Dažniausiai užduodami klausimai* – atsakymai apie įslaptintos informacijos ryšių ir informacines sistemas (ĮIRIS)

* Sąrašas parengtas atsižvelgiant į institucijų bei įstaigų klausimus, pateiktus konsultacijų metu

Eil. Nr.	Klausimas	Atsakymas
1.	Kas yra ĮIRIS ir kas ją sudaro?	Vadovaujantis LR valstybės ir tarnybos paslapčių įstatymo 2 str., **Įslaptintos informacijos ryšių ir informacinė sistema (toliau – ĮIRIS)** – iš vieno ar daugiau kompiuterių, išorinių įrenginių ir programinės įrangos sudaryta ir informacinių technologijų pagrindu veikianti infrastruktūra įslaptintai informacijai apdoroti ir elektroninių ryšių tinklai, kuriais perduodama įslaptinta informacija (išskyrus viešuosius ryšių tinklus).
2.	Kokiais atvejais reikia įteisinti ĮIRIS?	Vadovaujantis LR valstybės ir tarnybos paslapčių įstatymo 41 str. 1 dalimi, apdoroti ir perduoti įslaptintą informaciją galima **tik įteisintomis ĮIRIS.** ĮIRIS laikoma įteisinta, kai paslapčių subjektui, paslapčių subjektui pavaldžiai ar jo reguliavimo sričiai priskirtai įstaigai, įmonei, tiekėjui yra išduodamas **leidimas naudoti ĮIRIS.**
3.	Jeigu kompiuteris yra naudojamas įslaptintos informacijos rengimui bei atspausdinimui, bet nėra prijungtas prie tinklo, ar tokiu atveju reikia steigti ir įteisinti ĮIRIS?	Jei kompiuteryje yra apdorojama įslaptinta informacija, **tai yra ĮIRIS** ir ji turėtų būti įteisinta.
4.	Nuo ko pradėti ir kokiais teisės aktais vadovautis norint įsteigti ir įteisinti ĮIRIS?	Pirmiausia, norint įsteigti ir įteisinti ĮIRIS, siūlome susipažinti su Įslaptintos informacijos ryšių ir informacinių sistemų steigimo ir įteisinimo taisyklėmis (toliau – ĮIRIS steigimo taisyklės). Kai kurie ĮIRIS įteisinimui skirti dokumentai turės slaptumo žymas, todėl atkreipkite dėmesį į ĮIRIS steigimo taisyklių IV skyriaus antrąjį skirsnį. 1. Vadovaujantis ĮIRIS steigimo taisyklių II skyriumi, rengiamas ĮIRIS nuostatų projektas ir teikiamas derinimui su ĮIRIS steigimo taisyklių 6 punkte nurodytomis institucijomis. Nacionalinis kibernetinio saugumo centras (toliau – NKSC) atlieka Saugumo priežiūros tarnybos (toliau – SPT) ir Nacionalinės komunikacijų apsaugos tarnybos funkcijas (toliau – NKAT). 2. Patvirtinus ĮIRIS nuostatus, rengiamas specifikacijos projektas (ĮIRIS steigimo taisyklių III skyrius). Specifikacija rengiama vadovaujantis Reikalavimų įslaptintos informacijos ryšių ir informacinių sistemų specifikacijoms aprašu, patvirtintu Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos direktoriaus 2020 m. vasario 24 d. įsakymu Nr. 2-2RN „Dėl Reikalavimų įslaptintos informacijos ryšių ir informacinių sistemų specifikacijoms aprašo patvirtinimo ir Vyriausybinių ryšių centro prie Lietuvos Respublikos valstybės saugumo departamento direktoriaus 2013 m. spalio 31 d. įsakymo Nr. 2-31RN „Dėl

		Reikalavimų automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, specifikacijoms aprašo patvirtinimo“ pripažinimo netekusiu galios“. Šį aprašą galite gauti pateikę prašymą NKSC info@nksc.lt. Parengtas specifikacijos projektas teikiamas derinimui su JIRIS steigimo taisyklių 14 punkte nurodytomis institucijomis. 3. Patvirtinus ĮIRIS nuostatus ir specifikaciją, reikia pateikti prašymą žinybinei SPT arba SPT dėl leidimo naudoti ĮIRIS išdavimo. Kartu su prašymu reikia pateikti JIRIS steigimo taisyklių IV skyriaus pirmo skirsnio 22 punkte nurodytus dokumentus, kurie rengiami vadovaujantis Įslaptintos informacijos ryšių ir informacinių sistemų saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2019 m. sausio 16 d. nutarimu Nr. 40-1 „Dėl įslaptintos informacijos ryšių ir informacinių sistemų apsaugos įgyvendinimo“ nurodytais reikalavimais. Šį aprašą galite gauti pateikę prašymą LR Vyriausybės kanceliarijai arba Valstybės saugumo departamentui (teikia tiekėjai). Be aukščiau minėtų teisės aktų, įslaptintos informacijos apsaugos priemonėms reikalavimus nustato ir jų taikymą reglamentuoja Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas, Įslaptintos informacijos administravimo ir išslaptinimo tvarkos aprašas, Įslaptintos informacijos fizinės apsaugos reikalavimų ir jų įgyvendinimo tvarkos aprašas , Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas ir kt. teisės aktai.
5.	Ar NKSC atlieka ĮIRIS įrangos TEMPEST matavimus ir išduoda TEMPEST sertifikatus?	TEMPEST matavimus atlieka ir sertifikatus išduoda Informacinių technologijų tarnyba prie KAM.
6.	Ar įsteigti ir įteisinti ĮIRIS, kurioje apdorojama ir (arba) perduodama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“ užtrunka tiek pat laiko kaip ir ĮIRIS, kurioje apdorojama ir (arba) perduodama įslaptinta informacija, žymima aukštesnėmis slaptumo žymomis („Konfidencialiai“, „Slaptai“ arba „Visiškai slaptai“)?	Jei steigiama ĮIRIS, kurioje bus apdorojama ir (arba) perduodama įslaptinta informacija pažymėta slaptumo žyma „Konfidencialiai“ ar aukštesne, tuomet visa ĮIRIS naudojama įranga ir patalpos, kuriose bus įrengiama ĮIRIS privalo turėti TEMPEST sertifikatus ir kitas su apsauga nuo TEMPEST (elektromagnetinė spinduliuotė) susijusias priemones. Žiūrint praktiškai, įrengti tokią ĮIRIS yra brangiau ir įsteigti paprastai užtrunka ilgiau nei pvz. ĮIRIS, kurioje apdorojama ir (arba) perduodama įslaptinta informacija, žymima slaptumo žyma „Riboto naudojimo“. **Įteisinimo trukmė nepriklauso** nuo slaptumo žymos. Žinybinė SPT arba SPT ne vėliau kaip per 3 mėnesius nuo visų leidimui naudoti ĮIRIS dokumentų gavimo dienos atlieka ĮIRIS saugos dokumentų vertinimą, ĮIRIS darbo vietų patikrinimą ir priima sprendimą dėl leidimo naudoti ĮIRIS išdavimo arba neišdavimo. Į nurodytą sprendimo priėmimo terminą JIRIS steigimo taisyklių 27 ir

		28 punktuose nurodytas leidimo naudoti ĮIRIS išdavimo procedūrų sustabdymo laikas neįskaičiuojamas.
7.	Ar ĮIRIS įteisinimui reikalingi dokumentai (ĮIRIS nuostatai, ĮIRIS specifikacija, ĮIRIS saugos dokumentai) gali būti parengti ĮIRIS steigėjo ar ĮIRIS valdytojo subteikėjo, t. y. trečios šalies?	Taip.
8.	Ar ĮIRIS įteisinimui reikalingi dokumentai rengimo ir derinimo metu gali būti neįslaptinti?	Tipiniu atveju ĮIRIS nuostatai būna neįslaptinti, o ĮIRIS specifikacija ir saugos dokumentai turi slaptumo žymą. ĮIRIS valdytojo, kuris yra tiekėjas, ĮIRIS specifikacija ir saugos dokumentai gali neturėti slaptumo žymos
9.	Kuo vadovaujantis atlikti ĮIRIS rizikos analizę ir parengti ĮIRIS rizikos analizės ataskaitą?	Reikalavimai ĮIRIS rizikos analizės ataskaitai pateikiami Įslaptintos informacijos ryšių ir informacinių sistemų saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2019 m. sausio 16 d. nutarimu Nr. 40-1 „Dėl įslaptintos informacijos ryšių ir informacinių sistemų apsaugos įgyvendinimo“. Atliekant ĮIRIS rizikos analizę rekomenduojame vadovautis metodine medžiaga – Rizikos analizės vadovu arba ISO/IEC 27005. Atkreipiame dėmesį, kad ĮIRIS rizikos analizės ataskaitoje turėtų būti aiškiai aprašyta rizikos įvertinimo metodika (kaip apskaičiuojamas rizikos laipsnis ir kt.), pateiktas išsamus grėsmių sąrašas, jų padarinių zona, susijusios informacines vertybės. Kiekvienai nustatytai grėsmei nurodyti grėsmės valdymo priemones. Siūlome aiškiai pateikti įvertintas liekamąsias rizikas ir nurodyti, kad ĮIRIS valdytojas suvokia ir prisiima šias rizikas.
10.	Į ką atkreipti dėmesį rengiant ĮIRIS saugumo reikalavimų įgyvendinimo patikrinimo ataskaitą?	Šioje ataskaitoje turėtų būti pateikta informacija kaip ĮIRIS įdiegtos jūsų parengtuose ĮIRIS saugos dokumentuose aprašytos ĮIRIS saugumui naudojamos apsaugos priemonės. Siūlome prie kiekvienos apsaugos priemonės trumpai aprašyti kaip ji įgyvendinama ir pateikti nuorodas į jūsų ĮIRIS SSRA, ĮIRIS SVPA ar kitų ĮIRIS saugą reglamentuojančių dokumentų punktus.
11.	Kokių papildomų dokumentų, reikalingų ĮIRIS taikomoms saugumo užtikrinimo priemonėms įvertinti ir (arba) ĮIRIS patikrinti, ĮIRIS valdytojo gali prašyti SPT?	• ĮIRIS personalo leidimų dirbti ar susipažinti su įslaptinta informacija. • Tiekėjo leidimo dirbti ar susipažinti su įslaptinta informacija. • Pažymėjimo, patvirtinančio, kad saugumo zonoms priskirtos patalpos ir (arba) teritorijos atitinka fizinės apsaugos reikalavimus ir jose galima dirbti su įslaptinta informacija ar ją saugoti. • ĮIRIS įrangos apsaugos nuo elektromagnetinės spinduliuotės lygių arba zonų atitikties nustatymas. • Įsakymų dėl ĮIRIS naudotojų, ĮIRIS saugos įgaliotinio ir jo pavaduotojo, ĮIRIS administratoriaus ir jo pavaduotojo, ĮIRIS

		kriptografinių priemonių administratoriaus ir jo pavaduotojo paskyrimo kopijų. • Įsakymų dėl techninės ir programinės įrangos sąrašų patvirtinimo kopijos. • Patalpų priskyrimo saugumo zonoms įsakymo kopijos. • Įsakymų dėl ĮIRIS saugos dokumentų patvirtinimo kopijos. • Kitų ĮIRIS įteisinimui reikalinguose dokumentuose paminėtų teisės aktų/tvarkų, kurių SPT neturi galimybės gauti.
12.	Kokie asmenys dalyvauja SPT vykdomame ĮIRIS patikrinime?	Patikrinime turėtų dalyvauti saugos įgaliotinis ir (arba) administratorius (arba jų pavaduotojai).
13.	Kam teikia ĮIRIS įteisinimui reikalingus dokumentus ĮIRIS valdytojas, kuris yra tiekėjas?	Įslaptintų sandorių saugumą užtikrinančiai institucijai (nurodytai LR valstybės ir tarnybos paslapčių įstatymo 34 straipsnio 1 dalyje), kuri, vadovaudamasi Tiekėjų patikimumo vertinimo tvarkos aprašo nustatyta tvarka, juos perduoda paslapčių subjekto, su kuriuo sudaromas įslaptintas sandoris, žinybinei SPT arba, jeigu ji neįsteigta, SPT.
14.	Kuriuos parengtus leidimui naudoti ĮIRIS gauti dokumentus reikia derinti, o kurių nereikia ir su kokiomis institucijomis šie dokumentai derinami?	**ĮIRIS nuostatų projektą** ĮIRIS steigėjas derina su: • NKAT; • žinybine SPT arba SPT; • Valstybine duomenų apsaugos inspekcija, jeigu ĮIRIS numatoma tvarkyti asmens duomenis (išskyrus atvejus, kai tokia informacija ĮIRIS tvarkoma valstybės saugumo arba gynybos tikslais); • ĮIRIS ir kitų informacinių sistemų, iš kurių bus gaunami ar kurioms bus teikiami duomenys, valdytojais. **ĮIRIS specifikacijos projektą** ĮIRIS valdytojas derina su: • NKAT; • žinybine SPT arba SPT; • ĮIRIS, iš kurių bus gaunami ar kurioms bus teikiami duomenys, valdytojais. ĮIRIS specifinių saugumo reikalavimų aprašo, ĮIRIS saugumo valdymo procedūrų aprašo, ĮIRIS rizikos analizės ataskaitos ir ĮIRIS saugumo reikalavimų įgyvendinimo patikrinimo ataskaitos su jokiomis institucijomis **derinti nereikia.**
15.	Kokia informacija gali būti apdorojama ĮIRIS, skirtoje ĮIRIS kūrimo ir įteisinimo įslaptintiems dokumentams parengti?	Šioje ĮIRIS gali būti apdorojama **tik** ĮIRIS kūrimo ir įteisinimo dokumentams parengti reikalinga įslaptinta informacija.
16.	Ar gali būti taikomos išimtys, norint skubos tvarka gauti leidimą naudoti ĮIRIS?	Išimtys **nėra taikomos** ir sprendimas dėl leidimo naudoti ĮIRIS išdavimo yra priimamas teisės aktų numatytais terminais ir tvarka.

17.	Jei planuojama, kad ĮIRIS bus sujungtos su kitomis informacinėmis sistemomis ar ĮIRIS, kokios kriptografinės priemonės ir produktai gali būti naudojami apdorojamos ir (arba) perduodamos įslaptintos informacijos apsaugai?	Gali būti naudojami NKAT patvirtinti kriptografiniai metodai ir (arba) priemonės. Tokių priemonių sąrašas yra pateiktas NKSC tinklapyje. Jei norima naudoti kriptografinę priemonę, kurios nėra šiame sąraše, siūlome kreiptis į NKAT su prašymu išduoti kriptografinės priemonės patvirtinimo pažymą.