

Užduotis: **20. Asmens duomenų teisėtas naudojimas, elektroninis parašas ir duomenų šifravimas**

Klasė: **IV**

Užduoties turinys (Informatikos bendroji programa: 31.6.1–31.6.2). **Saugus elgesys:**

Asmens duomenų teisėtas naudojimas. 31.6.1. Asmens duomenų teisėtas naudojimas. Prisimenama, kas yra asmens duomenys. Susipažįstama su pagrindiniais Europoje ir Lietuvoje galiojančiais teisės aktais, reglamentuojančiais asmens duomenų, kibernetinės saugos ir privatumo apsaugą: Bendroju duomenų apsaugos reglamentu, Asmens duomenų teisinės apsaugos įstatymu, Kibernetinio saugumo įstatymu. Ypatingas dėmesys skiriamas Europos komisijos patvirtintam Bendrajam duomenų apsaugos reglamentui, sudarančiam Europos Sąjungos piliečiams galimybę geriau kontroliuoti savo asmens duomenis. Susipažįstama su duomenų subjekto teisėmis ir jų realizavimu (pavyzdžiui, gauti informaciją apie savo asmens duomenų tvarkymą; susipažinti su savo asmens duomenimis, kurie yra saugomi įstaigose; atšaukti savo sutikimą tvarkyti asmens duomenis; prašyti ištaisyti netikslius, papildyti neišsamius asmens duomenis; prašyti ištrinti (teisė „būti pamirštam“) su duomenų subjektu susijusius asmens duomenis; prašyti apriboti savo asmens duomenų tvarkymą; pasinaudoti teise į duomenų perkeliamumą; nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi; pateikti skundą priežiūros institucijai, pasinaudoti teise į žalos atlyginimą dėl netinkamo asmens duomenų tvarkymo. Aptariamos institucijos, kontroliuojančios, kaip laikomasi asmens duomenų apsaugos įstatymų nuostatų. Susipažįstama su pagrindinėmis kibernetinio saugumo sąvokomis, apibrėžtomis Kibernetinio saugumo įstatyme (elektroninės informacijos prieglobos paslaugos, ypatingos svarbos informacinė infrastruktūra, kibernetinė erdvė, kibernetinio saugumo krizė, kibernetinis incidentas, kibernetinis saugumas, kibernetinių incidentų valdymas, ryšių ir informacinė sistema, ryšių ir informacinės sistemos spraga, rizika, saugusis valstybinis duomenų perdavimo tinklas) bei kibernetinės saugos principais. Nagrinėjamas kibernetinės saugos ir duomenų saugos ryšys.

Elektroninis parašas ir duomenų šifravimas. Išsiaiškinama elektroninio parašo sąvoka, susipažįstama su elektroninio spaudo, elektroninės laiko žymos sąvokomis. Aptariama, kuo skiriasi kvalifikuotas ir nekvalifikuotas elektroninis parašas, nurodoma kvalifikuoto elektroninio parašo teisinė galia ir paskirtis: saugi, patogi ir juridinę galią turinti priemonė pasirašyti dokumentus ir patvirtinti savo tapatybę internetinėje erdvėje. Pateikiami ir aptariami elektroninio parašo, elektroninio spaudo, elektroninės laiko žymos naudojimo pavyzdžiai. Susipažįstama su duomenų ir pranešimų šifravimu, aiškinamasi, kas yra privatieji ir viešieji šifravimo raktai. Praktiškai išbandomas duomenų ir pranešimų šifravimas ir (ar) dešifravimas, naudojant, pavyzdžiui, „Kleopatros“ pranešimų šifravimo įrankį (jis yra „Gpg4win“ programų paketo dalis).

Testo klausimai

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėtingumo lygis (1–4)	Ugdomos kompetencijos
1	Kas laikoma asmens duomenimis pagal Europos Parlamento ir Tarybos Bendrąjį duomenų apsaugos reglamentą (BDAR)? Pažymėkite visus teisingus atsakymus: • Vardas ir pavardė • Asmens kodas • Namų adresas • El. pašto adresas • Telefono numeris • Interneto identifikatorius • Atsitiktinės nuotraukos ar vaizdo įrašai, kuriuose matomas asmuo • Visi pateikti atsakymai teisingi	Visi pateikti variantai teisingi	2	1	Pilietiškumo, Pažinimo
2	Europos Parlamento ir Tarybos Bendrajame duomenų apsaugos		2	2	Pilietiškumo,

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėti ngumo lygis (1–4)	Ugdomos kompetencijos
	reglamente (BDAR) tarp asmens duomenų minimas interneto identifikatorius (angl. „online identifier“). Kas yra interneto identifikatorius? - Tai IP adresas, el.pašto adresas, socialinių tinklų vartotojo vardas, slapukai (angl. cookies) ir kt. Duomenys, kurie gali būti naudojami fizinio asmens nustatymui internete - Interneto identifikatorius yra tik fizinio asmens vardas ir pavardė, nes tai yra pagrindiniai duomenys, reikalingi asmens identifikavimui - Interneto identifikatorius yra visų interneto svetainių, kurias aplankė vartotojas, sąrašas, tačiau tai nesusiję su interneto vartotojo identifikavimu - Tai prieigos prie interneto svetainių, kuriose būtina registracija, vartotojo slaptažodis, kurį jis naudoja prisijungimui prie interneto paslaugų.				Pažinimo
3	Europos Parlamento ir Tarybos Bendrajame duomenų apsaugos reglamente (BDAR) nurodyta, nepilnametis nuo 16 metų pats gali duoti sutikimą tvarkyti savo asmens duomenis. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatyme (ADTA) sakoma, kad vaiko vaiko asmens duomenų tvarkymas yra teisėtas, jei sutikimą davė ne jaunesnis negu 14 metų vaikas. Tad nuo kokio amžiaus asmuo Lietuvoje pats gali duoti sutikimą tvarkyti savo asmens duomenis? - Nuo 18 metų, t.y. tapęs pilnamečiu - Nuo 16 metų, kaip nurodyta BDAR - Nuo 14 metų, kaip nurodyta Lietuvos ADTA įstatyme	Nuo 14 metų	1	1	Pilietiškumo, Pažinimo
4	Kurie du iš paminėtų teiginių priskirtini kibernetinio saugumo principams: - Teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje - Taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti kiekvieno asmens interesų apsaugą, ir niekada negali riboti asmens laisvės - Už tinklų ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi Teisingumo ministerija ir Savivaldybės, kuriose veikia įmonės, kurioms priklauso tos informacinės sistemos - Taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos labiau, negu tai	Teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje Taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos labiau, negu tai būtina kibernetiniam	2	1	Pilietiškumo, Pažinimo

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėti ngumo lygis (1–4)	Ugdomos kompetencijos																								
	būtina kibernetiniam saugumui užtikrinti	saugumui užtikrinti																											
5	Antrame stulpelyje prie kiekvieno teiginio įrašykite K kaidę, jei atitinkamoje pirmo stulpelio eilutėje esantis teiginys taikytinas <i>kvalifikuotam elektroniniam parašui</i> arba N raidę, jei tas teiginys priskirtinas <i>nekvalifikuotam elektroniniam parašui</i>: <table><tr><td>Teisiškai prilyginamas ranka pasirašytam parašui</td><td></td></tr><tr><td>Nėra prilyginamas ranka pasirašytam parašui ir gali būti ginčijamas teisme</td><td></td></tr><tr><td>Priimamas visose ES valstybėse</td><td></td></tr><tr><td>Teisinis statusas priklauso nuo to, kaip jis buvo sukurtas ir naudojamas</td><td></td></tr><tr><td>Sukuriamas naudojant kvalifikuotą elektroninio parašo sukūrimo priemonę</td><td></td></tr><tr><td>Dažnai remiasi viešųjų raktų infrastruktūra (VRI) ir išduodamas sertifikuotų paslaugų teikėjų</td><td></td></tr><tr><td>Gali būti sukurtas naudojant paprastas programines priemones, pavyzdžiui, el. pašto programas ar tekstų redaktorius ir pan.</td><td></td></tr><tr><td>Tinka įvairioms teisės aktų reikalaujamos situacijoms, pavyzdžiui, sudarant sutartis, teikiant oficialius dokumentus, pasirašant elektroninius mokesčius ir pan.</td><td></td></tr></table>	Teisiškai prilyginamas ranka pasirašytam parašui		Nėra prilyginamas ranka pasirašytam parašui ir gali būti ginčijamas teisme		Priimamas visose ES valstybėse		Teisinis statusas priklauso nuo to, kaip jis buvo sukurtas ir naudojamas		Sukuriamas naudojant kvalifikuotą elektroninio parašo sukūrimo priemonę		Dažnai remiasi viešųjų raktų infrastruktūra (VRI) ir išduodamas sertifikuotų paslaugų teikėjų		Gali būti sukurtas naudojant paprastas programines priemones, pavyzdžiui, el. pašto programas ar tekstų redaktorius ir pan.		Tinka įvairioms teisės aktų reikalaujamos situacijoms, pavyzdžiui, sudarant sutartis, teikiant oficialius dokumentus, pasirašant elektroninius mokesčius ir pan.		<table><tr><td>K</td></tr><tr><td>N</td></tr><tr><td>K</td></tr><tr><td>N</td></tr><tr><td>K</td></tr><tr><td>K</td></tr><tr><td>N</td></tr><tr><td>K</td></tr></table>	K	N	K	N	K	K	N	K	4	2	Pilietiškumo, Pažinimo
Teisiškai prilyginamas ranka pasirašytam parašui																													
Nėra prilyginamas ranka pasirašytam parašui ir gali būti ginčijamas teisme																													
Priimamas visose ES valstybėse																													
Teisinis statusas priklauso nuo to, kaip jis buvo sukurtas ir naudojamas																													
Sukuriamas naudojant kvalifikuotą elektroninio parašo sukūrimo priemonę																													
Dažnai remiasi viešųjų raktų infrastruktūra (VRI) ir išduodamas sertifikuotų paslaugų teikėjų																													
Gali būti sukurtas naudojant paprastas programines priemones, pavyzdžiui, el. pašto programas ar tekstų redaktorius ir pan.																													
Tinka įvairioms teisės aktų reikalaujamos situacijoms, pavyzdžiui, sudarant sutartis, teikiant oficialius dokumentus, pasirašant elektroninius mokesčius ir pan.																													
K																													
N																													
K																													
N																													
K																													
K																													
N																													
K																													
6	Elektroninis spaudas – tai - o fizinio asmens naudojama elektroninė technologija, skirta dokumentams elektroniniu būdu pasirašyti ir patvirtinti, jog asmuo pats sukūrė dokumentą bei užtikrinti jo vientisumą - o elektroninė technologija, skirta dokumentams arba duomenims autentifikuoti, užtikrinant jų kilmės patikimumą ir nepažeistumą bei	elektroninė technologija, skirta dokumentams arba duomenims autentifikuoti, užtikrinant jų kilmės patikimumą ir nepažeistumą bei naudojamas įmonės,	1	1	Pilietiškumo, Pažinimo																								

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėtingumo lygis (1–4)	Ugdomos kompetencijos
	naudojamas įmonės, organizacijos ar kitos juridinio asmens tapatybei patvirtinti. - elektroninė sistema, naudojama dokumentų turiniui redaguoti ir keisti, kai reikia užtikrinti informacijos tikslumą ir nuoseklumą - elektroninė priemonė, leidžianti fiziniam asmeniui anonimiškai siųsti dokumentus internetu, neatskleidžiant nei jo, nei organizacijos tapatybės	organizacijos ar kitos juridinio asmens tapatybei patvirtinti.			
7	Kam gali būti išduodamas elektroninis spaudas? - Kiekvienam pilnamečiui fiziniam asmeniui - Tik juridiniams asmenims - Ir fiziniams ir juridiniams asmenims - Tik valstybinėms institucijoms	Tik juridiniams asmenims	1	1	Pilietiškumo, Pažinimo
8	Kokia elektroninės laiko žymos paskirtis? - Laiko žyma suteikia unikalų dokumento registracijos numerį, kuris leidžia nustatyti to dokumento savininką, sukūrimo vietą ir laiką - Laiko žyma nurodo dokumento galiojimo laikotarpį, po kurio dokumentas tampa nebegaliojantis ir turi būti pakeistas nauju - Laiko žyma garantuoja, kad konkretus dokumentas arba duomenys egzistavo tam tikru metu ir nuo to momento nebuvo pakeisti - Laiko žyma suteikia galimybę elektroninį dokumentą perskaityti tik nurodytam laiko momentui praėjus ir fiksuoja dokumento peržiūrų skaičių	Laiko žyma garantuoja, kad konkretus dokumentas arba duomenys egzistavo tam tikru metu ir nuo to momento nebuvo pakeisti	1	1	Pilietiškumo, Pažinimo
9	Pažymėkite du iš šių teiginių, taikytinus <i>privačiąjam</i> šifravimo raktui. - Tai raktas, naudojamas duomenims užšifruoti, kad tik turintis atitinkamą viešąjį raktą galėtų juos dešifruoti - Tai slaptas raktas, kurį turi tik duomenų savininkas, ir naudojamas užšifruotiems duomenims iššifruoti - Tai raktas, kuris leidžia visiems vartotojams, turintiems kurį nors viešąjį raktą, dešifruoti užšifruotus duomenis - Tai raktas, kuriuo gali būti dalijamas su kitais, kad jie galėtų iššifruoti užšifruotus duomenis - Tai raktas, kuriuo nesidalijama su kitais, ir kuris užtikrina, kad tik duomenų savininkas gali pasiekti ir iššifruoti užšifruotus duomenis	Tai slaptas raktas, kurį turi tik duomenų savininkas, ir naudojamas užšifruotiems duomenims iššifruoti Tai raktas, naudojamas duomenims užšifruoti, kad tik turintis atitinkamą viešąjį raktą galėtų juos dešifruoti Tai raktas, kuriuo nesidalijama su kitais, ir kuris užtikrina, kad tik duomenų savininkas gali pasiekti ir iššifruoti užšifruotus duomenis	2	1	Pilietiškumo, Pažinimo

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėtingumo lygis (1–4)	Ugdomos kompetencijos
10	Pažymėkite du iš šių teiginių, taikytinus <i>viešajam</i> šifravimo raktui - Tai raktas, kuriuo galima laisvai dalytis, kad kiti galėtų užšifruoti duomenis, kuriuos jie nori siųsti asmeniui, turinčiam privatųjį raktą - Tai slapto raktas, kurį turi tik duomenų savininkas, ir jis naudojamas užšifruotiems duomenims iššifruoti - Tai raktas, kuris leidžia bet kuriam, turinčiam privatųjį raktą, iššifruoti užšifruotus duomenis. - Tai raktas, naudojamas duomenims užšifruoti taip, kad tik turintis atitinkamą privatųjį raktą galėtų juos iššifruoti - Tai slapto raktas, užtikrinantis duomenų vientisumą	Tai raktas, kuriuo galima laisvai dalytis, kad kiti galėtų užšifruoti duomenis, kuriuos jie nori siųsti asmeniui, turinčiam privatųjį raktą. Tai raktas, naudojamas duomenims užšifruoti taip, kad tik turintis atitinkamą privatųjį raktą galėtų juos iššifruoti	2	1	Pilietiškumo, Pažinimo
11	Kurie iš išvardintų teisės aktų reglamentuoja asmens duomenų apsaugą Lietuvos Respublikoje? Pažymėkite visus teisingus atsakymus. - Europos Parlamento ir Tarybos Bendrasis duomenų apsaugos reglamentas - Lietuvos Respublikos Autorių teisių ir gretutinių teisių įstatymas - Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas - Lietuvos Respublikos Kibernetinio saugumo įstatymas	Europos Parlamento ir Tarybos Bendrasis duomenų apsaugos reglamentas Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas	2	1	Pilietiškumo, Pažinimo
12	Kurios Lietuvos Respublikos institucijos kontroliuoja, kaip laikomasi asmens duomenų apsaugos įstatymų nuostatų? - Valstybinė vartotojų teisių apsaugos tarnyba - Valstybinė duomenų apsaugos inspekcija - Vadovybės apsaugos tarnyba - Valstybės kontrolė	Valstybinė duomenų apsaugos inspekcija	1	1	Pilietiškumo, Pažinimo
13	Organizacija nori kaupti nuotraukų, turinčių istorinę ar visuomeninę svarbą šios organizacijos veiklai, archyvą. Kokio pobūdžio nuotraukas ji galėtų kaupti tame archyve, neturėdama nuotraukose užfiksuotų asmenų sutikimo? - Organizacijos darbuotojų gimtadienių šventimo vakarėlių nuotraukos - Organizacijos vadovo paskyrimo ceremonijos nuotraukos - Organizacijos darbuotojų valstybinio apdovanojimo akimirkų nuotraukos - Kalėdų eglutės renginio darbuotojų vaikams akimirkos - Organizacijos darbuotojų turistinės poilsinės išvykos nuotraukos	Organizacijos vadovo paskyrimo ceremonijos nuotraukos Organizacijos darbuotojų valstybinio apdovanojimo akimirkų nuotraukos	2	2	Pilietiškumo, Pažinimo
14	Ar gali organizacija kaupti ir laikyti visas ir visų savo organizacijos renginių nuotraukas, padarytas ir gautas iki BDAR įsigaliojimo? Taip, gali, nes įstatymai netaikomi atgaline data	Ne, negali, nes BDAR taikomas visiems asmens duomenims, kuriuos	1	1	Pilietiškumo, Pažinimo

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėti ngumo lygis (1–4)	Ugdomos kompetencijos
	Ne, negali, nes BDAR taikomas visiems asmens duomenims, kuriuos organizacija turi arba tvarko, nepriklausomai nuo jų gavimo datos	organizacija turi arba tvarko, nepriklausomai nuo jų gavimo datos			
15	Kurių duomenų organizacija (duomenų valdytojas), net gavusi asmens (duomenų subjekto) prašymą, negali atskleisti? Pažymėkite visus teisingus atsakymus: - Duomenų, susijusių su kitų asmenų teisėmis ir privatumu - Duomenų, kurių atskleidimas gali trukdyti vykstantiems teisėsaugos tyrimams arba kelti pavojų visuomenės ar nacionaliniam saugumui - Duomenų, susijusių su vidaus tyrimais ar darbuotojų vertinimais - Konfidencialių verslo ar profesinių duomenų - Duomenų, kurių pateikimas lemtų duomenų apsaugos technologijų, prieigos kontrolės metodų atskleidimą ir tai galėtų padaryti sistemas pažeidžiamas - Visi atsakymai teisingi	Visi atsakymai teisingi	3	2	Pilietiškumo, Pažinimo
16	Kurias iš žemiau išvardytų teisių turi asmuo (duomenų subjektas): - gauti informaciją apie savo asmens duomenų tvarkymą - susipažinti su saugomais savo asmens duomenimis - atšaukti savo sutikimą tvarkyti asmens duomenis - prašyti ištrinti su duomenų subjektu susijusius asmens duomenis - prašyti apriboti savo asmens duomenų tvarkymą - nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi - turi visas išvardytas teises	turi visas išvardytas teises	3	1	Pilietiškumo, Pažinimo
17	Kurios paslaugos laikytinos elektroninės informacijos prieglobos paslaugomis? - Tinklalapių priegloba - Programinės įrangos licencijavimas - Debesų saugykla - El. pašto priegloba - Išorinių laikmenų su svarbia informacija saugojimo paslauga nuomojamame banko seife	Tinklalapių priegloba Debesų saugykla El. pašto priegloba			Pilietiškumo, Pažinimo
18	Kas laikoma ypatingos svarbos informacine infrastruktūra? - Aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą. - Elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos	Elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar			Pilietiškumo, Pažinimo

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėti ngumo lygis (1–4)	Ugdomos kompetencijos
	dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams. ○ Visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti. ○ Informacinės visuomenės paslaugos, apimančios galimybės naudotis elektroninės informacijos ir elektroninių duomenų (toliau – elektroninė informacija) kūrimo ir tvarkymo priemonėmis sudarymą ir (arba) paslaugų gavėjo pateiktos elektroninės informacijos saugojimą	viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.			
19	Kurie iš paminėtų pavyzdžių priskirtini kibernetinėms erdvėms? ● Debesų saugykla. ● „Pokalbiai, vykstantys realioje kavinėje. ● Socialinis tinklas „Facebook“. ● Spausdintų laikraščių saugykla.	Debesų saugykla. Socialinis tinklas „Facebook“.	2	1	Pilietiškumo, Pažinimo
20	Kurie iš šių įvykių tikrai laikytini kibernetiniais incidentais: ● Svarbių duomenų nutekėjimas. ● Dėl techninių problemų nutrūkęs interneto ryšys, laikinai pertraukęs Valstybės vadovo kreipimosi šalies gyventojus, transliaciją. ● Kenkėjiškos programinės įrangos (angl. malware) infekcija ● Kompiuterio kietojo disko gedimas, dėl kurio sutrūko kompiuterio darbas, o duomenys diske tapo nebeprieinami. ● Kompiuterio veikimo nestabilumas, atsiradęs nepavykus atnaujinti operacinės sistemos ● Vartotojas nustatė netinkamus programos parametrus, dėl ko programos veikimas tapo nestabilus.	Svarbių duomenų nutekėjimas. Kenkėjiškos programinės įrangos (angl. malware) infekcija	2	1	Pilietiškumo, Pažinimo
21	Koks ryšys tarp kibernetinės saugos ir duomenų saugos? Nurodykite du teisingus atsakymus ● Kibernetinė sauga apima tik fizinius saugumo aspektus, o duomenų sauga susijusi tik su duomenų šifravimu. ● Duomenų sauga yra kibernetinės saugos dalis, nes ji užtikrina,	Duomenų sauga yra kibernetinės saugos dalis, nes ji užtikrina, kad duomenys būtų saugūs ir apsaugoti nuo neautorizuoto	2	2	Pilietiškumo, Pažinimo

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėti ngumo lygis (1–4)	Ugdomos kompetencijos
	kad duomenys būtų saugūs ir apsaugoti nuo neautorizuoto prieigos. • Kibernetinė sauga yra atsakinga už tinklų apsaugą, o duomenų sauga neturi jokios įtakos kibernetiniams incidentams. • Kibernetinė sauga ir duomenų sauga yra visiškai skirtingos sritys, kurios nesusijusios tarpusavyje. • Kibernetinė sauga apima technologijas ir procesus, kurie padeda užtikrinti duomenų saugumą ir konfidencialumą organizacijoje.	prieigos. Kibernetinė sauga apima technologijas ir procesus, kurie padeda užtikrinti duomenų saugumą ir konfidencialumą organizacijoje.			
22	Kuris iš pateiktų apibrėžimų apibūdina saugųjį valstybinį duomenų perdavimo tinklą? ○ Tai interneto platforma, kuri sudaro galimybes galutiniams naudotojams įvairiais įrenginiais prisijungti, dalytis turiniu, rasti vienam kitą ir skelbiamą turinį, visų pirma per pokalbius, įrašus, vaizdo įrašus ir rekomendacijas. ○ Tai kompiuterių tinklas, į kurį sujungti visi Seimo ir ministerijų darbuotojų kompiuteriai. ○ Tai valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas ○ Tai tinklas, naudojamas duomenis perduoti tarp valstybinių ir savivaldybių institucijų.	Tai valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas	1	2	Pilietiškumo, Pažinimo
23	Kuris iš šių atvejų laikytinas rizika, galinčia pakenkti informacinės sistemos saugumui? ○ Duomenų bazės apsauga naudojant šifravimą. ○ Netikėti elektros tiekimo sutrikimai, galintys paveikti sistemos prieinamumą. ○ Nuolatinis sistemos auditas saugumui užtikrinti. ○ Prieigos prie duomenų ribojimas, laikantis BDAR reikalavimų.	Netikėti elektros tiekimo sutrikimai, galintys paveikti sistemos prieinamumą.	1	1	Pilietiškumo, Pažinimo
24	Ryšių ir informacinės sistemos spraga – ○ tai kenkėjiškos programos (angl. malware) atliktas ryšių ir informacinės sistemos pakeitimas. ○ tai ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas. ○ tai ryšių ir informacinės sistemos darbo sutrikimas dėl interneto ryšio nutrūkimo. ○ Tai laikinas ryšių ir informacinės sistemos sutrikimas, kuris nekelia grėsmės duomenų saugumui.	ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas	1	1	Pilietiškumo, Pažinimo
25	Kuris iš pateiktų atsakymų variantų apibūdina kibernetinių incidentų	Incidentų aptikimas, analizė,	1	1	Pilietiškumo,

Nr.	Testo klausimas	Teisingas atsakymas	Taškų skaičius	Sudėtingumo lygis (1–4)	Ugdomos kompetencijos
	valdymo procesą? ○ Incidento tyrimas ir su juo susijusių duomenų kaupimas ○ Incidentų aptikimas, analizė, reagavimas ir sistemos veiklos atkūrimas. ○ Svarbiausių tinklo veikimo parametrų stebėjimas ir informacijos apie tai kaupimas. ○ Informacinės sistemos apsaugos priemonių ir incidentų įrašų saugojimas	reagavimas ir sistemos veiklos atkūrimas			Pažinimo
26	Kurie iš išvardintų failų formatų vartojami viešiesiems ir privatesiems raktams, naudojamiems duomenų užšifravimui ir iššifravimui, įrašyti? ○ .docx, .xlsx, .odt ○ .pem, .key, .crt, .txt ○ .bmp, .gif, .png ○ .mp4, .mov, .mp3	.pem, .key, .crt, .txt	1	1	Pilietiškumo, Pažinimo

Panaudoti šaltiniai:

- Europos Parlamento ir Tarybos Bendrasis duomenų apsaugos reglamentas:
<https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016R0679>
- Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas:
<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr>
- Lietuvos Respublikos Kibernetinio saugumo įstatymas:
<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr>

Pastabos dėl „Kibernetinio saugumo įstatymo“ įstatymo

2023–2024 metais įstatymas buvo keistas 3 kartus ir naujausioje jo redakcijoje nebeliko ankstesnėse redakcijose buvusių kai kurių apibrėžimų, kai kurie apibrėžimai perimti iš ES direktyvų. Tad čia pateikiame mokytojams visus, kad nereikėtų ieškoti. Įstatymo keitimai nekeičia pačių sąvokų apibrėžčių esmės (kartais kai kurios gali būti patikslinamos, bet esmė nesikeičia). Nepriklausomai nuo to, yra tos sąvokos apibrėžtos įstatyme, ar nera, bet jas galima apibrėžti taip, kaip buvo 2021 m. įstatymo redakcijoje.

Informatikos Bendrojoje programoje minimos su kibernetinio saugumo tema susijusios sąvokos

(pilka spalva – tos, kurių nebėra 2024-07-11 įstatymo redakcijoje)

Elektroninės informacijos prieglobos paslaugos – paslaugos, apimančios galimybės naudotis elektroninės informacijos ir elektroninių duomenų (toliau – elektroninė informacija) kūrimo ir tvarkymo priemonėmis sudarymą ir (arba) paslaugų gavėjo pateiktos elektroninės informacijos laikymą.

Ypatingos svarbos informacinė infrastruktūra – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriamą ir (arba) jais perduodama elektroninė informacija.

Kibernetinio saugumo krizė – kibernetinis incidentas arba incidentai, kurių sukulto neigiamo poveikio Lietuvos Respublika negali pašalinti viena pati arba kurie Lietuvos Respublikai ir kitoms valstybėms, priklausančioms tarptautinėms organizacijoms, kurių narė yra Lietuvos Respublika, arba tų tarptautinių organizacijų institucijoms sukelia tokio masto ir tokios techninės arba politinės reikšmės neigiamą poveikį, kad iškyla poreikis koordinuoti politiką ir reaguoti tarptautiniu lygmeniu.

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdančios ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

Kibernetinis saugumas [iš Reglamento [\(ES\) 2019/881](#)] – visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių

Kibernetinio incidento valdymas – veiksmai ir procedūros, kuriais siekiama užkirsti kelią kibernetiniam incidentui, jį atskleisti, išanalizuoti ir sustabdyti arba jį reaguoti ir atkurti veiklą po jo.

Ryšių ir informacinė sistema – elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriamą arba perduodama elektroninė informacija.

Ryšių ir informacinės sistemos spraga (toliau – spraga) – ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas.

Kibernetinio saugumo rizika – potencialus praradimas arba sutrikimas, kurį gali sukelti kibernetinis incidentas. Kibernetinio saugumo rizika išreiškiama kaip tokio praradimo arba sutrikimo masto ir kibernetinio incidento tikimybės derinys.]

Saugusis valstybinis duomenų perdavimo tinklas – valstybės valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis ir nuo viešųjų elektroninių ryšių tinklų nepriklausomas elektroninių ryšių tinklas.

Kibernetinio saugumo principai

1. Kibernetinis saugumas grindžiamas šiais kibernetinio saugumo principais:

- 1.1. **kibernetinės erdvės nediskriminavimo** – teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje;
- 1.2. **kibernetinio saugumo rizikos valdymo** – taikomos kibernetinio saugumo rizikos valdymo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;
- 1.3. **kibernetinio saugumo proporcingumo** – taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos labiau, negu tai būtina kibernetiniam saugumui užtikrinti;
- 1.4. **viešojo intereso viršenybės** – taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų, kibernetinio saugumo subjektų teisių ir teisėtų interesų ar neproporcingai apriboti jų laisvės;
- 1.5. **standartizacijos ir technologinio neutralumo** – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir informacinių sistemų saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;
- 1.6. **subsidiarumo** – už tinklų ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinai kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai tinklų ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo neužtikrina šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

2. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus šio straipsnio 1 dalyje nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.