APSTIPRINĀTS
Ar 18.05.2026 NAA. Senāta sēdes
Protokola Nr. 04/2026 lēmumu Nr.3
Ir spēkā ar 02.06.2026 NAA rektora pavēli Nr. 51

Mākslīgā intelekta izmantošanas noteikumi Latvijas Nacionālajā aizsardzības akadēmijā

I. Vispārīgie noteikumi

1. Mākslīgā intelekta (turpmāk – MI) izmantošanas noteikumi sniedz skaidrojumu par MI korektas izmantošanas pamatprincipiem, to ievērošanu un pārkāpumu izskatīšanas kārtību Latvijas Nacionālajā aizsardzības akadēmijā (turpmāk – NAA).

2. NAA vadībai, studējošajiem, klausītājiem, akadēmiskajam, administratīvajam personālam un citām personām, kuras NAA piedalās un līdzdarbojas izglītības procesā, ir pienākums ievērot MI izmantošanas noteikumus NAA, kā arī MI lietošanas vadlīnijas ar klasifikācijas līmeņiem un atļauto/darāmo darbību precizējumiem (sk. Pielikumu Nr. 1), nepieļaut pārkāpumus un informēt par tiem.

II. Izmantotie termini

3. Mākslīgais intelekts – mašinizēta sistēma, kura projektēta darboties ar dažādiem autonomijas līmeņiem, tā var būt adaptīva, un kura pēc eksplicētajiem (izpaustajiem) vai implicētajiem (pieņemtajiem) mērķiem spēj ģenerēt produktus no sistēmā ievadītās informācijas, kā, piemēram, prognozes, teksta saturu, ieteikumus un lēmumus, kuri var ietekmēt fizisko vai virtuālo vidi.

4. MI mašinizēta sistēma – paredzēta šaura procedūras uzdevumu veikšanai, iepriekš pabeigtas cilvēka darbības rezultāta uzlabošanai, bet tā nav paredzēta, lai aizstātu vai ietekmētu iepriekš pabeigtu cilvēku veiktu novērtējumu bez cilvēka veiktas pārraudzības.

5. Plaši izmantotās mašinizētās sistēmas – MI rīki (piemēram: *Chat GPT*, *Microsoft Copilot*, *Bard*, *Bing*, *Claude*) izmantojami, lai, veicot patstāvīgo izpētes darbu, iegūtu jēdzienu skaidrojumus, radītu jaunas idejas, uzlabotu teksta kvalitāti, gūtu vispārēju priekšstatu par liela apjoma materiālu kā palīgu tekstu tulkošanai un "prāta vētras" asistentu.

6. Zema riska MI rīki – mašinizētas sistēmas, kuras atbalsta patstāvīgi radīto darbu labošanu un pārbaudi, kā arī sistēmas, kuras ļauj vākt un apstrādāt datus, kā, piemēram, gramatikas korekcijas, tulkošanas, audio pārrakstīšanas rīki tekstā un informācijas meklēšanas rīki internetā.

7. Augsta riska MI rīki – mašinizētas sistēmas, kurām var piekļūt izmantojot MI rīkus (piemēram: *Chat GPT*, *Microsoft Copilot*, *Bard*, *Bing*, *Claude*), kuri ir spējīgi ģenerēt autonomus produktus pēc mašinizētā sistēmā ievadītās informācijas.

8. Akadēmiskā godīguma komisija – ar NAA rektora pavēli izveidota komisija akadēmiskā godīguma pārkāpuma gadījumu izskatīšanai, tai skaitā par MI noteikumu neievērošanu NAA.

9. CAPS – plaģiātisma un tekstu oriģinalitātes pārbaudes sistēma, ko izmanto NAA izglītības procesā un kura nosaka MI procentuālo daudzumu izpētes darbā.

III. Mākslīgā intelekta izmantošanas godīguma ievērošana un veicināšana

10. NAA atbalsta un veicina modernu pieeju tehnoloģiju izmantošanu mācību procesā, tai skaitā MI dažādus rīkus. Vienlaikus NAA rūpējas, ka tiek sasniegti kvalitatīvi mācību mērķi un netiek pārkāpti akadēmiskā godīguma principi. NAA sniedz norādījumus un rekomendācijas par MI korektu izmantošanu mācību procesā, lai novērstu un samazinātu akadēmisko pārkāpumu iespējas.

11. NAA akadēmiskajam un administratīvajam personālam un citām personām, kuras NAA piedalās un līdzdarbojas izglītības procesā, ir pienākums veicināt studējošo un klausītāju izpratni par MI korektu izmantošanu un pārkāpumu mazināšanu.

12. MI korektas izmantošanas pasākumi NAA:

12.1. sagatavojot izglītojošu aktivitāti (piemēram, studiju kursu, individuālo izpētes darba uzdevumu, lekciju, grupu darba uzdevumu), docētājam vai personai, kas vada mācību aktivitāti vai atbildīga par to, ir skaidri jādefinē MI izmantošana (atļauts izmantot MI vai nē, un ja atļauts, tad kādā apjomā);

12.2. studējošie un klausītāji var brīvi izmantot zema riska MI rīkus, veidojot atsauces, jo šie MI rīki nerada autonomu jaunu saturu, izņemot gadījumus, kad docētājs vai atbildīgais par mācību aktivitāti ir noteicis citādi;

12.3. studējošie un klausītāji var izmantot MI rīkus kā iedvesmas avotus, lai uzlabotu teksta labskanību, identificētu sinonīmus, paplašinātu izmantotās literatūras apskatus, tulkotu un saprastu komplicētas teorijas. Izpētes darbā MI ģenerētais saturs ir jācitē kā jebkurš cits avots un jāveido atsauces;

12.4. izmantojot MI ģenerētus produktus, studējošie un klausītāji norāda MI rīka izstrādātāju (izstrādes gads), nosaukumu oriģinālvalodā (versiju) (piemēram, *Open AI. (2025). ChatGPT (January 25 version) [Large language model]*. https://chat.openai.com/).

IV. Ierobežojumi, izmantojot mākslīgā intelekta rīkus

13. Individuālās pārbaudes darbos (testi, ieskaites, eksāmeni) nav atļauts izmantot augsta riska MI rīkus, izņemot gadījumos, ja to nepārprotami ir atļāvis docētājs vai cita par izglītības aktivitāti atbildīgā persona. Ja studējošais vai klausītājs neievēro šo noteikumu, tad tas tiks uzskatīts par akadēmiskās krāpšanas gadījumu:

13.1. pirms izvēlētā augsta riska MI rīka izmantošanas studējošajam vai klausītājam ir jāizpēta, kas ir izstrādājis attiecīgo MI rīku, ko izstrādātājs dara ar informāciju, ko tas savāc no MI rīka un izvērtē riskus, ko tas var radīt lietotājam vai trešajām personām;

13.2. studējošajam vai klausītājam ir jāspēj nodalīt savu intelektuālo veikumu no produkta, ko ir ģenerējis MI rīks un, kas nevar tikt uzskatīts par autora radīto, tāpat kā MI rīks nevar tikt uzskatīts par līdzautoru, jo MI rīks nav persona;

13.3. studējošajam vai klausītājam jāizvairās izmantot augsta riska MI rīku kā galveno vai vienīgo informācijas avotu, jo izstrādātās interneta meklētājprogrammas (zema riska MI rīki) ir speciāli izstrādātas šim mērķim un ir ar augstāku ticamības pakāpi;

13.4. augsta riska MI rīki nav izstrādāti matemātisko aprēķinu vai datu apstrādes veikšanai un līdz ar to nedarbojas ar precizitāti kā citi speciāli šo funkciju veikšanai izstrādāti rīki (piemēram, kalkulatori);

13.5. studējošajam vai klausītājam jāapzinās, ka pārmērīga augsta riska MI izmantošana, ģenerējot tekstu, var novest pie situācijas, ka izpētes darbā nav autora novitātes un intelektuālā pienesuma un, izskatot šādu darbu, tiks piemērota procedūra ar pieeju kā plaģiātisma gadījumos;

13.6. ievērojot akadēmiskā godīguma principus, NAA nodrošina visu individuālo izpētes darbu pārbaudi ar CAPS programmu divas reizes. Bakalaura, maģistra vai kvalifikācijas darbu pārbaudei tas tiek nodrošināts pirms darba priekšaizstāvēšanas (pirmo reizi) un pirms darba aizstāvēšanas (otro reizi), pārējos gadījumos studējošais vai klausītājs var vērsties pie docētāja, izglītības aktivitātes nodrošinātāja vai izpētes darba vadītāja, lai veiktu darba pārbaudi ar CAPS programmu, šī aktivitāte netiek reglamentēta un ir docētāja, izglītības aktivitāšu nodrošinātāja, darba vadītāja un studējošā/klausītāja sadarbības process.

V. Akadēmiskā godīguma pārkāpumu veidi, izmantojot mākslīgā intelekta rīkus

14. Par akadēmiskā godīguma pārkāpumu, izmantojot MI rīkus, tiek uzskatīta šāda apzināta rīcība:

14.1. augsta riska MI rīku izmantošana, ja docētājs vai izglītības aktivitātes nodrošinātājs nepārprotami norādījis par aizliegumu tos lietot;

14.2. augsta riska MI rīku izmantošana, neveicot atsauces atbilstoši šo noteikumu 12.4. punktam;

14.3. nepārprotama teksta ģenerēšana, izmantojot augsta riska MI rīkus, ko uzrāda CAPS (izpētes darbā nav iespējams novērtēt autora intelektuālo pienesumu);

14.4. no izpētes darba kopējā apjoma augsta riska MI rīku ģenerētais teksts pārsniedz 20 %.

VI. Pārkāpumu izskatīšana un lēmumu pieņemšana

15. Personu var atzīt par vainīgu, ja tā ir iesaistīta kādā no akadēmiskā godīguma pārkāpumiem – rakstiski, mutiski vai citā formā. Šo noteikumu neievērošanas gadījumā pārkāpums tiek nodots izskatīšanai komisijai, kura izveidota ar rektora pavēli.

1. pielikums

Mākslīgā intelekta (MI) lietošanas vadlīnijas ar klasifikācijas līmeņiem un atļauto/darāmo darbību precizējumiem

1. Vispārējie principi

Visi publiski pieejamie MI rīki, tostarp ģeneratīvie MI (piem., tērzētāji, koda ģeneratori, attēlu un dokumentu ģenerēšanas platformas), tiek uzskatīti par **neuzticamiem**.

NBS nav iespēju kontrolēt, izsekot, labot vai dzēst informāciju, kas ievadīta šādos rīkos, kā arī nav garantiju par datu glabāšanas drošību, rīka drošības praksi vai modeļa turpmāko izmantošanu.

2. Aizliegtie MI rīki

Visi zemāk minētie rīki ir aizliegti, jo tie ir izstrādāti, uzturēti vai tiek nodrošināti valstīs, kuras nav uzskatāmas par drošām informācijas apstrādes jomā. Šo rīku izmantošana var radīt datu noplūdes, izsekošanas un kiberapdraudējumu riskus.

- Ķīnas MI rīki: DeepSeek, Baidu ERNIE Bot (Wenxin Yiyan), Alibaba Qwen / Tongyi Qianwen, Tencent Hunyuan AI, iFlytek SparkDesk, Zhipu AI / ChatGLM / GLM-4, ByteDance AI rīki (t.sk. CapCut MI funkcijas, TikTok MI rīki ar datu augšupielādi), SenseTime SenseNova, Huawei Pangu AI, Kimi AI (Moonshot AI) u. c.;
- Krievijas MI rīki: YandexGPT un Yandex generatīvie MI pakalpojumi, SberGPT / SberDevices "GigaChat", RuGPT-3 / RuGPT modeļi, Tinkoff "TinkoffGPT", VK / Mail.ru MI risinājumi (MARU u. c.), jebkuri MI rīki vai platformas, kas tiek hostētas Krievijas datu centros;
- Baltkrievijas MI rīki: jebkurš rīks, kas tiek pārvaldīts vai hostēts Baltkrievijā, ir aizliegts, piemēram, Synesis un ar to saistītie analītikas/MI rīki, GOV.BY digitālie MI servisi.

3. Ko darbinieki[1] drīkst darīt ar publiskajiem MI rīkiem

- rakstīt ideju prototipus bez datiem;
- lūgt ieteikumus par publiski zināmām tēmām;
- izmantot MI valodas stilistiskai uzlabošanai, ja saturs ir publisks;
- lūgt palīdzību konceptu veidošanā, ja nav izmantoti organizācijas dati;
- pētīt industrijas tendences un publiskus materiālus.

[1] Šajās vadlīnijās termins "darbinieki" ietver NAA vadību, akadēmisko un administratīvo personālu, kā arī studējošos, klausītājus un citas personas, ciktāl tās NAA ietvaros izmanto MI rīkus.

4. Ko darbinieki kategoriski nedrīkst darīt

- ievadīt jebkādus iekšējos vai ierobežotas pieejamības dokumentus MI sistēmā;
- augšupielādēt failus, ekrānuzņēmumus vai fotogrāfijas, kas satur darba informāciju;
- ievadīt personas datus — pat ja tie šķiet sekundāri vai maznozīmīgi (GDPR pārkāpums);
- izmantot MI, lai analizētu vai uzlabotu procesus ar iekšējo informāciju;
- atjaunot vai ģenerēt dokumentus, kas organizācijā klasificēti kā iekšēji vai ierobežota pieejamība;
- izmantot MI rīkus lēmumu pieņemšanai, kas ietekmē drošību, personas datus, SIS vidi, finanšu un apgādes procesus.

5. Informācijas klasifikācijas līmeņi un pieļaujamās darbības

Klasifikācijas līmenis	Ko drīkst darīt	Ko kategoriski nedrīkst darīt
Publiska informācija	Ģenerēt idejas, tekstus, struktūras; Pārfrāzēt informāciju, kas jau publicēta; Lūgt stila vai valodas uzlabojumus; Veidot prezentāciju rāmjus; Uzdot jautājumus par publiski pieejamām tēmām.	Nedrīkst MI norādīt nekādas iekšējās organizācijas detaļas, kas nav publiski apstiprinātas; Nedrīkst ievietot prezentācijas, kurās vēlāk tiks ievietota iekšējā informācija.
Iekšēja informācija	Drīkst izmantot MI tikai konceptuālā līmenī, nesniedzot nekādas detaļas; Var lūgt padomu par procesa labām praksēm bez konkrētiem datiem; Var testēt idejas, ja teksts ir pilnībā pārrakstīts un informācija nav identificējama.	Nedrīkst ievadīt iekšējus dokumentus, protokolus, procedūras; Nedrīkst ievietot piemērus, kas satur organizācijas darbības kontekstu; Nedrīkst augšupielādēt failus vai ekrānuzņēmumus.
Ierobežota pieejamība	MI nedrīkst izmantot nekādos veidos, kas saistīti ar šīs informācijas apstrādi; Vienīgais atļautais MI lietojums: vispārīgi jautājumi bez satura vai konteksta.	Pilnīgs aizliegums jebkādai ierobežotas pieejamības informācijas augšupielādei, kopēšanai, ievadei vai aprakstīšanai MI sistēmās; Nedrīkst veikt rediģēšanu, teksta uzlabošanu vai analīzi, izmantojot MI rīkus; Nedrīkst veidot dokumentus vai politikas ar MI palīdzību.

6. Specifiskais izņēmums: anonimizēti dati

Darbiniekiem ir atļauts izmantot publiskos MI rīkus tehnisko problēmu risināšanai vai kādai datu analīzei tikai tad, ja ievadītie dati ir **pilnībā anonimizēti un nav iespējams atjaunot** (jāizstrādā anonimizācijas algoritms, kas ir jāsaskaņo ar Kiberdrošības pārvaldnieku):

- personas datus;
- sistēmas konfigurācijas;
- drošības incidentu informāciju;
- tīkla struktūru;
- piekļuves tiesības;
- u. c. informācija, kas ir klasificēta.

Anonimizācija nozīmē, ka dati nav tikai aizvietoti ar citiem nosaukumiem, bet ir pilnībā pārvērsti tā, ka nav iespējams deanonimizēt, lai atpazītu reālo sistēmu vai personas.
IT darbiniekiem aizliegts:

- ievadīt jebkādus žurnālfailus, kas satur IP adreses vai sistēmas identifikatorus;
- ievadīt konfigurācijas fragmentus, kurus var atpazīt pēc struktūras;
- sūtīt koda fragmentus, kas satur piekļuves metodes, klasificētas funkcijas vai arhitektūras uzbūvi;
- izmantojot MI, veikt analīzi par reālu incidentu vai ievainojamību.