

## Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET



Vilniaus Gedimino technikos universitetas

# Automatinio informacijos saugumo audito paslauga

## Naudotojo vadovas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą "Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra" Nr. 09.3.3-ESFA-V-711-01-0003



Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

## Turinys

Įvadas	
Naudotojai	3
Pirmas jungimasis ir registracija prie paslaugos	3
Prisijungimas prie paslaugos	5
Automatinio saugumo audito vykdymas	6
Naujas skenavimas	6
Saugumo audito ataskaita	9
Skenavimo redagavimas	
Žurnaliniai įrašai	
Kontaktai	14

### Įvadas

Šiame dokumente pateikiama Automatinio saugos audito paslaugos naudotojo darbo instrukcija. Automatinio informacijos saugumo audito paslauga (toliau – AISAP) skirta atlikti pasirinkto serverio ar interneto svetainės informacinio pažeidžiamumo skenavimą ir gauti jo ataskaitą. Paslauga prieinama LITNET tinkle visoms mokslo ir studijų institucijoms (MSI), įsidiegusioms elektroninių tapatybių federaciją LITNET FEDI.

### Naudotojai

Automatinio informacijos saugumo audito paslaugos informacinėje sistemoje (AISAP IS) yra dvi naudotojų grupės:

- Naudotojai. Ši rolė suteikiama MSI kompiuterių specialistams ar kitiems darbuotojams (mokslininkams, tyrėjams) norintiems atlikti savo naudojamų kompiuterinių resursų (serverių, interneto svetainių) saugos auditą. Naudotojai gali atlikti veiksmus, reikalingus saugos audito planavimui, vykdymui bei rezultatų valdymui savo audituojamuose serveriuose bei interneto svetainėse.
- Administratoriai. Ši rolė suteikiama paslaugą administruojančio ar kito Litnet techninio centro darbuotojams. Administratoriai gali atlikti saugos audito planavimo, vykdymo bei rezultatų valdymo veiksmus visame *Litnet* tinkle, taip pat atlikti paslaugos portalo bei informacinės sistemos administravimo veiksmus.

Šiame naudotojo vadove aprašoma naudotojo rolę turinčio naudotojo sąsaja, per kurią prisijungęs naudotojas gali valdyti jo sukurtus sistemų testavimus bei rezultatus. Dirbant su sistema galima naudoti visas šiuo metu plačiai naudojamas naršykles, tokias kaip *Internet Explorer*, *Mozilla Firefox*, *Google Chrome*.

Automatinio saugos audito paslauga naudotis gali tik užsiregistravę ir gavę registracijos patvirtinimą iš paslaugos administratoriaus.

### Pirmas jungimasis ir registracija prie paslaugos

Paslauga pasiekiama adresu <u>https://aisa.vgtu.lt</u> arba <u>https://www.litnet.lt/lt/paslaugos</u>. Jos pradinis langas pateiktas 1 paveiksle.



**1 pav.** Pradinis paslaugos langas

Prisijungimas prie paslaugos galimas tik per Litnet elektroninių tapatybių federaciją LITNET FEDI. Atitinkamas registracijos langas pasirodys paspaudus mygtuką *Prisijungti* (žr.2 pav.).

LITNET FEDI eduGAIN	
	Incremental search
🧼 Vilnius Gediminas Technical University	
Aleksandras Stulginskis University	
ISM University of Management and Economics	
Kaunas University of Technology	
☆ Klaipeda State University of Applied Sciences	
Klaipeda University	
Lithuanian Academy of Music and Theatre	
Lithuanian Maritime Academy	
Lithuanian Sports University	
Mykolas Romeris University	
University of Šiauliai	
Utena University of Applied Sciences	
Vilnius University	
Vilnius University of Applied Sciences	
Vytautas Magnus University	

2 pav. LITNET FEDI prisijungimo langas

Pasirinkus savo MSI ir prisijungus pirmą kartą, naudotojui pateikiamas pranešimas apie registracijos pradžią. (žr. 3 pav.).



#### 3 pav. Pranešimas naudotojui po pirmo prisijungimo

Naujo naudotojo registracija nėra vykdoma automatiškai. Ji atliekama ne vėliau, kaip per vieną darbo dieną. Paslaugos administratorius, gavęs iš sistemos pranešimą apie naujo naudotojo registraciją, atlieka papildomą naujo naudotojo autentifikaciją. Esant poreikiui, naudodamasis elektroninių tapatybių federacijoje LITNET FEDI esamais kontaktiniais duomenimis, susisiekia su būsimu naudotoju, aptaria bei patikslina jo poreikius vykdyti automatinį saugos auditą. Registracija užbaigiama, kai paslaugos administratorius suteikia teisę prisijungti prie paslaugos valdymo lango ir naudotis paslauga ir naudotojui apie tai pranešama el. laišku.

## Prisijungimas prie paslaugos

Registruotam naudotojui prisijungus per naršyklę prie paslaugos, jos valdymo įrankiai pateikiami viršutinio meniu skiltyje *ADMINISTRAVIMAS* (žr. 4 pav.).



4 pav. Naudotojo paslaugos valdymo langas

Šiame lange taip pat pateikiama visa naudotojo atliktų automatinio saugumo audito skenavimų statistika.

### Automatinio saugumo audito vykdymas

Automatinio saugumo auditas vykdomas skenuojant pasirinktus auditavimo objektus. Tai atliekama viršutinio meniu skiltyje *ADMINISTRAVIMAS* pasirinkus išsiskleidusiame sąraše punktą *SKENAVIMAI* ir perėjus į atsivėrusį skenavimų valdymo langą (5 pav.).

		19. J. 1.	0040.00		nu od	
	Büsena	Skenavimo pava	adinimas Data	Ins	titucija Tipas	Naudotoja
	Būsena: visi 🔻 Tipa:	s: visi 🔻 Intensy	vumas: vit 🔻 P	aieška	Go!	
	Skenavima	+ NAUJAS	SKENAVIMAS			
Lie™		NAUJIENOS	DOKUMENTAI	KONTAKTAI	ADMINISTRAVI	MAS 🗸

5 pav. Naudotojo skenavimų valdymo langas

## Naujas skenavimas

Naujas skenavimas pradedamas pasirinkus mygtuką +NAUJAS SKENAVIMAS (5 pav.). Atsidaro naujo skenavimo langas (6 pav.), kuriame reikia sukurti skenavimo užduotį nurodant atitinkamus skenavimo parametrus.

**Pavadinimas** – tai naudotojo laisvai įrašomas tekstas. Rekomenduojame pavadinime užrašyti skenuojamo objekto pavadinimą ar DNS adresą. Tada skenavimų sąraše aiškiai matysis, koks objektas buvo audituojamas.

**Skenavimo objektai** – tai serverių ar interneto tinklalapių, kuriems norime atlikti automatinį saugumo auditą, DNS arba IP adresai. Leidžiami tiek IPv4, tiek ir IPv6 adresai CIDR notacijoje. Galima sukurti skenavimą ir keletui objektų, jei jų IP adresai kinta nuosekliai viename intervale. Šiuo atveju užpildome IP rėžį Nuo – Iki.

Taip pat galima nustatyti norimą skenavimo tipą, skenavimo laiką ir intensyvumą (žr. 5 pav.).

**Skenavimo tipas** – galima pasirinkti vieną iš trijų tipų:

*Pilnas* – skenuojamos visos nurodyto skenuojamo objekto kompiuterių tinklo tarnybos ir paslaugos;

- *Tik web* skenuojamatik žiniatinklio tarnyba be prisijungimo duomenų;
- *Web su prisijungimu* skenuojama žiniatinklio tarnyba su pateiktais prisijungimo duomenimis.

Pavadinim	as	
Mano se	rveris	
Skenavir	no objekta	ai
Įrašykite IP	arba DNS ad	Iresą
IP arba DN	S	
itsc.vgtu.	It	
		arba
IP rėžis		
Nuo		- Iki
Pridé	tipas	ą objektą
<ul> <li>Pridé</li> <li>Skenavimo</li> <li>Pilnas</li> </ul>	tipas Tik web	į objektą Web su prisijungimu
<ul> <li>Pridé</li> <li>Skenavimo</li> <li>Pilnas</li> <li>Skenavimo</li> <li>Nedelsia</li> </ul>	tipas Tik web pradžia	ą objektą Web su prisijungimu ata ir laikas
<ul> <li>Pridé</li> <li>Skenavimo</li> <li>Pilnas</li> <li>Skenavimo</li> <li>Nedelsia</li> <li>Skenavimo</li> </ul>	tipas Tik web pradžia nt m Da	ą objektą Web su prisijungimu ata ir laikas

6 pav. Naujo skenavimo sukūrimo langas

**Skenavimo pradžia** – galima pasirinkti pradėti skenavimą nedelsiant arba nurodyti skenavimo pradžios konkrečią datą ir laiką.

Skenavimo intensyvumas – galim trys skenavimo intensyvumo lygiai:

- *Lengvas* bus atliktas standartinių pažeidžiamumų pagal anksčiau surinktą informaciją skenavimas, nevykdant veiksmų, galinčių kenkti skenuojamos sistemos darbui;
- Normalus tai lėtesnis skenavimas. Jo metu bus skenuojami ir prievadai bei tikrinama daugiau kitų galimų pažeidžiamumų, kurie gali būti ir ne tokie reikšmingi. Skenavimai, galintys kenkti skenuojamos sistemos darbui nebus vykdomi;
- Intensyvus bus atliekami visi skenavimai kaip ir Lengvas ir Normalus atvejais, bei papildomai atliekami pavojingesni pažeidžiamumų testavimai, imituojantys paslaugos nutraukimo atakas. Šis skenavimas gali užtrukti gana ilgai, jie reikėtų vykdyti tik suderinus su skenuojamo objekto administratoriumi.

Užpildžius ir pažymėjus visus skenavimo parametrų laukus, spaudžiame mygtuką *Sukurti skenavimą* ir grįžtame į ankstesnį skenavimo valdymo langą. Jo skenavimų sąraše atsiranda sukurtas naujas skenavimas, kurio būsena yra *Laukiantis* (žr. 7 pav.).

Skenavimai	+ NAUJAS SKENAVIM	IAS					
Skenavimo užduotis sėkmingai	i sukurta!						
Būsena: visi 🔻 Tipas: v	isi 🔻 Intensyvumas: vi:	▼ Paieška	Go!				
<ul> <li>Būsena</li> </ul>	Skenavimo pavadinimas	Data	Institucija	Tipas	Naudotojas	Intensyvumas	Rezultatai
Laukiantis	Mano serveris	2018-04-10 09:59:04	VGTU	Pilnas	Remigijus Kutas	Normalus	Redaguoti Rezultatai
_			···				

7 pav. Naudotojo skenavimų valdymo langas, sukūrus nauja skenavimą

Sistema saugumo auditą (pažeidžiamumų skenavimus) vykdo eilės tvarka, todėl priklausomai nuo apkrovimo (sukurtų skenavimų skaičiaus), skenavimas gali neprasidėti iš karto ir kurį laiką būti būsenos *Laukiantis*. Sistemai pradėjus vykdyti pažeidžiamumų skenavimą, skenavimo būsena pasikeičia į *Vykdymas*, nurodant skliausteliuose įvykdymo procentą (žr. 8 pav.)

Skenavimai	+ NAUJAS SKENAVIM	AS					
Būsena: visi 🔻 Tipas: vis	si 🔻 Intensyvumas: vit	▼ Paieška	Go!				
Büsena	Skenavimo pavadinimas	Data	Institucija	Tipas	Naudotojas	Intensyvumas	F
Vykdomas (1%)	Mano serveris	2018-04-09 12:55:44	VGTU	Pilnas	Remigijus Kutas	Normalus	[

8 pav. Naudotojo skenavimų valdymo langas, prasidėjus pažeidžiamumų skenavimui

#### Saugumo audito ataskaita

Atlikto saugumo audito ataskaitą galima peržiūrėti skenavimų sąrašo (žr. 9 pav) stulpelyje *Rezultatai* paspaudus mygtuką *Rezultatai*.

S	kenavimai	+ NAUJAS SKENAVIMA	AS					
В	ūsena: visi 🔻 Tipas: vis	Thtensyvumas: vi:	▼ Paieška	Go!				
	Būsena	Skenavimo pavadinimas	Data	Institucija	Tipas	Naudotojas	Intensyvumas	Rezultatai
	Įvykdytas	Mano serveris	2018-04-09 12:55:44	VGTU	Pilnas	Remigijus Kutas	Normalus	Redaguoti Rezultatai (32)
	Įvykdytas	www.litnet.lt	2018-03-13 09:46:08	VGTU	Pilnas	Remigijus Kutas	Normalus	Redaguoti Rezultatai (32)
	Įvykdytas	Litnet	2018-03-13 09:04:05	VGTU	Tik web	Remigijus Kutas	Lengvas	Redaguoti Rezultatai (33)
	Įvykdytas	itsc	2018-02-13 20:04:10	VGTU	Tik web	Remigijus Kutas	Normalus	Redaguoti Rezultatai (31)

#### 9 pav. Skenavimų sąrašas

Atsivėrusiame lange (žr. 10 pav.) pateikiamas nustatytų audituojamo objekto galimų saugumo pažeidimų sąrašas. Virš rezultatų sąrašo esančiuose laukuose pasirinkę reikiamus paieškos kriterijus ar įvedę paieškos žodį ir paspaudę *Go*, galite atlikti paiešką skenavimo rezultatų sąraše.

Galimi saugumo pažeidžiamumai yra surikiuojami pagal jų pavojingumo lygį. Aptikus galimą pažeidžiamumą sistema įvertina jį ir priskiria pavojingumo balą nuo 0 iki 10, pavojingiausiems skirdama 10 balų.. Priklausomai nuo pažeidžiamumui pavojaus balo reikšmės, jie suskirstomi į 4 pavojingumo lygius: Aukštas (7,1-10 balų), Vidutinis (4,1-7,0 balų), Žemas (0,1-4,0 balų), Pastaba (0,0 balų).

Pažeidžiamumų sąraše taip pat pateikiamas su pažeidžiamumu susijęs protokolas bei pažeidžiamumo aptikimo kokybės (QoD) rodiklis, kurio vertė nuo 0 % iki 100 %, parodo atlikto pažeidžiamumo aptikimo patikimumą.

Pavojus: visi       False positive: rodyti       Paleškin       Go!         Image: Pavadinimas       Pavojus       Protokolas       QoO       Veiksmin         Image: PHP Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       98%       Pertice         Image: PHP Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       98%       Pertice         Image: Phr Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       98%       Pertice         Image: Phr Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       98%       Pertice         Image: Phr Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       98%       Pertice         Image: Phr Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       96%       Pertice         Image: Phr Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Adkitass       80/tcp       9%       Pertice	S	kenavimo rezultatai 🛛 🔹 🔻	Eksportuoti rezultatus		
Pavadinimas         Pavojus         Protokolas         QoD         Veiksm           ID         PHP Inventory 'user' and pass' Parameters SQL Injection Vulnerability         7.5         Additions         80/tcp         98%         Period           ID         PHP Inventory 'user' and 'pass' Parameters SQL Injection Vulnerability         7.5         Additions         80/tcp         98%         Period           ID         http TRACE XSS attack         58         Vducinis         80/tcp         99%         Period	Pa	rojus: visi 🔻 False positive: rodyti 👻 Paleški	Got		
III       PHP Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Aukätass       80/tcp       98%       Period         III       PHP Inventory user and pass' Parameters SQL Injection Vulnerability       7.5       Aukätass       80/tcp       98%       Period         III       http TRACE XSS attack       58       Viduoins       80/tcp       99%       Period		Pavadinimae	Pavojos I	Protokolas QoD	Veiksmai
III         PHP Inventory user and 'pass' Parameters SQL Injection Vulnerability         7.5         AukStas         80/tcp         98%         Perform           III         http TRACE XSS attack         5.8         Viduoins         80/tcp         99%         Perform	10	PHP Inventory 'user' and 'pass' Parameters SQL Injection Vulnerability	7.5 Aukitas	80/tcp 98%	Peticieti
III http TRACE XSS attack 5.8 Vidusinis 80/tcp 99% Person	10	PHP Inventory user and pass' Parameters SQL Injection Vulnerability	7.5 Aukštas	80/tcp 98%	Perficient
	Ð	http TRACE XSS attack	5.8 Vidutinia	80/tcp 99%	Pertikireti
III http TRACE XSS attack 5.8 Vidutins 80/tcp 99% Person	10	http TRACE XSS attack	5.8 Vidutinia	80/tcp 99%	Perficient

10 pav. Nustatytų galimų saugumo pažeidimų sąrašas

Kiekvieno aptikto pažeidžiamumo ataskaita (11 pav.) pateikiama paspaudus mygtuką Peržiūrėti.

ProFTPD `mod\_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Pavojus	10.0 Aukštas		
Protokolas	21/tcp		
QoD	99%		
CVE	CVE-2015-3306		
<b>Aprašymas</b> ProFTPD is prone	to an unauthenticated copying of files vulne	erability.	
Poveikis			
Under some circu	mstances this could result in remote code e	xecution	
Siülomas sprendi Ask the vendor fo	imas Ir an update		
False positive:			
Ne		T	
Komentaras:			
	Išsaugoti rezutlatą		

11 pav. Aptikto galimo saugumo pažeidimo ataskaita

Ataskaitoje pakartojama skenavimo rezultatų sąraše pateikta informacija – galimo pažeidžiamumo pavadinimas, nurodantis pažeidžiamumo esmę, protokolas, pažeidžiamumo aptikimo kokybės (QoD) rodiklis bei nuoroda į pažeidžiamumų žinių bazės (CVE) įrašą (daugiau apie CVE įrašus rasite <u>https://cve.mitre.org</u>), kuriuo remiantis nustatytas šis pažeidžiamumas. *CVE išsamiau* tinklalapyje adresu <u>https://www.cvedetails.com/</u> naudojantis šia CVE įrašo nuoroda galima gauti detalesnę informaciją apie aptiktą pažeidžiamumą.

Toliau pateikiamas trumpas aptikto galimo pažeidžiamumo aprašymas, jo poveikis bei siūlomas sprendimas pažeidžiamumo panaikinimui. Pavyzdžiui, 10 pav. pateiktoje pažeidžiamumo ataskaitoje, jo aprašas sako, kad *per ProFTPD tarnybą galimas neautentifikuotas failų kopijavimas neautomatiniu būdu naudojant mod\_copy*. Šio pažeidžiamumo poveikis – *gali būti pradėtas vykdyti nuotoliniu būdu įkeltas programinis kodas*. Ir siūlomas sprendimas – *reikalingas esamo kodo atnaujinimas*.

Kadangi pažeidžiamumų aptikimas vykdomas automatiniu būdu analizuojant audituojamo serverio ar web svetainės programinį kodą, nėra šimtaprocentinės garantijos, kad pateikta auditavimo išvada bus visada teisinga. Todėl sistemoje yra sukurta galimybė naudotojui pažymėti, jei pateiktas perspėjimas yra neteisingas, t.y. nustatyti ataskaitos lauko *False positive* reikšmę *Taip* bei įrašyti atitinkamą komentarą. (žr. 12 pav.)

False positive:		
Taip		v
Komentaras:		
		/
	Išsaugoti rezutlatą	

#### 12 pav. Neteisingo perspėjimo pažymėjimo įrankis

Skenavimo rezultatų ataskaitą galima suformuoti ir išsaugoti atskirame faile. Leidžiami formatai – CSV, XML, HTML ir PDF. Ataskaitos suformavimui ir atsiuntimui, pasirinkite mygtuką *Eksportuoti rezultatus* ir pateiktame sąraše pasirinkite reikiamą formatą (žr. 13 pav.).

S	kenavimo	rezultatai 🗔	dl	Ŧ	Eksportuoti rezultatus	
Pa	vojus: visi 🔻	False positive: rodyti	•	Paieš	CSV formatu XML formatu	Go!
	Pavadinimas PHP Inventory 'user' an	d 'pass' Parameters SQL Injection	Vulnerability		PDF formatu	us Aukštas
0	PHP Inventory 'user' an	d 'pass' Parameters SQL Injection '	Vulnerability		7.5	Aukštas
	http TRACE XSS attack				5.8	Vidutinis

13 pav. Skenavimo rezultatų atsisiuntimas pasirinktu formatu.

### Skenavimo redagavimas

Jei skenavimas dar nėra pradėtas, t.y. jo būsena yra *Laukiantis* (žr. 7 pav.), skenavimą galima redaguoti. Norėdami redaguoti skenavimą, skenavimų sąrašo stulpelyje *Rezultatai* pasirinkite mygtuką *Redaguoti* (žr. 7 pav.), pateiktame Skenavimo redagavimo lange redaguokite reikiamus duomenis ir spauskite *Atnaujinti skenavimą* (žr. 14 pav.).

Pavauninas			
Mano tinkla	alapis		
Skenavimo Jrašykite IP ar Skenavimo pr	o objektai ba DNS adresą adžia		
Nedelsiant	2018-0	04-09 13:27:00	
Skenavimo in	tensyvumas		

14 pav. Skenavimo parametrų redagavimo langas

Naudotojas taip pat gali stabdyti ar ištrinti jau pradėtą ar laukiantį skenavimą bei pradėti skenavimą, kuriam buvo nurodytas vėlesnis laikas. Tai atliekama skenavimų sąraše pažymėjus pasirinktą skenavimą (- us), ir bakstelėjus vieną iš atsiradusių mygtukų – *Pradėti, Stabdyti* ar *Ištrinti* (15 pav.).

	Skenavimai	+ NAUJAS SKENAVIM	AS			
	Skenavimo užduotis sėkmingai s	ukurta!				
	Būsena: visi 🔻 Tipas: vis	i 🔻 Intensyvumas: vi:	▼ Paieška	Go!		
	Pasirinktus rezultatus: Pradéti	Stabdyti Ištrinti				
	<ul> <li>Būsena</li> </ul>	Skenavimo pavadinimas	Data	Institucija	Tipas	Naudotojas
$\left( \right.$	C Laukiantis	Mano serveris	2018-04-10 09:59:04	VGTU	Pilnas	Remigijus Kutas

15 pav. Veiksmai su pasirinktu skenavimo sąrašo elementu

## Žurnaliniai įrašai

Puslapyje Žurnaliniai įrašai pateikiama išsami įvykių, kuriuos naudotojas atliko sistemoje, informacija (žr. 16 pav.).

## Žurnaliniai įrašai

Paleška Goł									
Data	Veiksmas	Vartotojas	Institucija	Testavimas	P				
2018-03-13 09:09:31	Prisijungė prie sistemos.	Lijana	VGTU	-	158.129.207.3				
2018-03-08 15:12:24	Eksportavo skanavimo rezultatus (csv)	Lijana	VGTU	Mano tinklalapis	158.129.207.3				
2018-03-08 15:11:46	Eksportavo skanavimo rezultatus (xml)	Lijana l	VGTU	Mano tinklalapis	158.129.207.3				
2018-03-08 15:11:18	Eksportavo skanavimo rezultatus (pdf)	Lijana	VGTU	Mano tinklalapis	158.129.207.3				
2018-03-08 15:07:28	Eksportavo skanavimo rezultatus (html)	Lijana	VGTU	Mano tinklalapis	158.129.207.3				
2018-03-08 14:59:29	lštrynė testavimo rezultatą.	Lijana	VGTU	-	158.129.207.3				
2018-03-08 14:58:50	Prisijungė prie sistemos.	Lijana l	VGTU	-	158.129.207.3				
2018-03-08 14:58:50	Prisijungė prie sistemos.	Lijana I	VGTU		158.129.207.3				
2018-03-07 16:16:22	Atsijungė nuo sistemos.	Lijana	VGTU		158.129.207.3				

### 16 pav. Žurnalinių įrašų langas

## Kontaktai

Iškilus klausimams ar problemoms naudojantis automatinio saugumo audito paslauga, prašome kreiptis į paslaugos administratorių el. paštu adresu <u>aisa@vgtu.lt</u>