietuvos policijai taikant 48 val. blokavimo mechanizmą pagal Lietuvos Respublikos kibernetinio saugumo įstatymo 10 straipsnio 3 dalį;
3. Blokavimą inicijuojančioms institucijoms blokuojant veidrodines svetaines pagal ankstesnes teismo nutartis.

Nors integracijos su Lietuvos teismų informacine sistema LITEKO galimybė BDVIS modelio rengimo metu nebuvo plačiai vertinta, tačiau tokia integracija galimai leistų visiškai automatizuoti domenų blokavimo procesą teismui skyrus blokavimo sankciją. Tai leistų sumažinti domenų blokavimo sankcijų įgyvendinimo administracinę naštą blokavimą inicijuojančioms institucijoms bei tokiu būdu šiek tiek pagreitinant procesą. BDVIS įgyvendinimo metu rekomenduojama įvertinti tokios integracijos galimybę.

# Apibendrinimas

BDVIS – techninė priemonė, kuri leis greičiau įvykdyti interneto svetainės blokavimą po to, kai yra priimamas sprendimas, tokiu būdu efektyviai užkardant ne tik kenkėjiškas interneto svetaines, bet ir visas svetaines, kurios yra naudojamos nusikalstamai ar nelegaliai veikai elektroninėje erdvėje.

BDVIS centralizuos ir suvienodins visų interneto svetainių blokavimą galinčių inicijuoti institucijų blokavimo vykdymo procesą. Taip pat BDVIS automatizuos privalomų nurodymų vykdymas per visus Lietuvoje veikiančius IPPT.

BDVIS įgyvendinimas suteiks šias pagrindines naudas:

- sutrumpins blokavimo vykdymo laiką iki mažiau nei 2 val.;
- užtikrins, kad interneto svetainės blokavimas būtų faktiškai vykdomas kiekvieno IPPT;
- garantuos blokavimą 24/7 režimu per visus IPPT;
- sumažins administracinę naštą IPPT ir blokavimą inicijuojančioms institucijoms;

Vis dėlto, pagrindinė nauda tai, kad bus sudarytos technines galimybes realiu laiku reaguoti į nusikaltimus elektroninėje erdvėje, o tai yra ypač aktualu siekiant apsaugoti Lietuvos gyventojus nuo didelio masto duomenų viliojimo atakų.

kurklt.lt

**2022**