

Kandavas Lauksaimniecības tehnikuma
Saulaines teritoriālā struktūrvienība
METODISKAIS DARBS

Darba nosaukums:

Datortehnikas fiziskā drošība

Autors:

Uldis Šķirmants

Izglītības programma / Modulis:

Datorsistēmas, datu bāzes un datu tīkli / Datortehnikas drošība

Izstrādes vieta:

Kandavas LT Saulaines TS

Mācību gads: 2025. /2026.

**MODULĀRĀS PROFESIONĀLĀS IZGLĪTĪBAS PROGRAMMAS
obligātās daļas (B daļas) profesionālo kompetenču moduļu novērtēšanas**

**UZDEVUMI UN TO IZPILDES VĒRTĒŠANAS KRITĒRIJI
Elektronisko un optisko iekārtu ražošanas, informācijas un komunikācijas
tehnoloģijas nozare, profesionālā kvalifikācija "Datorsistēmu tehniķis",
4. LKI līmenis**

**Obligātā daļa (B daļa)
Modulis "Datortehnikas drošība"**

Pārbaudījuma programma

Mērķis	Veidot izglītojamo izpratni par datortehnikas fizisko drošību.									
Darba uzbūve	Uzdevumu skaits	3								
	Uzdevumu veidi	Atbildes uz zināšanu pārbaudes jautājumiem, atbilžu izvēles uzdevumi, praktiskais darbs								
	Uzdevumu kopējais izpildes laiks	80 minūtes: 10 minūtes sagatavoties; 70 minūtes uzdevumu izpildei								
Sasniedzamais rezultāts (15% no moduļa kopējā apjoma)	Spēj: nodrošināt datortehnikas fizisko drošību. Zina: datu aizsardzības pasākumus, kas ir vērsti uz fiziskās piekļuves vadību un ugunsdrošību. Izprot: datortehnikas fiziskās drošības risinājumus un to lietošanu.									
Norises vieta un nepieciešamie materiālie līdzekļi	Norises vieta: mācību klase ar atsevišķu darba vietu katram izglītojamajam, datoru ar interneta pieslēgumu. Katram izglītojamajam nepieciešams: uzdevumu lapa, A4 papīra lapas, rakstāmpiederumi un dators.									
Vērtēšanas kārtība	Pārbaudījuma uzdevumu izpildi vērtē pedagogs(-i). Vērtēta tiek katra uzdevuma izpilde. Maksimāli iegūstamais punktu skaits ir 40, kas atbilst 100%. Pārbaudījums ir nokārtots, ja uzdevumu izpildes apjoms nav zemāks par 60%. Pārbaudījuma vērtējums tiek izteikts ballēs atbilstoši vērtēšanas skalai:									
Profesionālo kompetenču līmenis	Nepietiekams kvalifikācijas ieguvei				Pietiekams kvalifikācijas ieguvei					
	zems ¹				vidējs ²	optimāls ³			augsts ⁴	
Vērtējums ballēs	1	2	3	4	5	6	7	8	9	10
Uzdevumu izpildes līmenis %	1-14	15-29	30-44	45-59	60-67	68-75	76-83	84-91	92-96	97-100
Iegūto punktu skaits	1-5	6-11	12-17	18-23	24-26	27-30	31-33	34-36	37-38	39-40

Piezīmes.

¹ Zems apguves līmenis: gandrīz viduvēji – 4, vāji – 3, ļoti vāji – 2, ļoti, ļoti vāji – 1.

² Vidējs apguves līmenis: viduvēji – 5.

³ Optimāls apguves līmenis: ļoti labi – 8, labi – 7, gandrīz labi – 6.

⁴ Augsts apguves līmenis: izcili – 10, teicami – 9.

Uzdevumi, to izpildes vērtēšanas kritēriji

Teorētiskā daļa

1.uzdevums. Doti desmit jautājumi par datortehnikas fizisko drošību un risinājumiem. Atbildot uz tiem ņem vērā, ka ir iespējama tikai viena pareizā atbilde uz jautājumu.

Vērtēšanas kritēriji:

Veicamā darbība	Vērtēšanas kritēriji	Izpildes laiks	Piešķirami punkti
Pareizās atbildes izvēle no dotajiem variantiem. Iezīmēt ar zaļu krāsu.	Izvēlas pareizo atbildi no dotajiem variantiem. (1 punkts par katru pareizu atbildi)	15 minūtes	10

1. Kas ir primārais mērķis datortehnikas fiziskās drošības nodrošināšanai?

- a) Uzlabot datora programmatūru.
- b) Novērst datu zudumus ugunsgrēka gadījumā.
- c) Ierobežot nesankcionētu piekļuvi datortechnikai.
- d) Nodrošināt ātrāku datu apstrādi.

2. Kāds ir svarīgākais ugunsdrošības elements datortelpās?

- a) Automātiska ugunsdzēsības sistēma.
- b) Logu restes.
- c) Tīklsavienojumu pārraudzības programmatūra.
- d) Papildus monitori.

3. Kas raksturo fiziskās piekļuves kontroli?

- a) BIOS paroles iestatīšana.
- b) Telpas aprīkošana ar piekļuves kartēm.
- c) Datora antivīrusa uzstādīšana.
- d) Pārlūkprogrammas iestatījumu maiņa.

4. Kādi datortehnikas fiziskās aizsardzības risinājumi ir efektīvi birojos?
- a) Uzglabāšana slēdzamā skapī.
 - b) Datu dublēšana mākoņkrātuvē.
 - c) Monitoru rezolūcijas pielāgošana.
 - d) Programmatūras atjauninājumu veikšana.
5. Ko neiekļauj datortehnikas fiziskās drošības pasākumos?
- a) Videonovērošanas uzstādīšanu.
 - b) Elektroenerģijas nepārtrauktības nodrošināšanu.
 - c) Logu un durvju aizsardzību.
 - d) Piekļuves kodu izmantošanu.
6. Kāda veida drošības risinājums ir atslēgas slēdzenes datoru korpusā?
- a) Programmatūras drošības risinājums.
 - b) Fiziskās drošības risinājums.
 - c) Datu drošības risinājums.
 - d) Tīkla drošības risinājums.
7. Kā rīkoties, lai novērstu aparatūras bojājumus no mitruma?
- a) Izmantojot pretvīrusu programmatūru.
 - b) Pārliecinoties, ka telpa ir pareizi ventilēta.
 - c) Pieslēdzot datoru UPS iekārtai.
 - d) Lietojot aizsardzības paroles.
8. Kas ir fiziskās drošības risinājuma piemērs, lai novērstu zādzību?
- a) Datora šifrēšana.
 - b) Datora stiprināšana ar trosi pie galda.
 - c) Interneta ātruma uzlabošana.
 - d) Lietotāju paroles maiņa.

9. Kas ir nozīmīgs datortehnikas ugunsdrošības aspekts?

- a) RCD (diferenciālās aizsardzības releja) uzstādīšana.
- b) Monitoru skaita ierobežošana.
- c) Interneta drošības programmu uzstādīšana.
- d) Fizisko slēdžu lietošana datora korpusā.

10. Kāds ir visbiežāk izmantotais veids, lai aizsargātu telpu ar datortehniku?

- a) Biometrijas piekļuves kontrole.
- b) Elektroenerģijas taupīšanas plāni.
- c) Vīrusu definīciju atjaunošana.
- d) Iekšējā tīkla konfigurēšana.

2.uzdevums. Doti desmit jautājumi par datu aizsardzības pasākumiem, kas saistīti ar fizisko drošību. Atbildot uz tiem ņem vērā, ka ir iespējama tikai viena pareizā atbilde uz jautājumu.

Vērtēšanas kritēriji

Veicamā darbība	Vērtēšanas kritēriji	Izpildes laiks	Piešķiramie punkti
Pareizās atbildes izvēle no dotajiem variantiem. Iezīmēt ar zaļu krāsu.	Izvēlas pareizo atbildi no dotajiem variantiem. (1 punkts par katru pareizu atbildi)	15 minūtes	10

1. Kas ir svarīgākais, lai nodrošinātu fizisko datu aizsardzību?

- a) Programmatūras regulāra atjaunošana.
- b) Telpu droša noslēgšana.
- c) Datora restartēšana.
- d) Uzstādīšana uz cietā diska.

2. Kas samazina risku aparatūras bojājumiem no elektroenerģijas pārrāvuma?

- a) Pārsprieguma aizsargi.
- b) Spēcīgāka tīkla karte.
- c) RAM palielināšana.
- d) Operētājsistēmas dublēšana.

3. Kāda ir ugunsdzēsamā aparāta nozīme datortehnikas drošībā?

- a) Ugunsgrēka likvidēšana.
- b) Datoru nofiksēšana.
- c) Tīkla drošības nodrošināšana.
- d) Aparatūras šifrēšana.

4. Kā pareizi jāuzstāda fiziskās piekļuves kontroles sistēmas?

- a) Lai aizsargātu tikai darbinieku datorus.
- b) Lai ierobežotu piekļuvi telpām ar sensitīviem datiem.
- c) Lai bloķētu piekļuvi internetam.
- d) Lai kontrolētu printeru darbību.

5. Kāds ir viens no pamata pasākumiem, lai samazinātu datu zuduma risku ugunsgrēka gadījumā?

- a) Fiziskās serveru atslēgšanas pogas izmantošana.
- b) Datu glabāšana ugunsdrošās telpās vai skapjos.
- c) Antivīrusu programmatūras instalēšana.
- d) Tīkla aizsargāšana ar ugunsdzēsmašīnām.

6. Kāda ir fiziskās piekļuves kontroles galvenā funkcija?

- a) Datora atjaunināšana uz jaunāko operētājsistēmu.
- b) Atļaut piekļuvi datortehnikai tikai pilnvarotām personām.
- c) Aizsargāt programmatūru no vīrusiem.
- d) Uzraudzīt interneta savienojuma kvalitāti.

7. Ko nozīmē drošības audits saistībā ar fiziskās piekļuves kontroli?

- a) Operētājsistēmas pārbaudi uz trūkumiem.
- b) Iekārtu fiziskās aizsardzības stāvokļa novērtēšanu.
- c) Datu šifrēšanas sistēmas izvērtēšanu.
- d) Lokālā tīkla konfigurācijas analīzi.

8. Kas ir svarīgs elements ugunsdrošības plānā datortechnikas telpām?

- a) Kabeļu uzglabāšana ugunsdrošos maisos.
- b) Ugunsdrošības signalizācijas uzstādīšana un uzturēšana.
- c) Lokālā tīkla ātruma paaugstināšana.
- d) Tīkla printera novietošana tālu no sienām.

9. Kāds ir iemesls, kāpēc datoru laboratorijās tiek izmantotas drošības kameras?

- a) Lai monitorētu tīkla ātrumu.
- b) Lai novērotu nesankcionētu piekļuvi telpām.
- c) Lai regulētu strāvas padevi datoriem.
- d) Lai pārbaudītu operētājsistēmas funkcionalitāti.

10. Kādi risinājumi ir efektīvi pret zādzībām datortechnikas telpās?

- a) Kabeļu pārbaude katru dienu.
- b) Videonovērošanas sistēmas un fiziskās aizsardzības ierīces (piemēram, slēdzenes).
- c) Lokālā tīkla darbības uzraudzība.
- d) Elektroniskās pastkastes uzstādīšana.

Praktiskā daļa

Datortechnikas fiziskās drošības risinājumu novērtējums

1.uzdevums. Izveido drošības plānu telpai ar 5 datoriem, izmantojot vismaz 4 dažādus fiziskās drošības risinājumus.

Plānā jāiekļauj:

- * Fiziskās piekļuves kontroles sistēmas risinājumi.
- * Ugunsdrošības un elektrodrošības pasākumi.
- * Aizsardzības pret zādzībām risinājumi.
- * Darba drošības un vispārējās cilvēka drošības un darba apstākļu risinājumi.

Rezultāts: Drošības plāns jānoformē rakstveidā, sniedzot īsu pamatojumu izvēlētajiem risinājumiem. Izpildes laiks: 40 minūtes.

Vērtēšanas kritēriji

Kopējais maksimālais punktu skaits: 20 punkti.

Uzdevuma sadalījums un punkti:

Praktiskais uzdevums tiek sadalīts vairākos izpildes kritērijos. Katrs kritērijs ir vērtējams atsevišķi, piešķirot punktus atbilstoši precizitātei un kvalitātei.

Vērtēšanas kritērijs	Punktu skaits	Vērtējuma apraksts
1. Fiziskās piekļuves kontroles sistēmas risinājumi	0–5	5: Skaidri aprakstīti pieejas kontroles mehānismi (slēdzamas durvis, piekļuves kartes, videonovērošana). 2–4: Apraksts nepilnīgs vai nepietiekami pamatots. 0–1: Nav iekļauts vai neatbilstošs.
2. Ugunsdrošības pasākumi	0–3	3: Norādīti konkrēti risinājumi (ugunsdzēsamie aparāti, dūmu detektori, evakuācijas plāni). 1–2: Apraksts nepilnīgs vai daļēji pamatots. 0: Nav iekļauts vai neatbilstošs.
3. Aizsardzība pret zādzībām	0–3	3: Norādīti konkrēti aizsardzības pasākumi (drošības slēdzenes, signalizācijas sistēmas, aparatūras nostiprināšana). 1–2: Apraksts nepilnīgs vai daļēji pamatots. 0: Nav iekļauts vai neatbilstošs.
4. Elektrodrošība	0–3	3: Novērtēta elektroinstalācijas un kabeļu drošība, nodrošināta aizsardzība pret elektrības noplūdēm un pārslodzēm. 1–2: Apraksts nepilnīgs vai nepietiekami pamatots. 0: Nav iekļauts vai neatbilstošs.
5. Ventilācija un darba vides komforts	0–2	2: Norādīts ventilācijas sistēmas stāvoklis un nodrošināta atbilstoša gaisa apmaiņa. 1: Daļēji aprakstīts vai mazāk pamatots. 0: Nav iekļauts vai neatbilstošs.
6. Grīdas segums, mēbeles un telpas plānojums	0–2	2: Izvērtēti riski (grīdas slīdēšana, asi stūri), nodrošināta ergonomiska telpas plānošana. 1: Daļēji izvērtēts vai mazāk pamatots. 0: Nav iekļauts vai neatbilstošs.
7. Pietiekams apgaismojums	0–2	2: Izvērtēts apgaismojuma līmenis un nodrošināts pietiekams apgaismojums darba videi. 1: Daļēji izvērtēts vai mazāk pamatots. 0: Nav iekļauts vai neatbilstošs.

Izstrādāja:

Kandavas Lauksaimniecības tehnikuma

Saulaines teritoriālā struktūrvienība,

Uldis Šķirmants