



**AKCINĖS BENDROVĖS „REGITRA“
GENERALINIS DIREKTORIUS**

**ĮSAKYMAS
DĖL AKCINĖS BENDROVĖS „REGITRA“ KIBERNETINIŲ INCIDENTŲ VALDYMO
TVARKOS APRAŠO PATVIRTINIMO**

2025 m.

d. Nr.

Vilnius

Vadovaudamasis Akcinės bendrovės „Regitra“ įstatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2024 m. birželio 7 d. įsakymu Nr. 1V-385 „Dėl valstybės įmonės „Regitra“ pertvarkymo į akcinę bendrovę „Regitra“, 63.1 papunkčiu bei Informacijos saugumo politikos, patvirtintos akcinės bendrovės „Regitra“ valdybos 2025 m. rugsėjo 16 d. posėdžio protokolu Nr. 2V-5754, 2.7 papunkčiu:

1. Tvirtinu Akcinės bendrovės „Regitra“ kibernetinių incidentų valdymo tvarkos aprašą (pridedama).

2. Paveidu akcinės bendrovės „Regitra“ Veiklos atsparumo ir korupcijos prevencijos skyriui su šiuo įsakymu supažindinti visus suinteresuotus akcinės bendrovės „Regitra“ darbuotojus.

Laikinai einantis generalinio direktoriaus pareigas

Rytis Polikauskas

PATVIRTINTA
Akcinės bendrovės „Regitra“
generalinio direktoriaus
2025 m. d. įsakymu Nr. V

AKCINĖS BENDROVĖS „REGITRA“ KIBERNETINIŲ INCIDENTŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Akcinės bendrovės „Regitra“ kibernetinių incidentų valdymo tvarkos aprašas (toliau – Tvarkos aprašas) reglamentuoja saugumo operacijų centro funkcijas ir atsakomybę, kibernetinių incidentų nustatymo, vertinimo ir valdymo tvarką, siekiant užtikrinti akcinės bendrovės „Regitra“ (toliau – AB „Regitra“) gebėjimą tinkamai ir laiku reaguoti į kibernetinius incidentus, sumažinti jų poveikį, atkurti pažeistus tinklus ir informacines sistemas.

2. Tvarkos apraše vartojamos sąvokos:

2.1. **Įvykis** – įprasto tinklų ir informacinių sistemų ar paslaugų veikimo sutrikimas ar veikla, galinti turėti reikšmės kibernetiniam saugumui.

2.2. **Kibernetinis incidentas** – įvykis, dėl kurio kyla pavojus saugumui, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.

2.3. **Kreipinys** – užklausa arba prašymas, pateiktas AB „Regitra“ IT pagalbos tarnybai atlikti tam tikrą veiksmą, kuris nėra susijęs su kibernetiniu incidentu ar įvykiu, tiesioginėmis kibernetinio saugumo grėsmėmis (pvz., prašymas sukurti naują vartotojo paskyrą, prašymas atnaujinti programinę įrangą ir kt.).

2.4. **Saugumo operacijų centras (toliau – SOC)** – AB „Regitra“ generalinio direktoriaus ar jo įgalioto asmens paskirtas (-i) darbuotojas (-ai) arba išorės paslaugų teikėjas, vykdamas šiame tvarkos apraše bei kituose teisės aktuose jam numatytas funkcijas. AB „Regitra“ generalinis direktorius užtikrina, kad Saugumo operacijų centro funkcijos nebūtų pavedamos Skaitmeninimo ir informacijų technologijų departamento arba AB „Regitra“ paslaugų teikėjo darbuotojui, atsakingam už tinkamą AB „Regitra“ tinklų ir (ar) informacinių sistemų veiklą.

2.5. **IT pagalbos tarnyba** – AB „Regitra“ įdiegta informacinių technologijų paslaugų valdymo sistema (angl. *Service Desk*). Šioje sistemoje registruojami ir valdomi kreipiniai, įvykiai, incidentai ir problemos.

2.6. Kitos Tvarkos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, jį įgyvendinančiuose teisės aktuose ir AB „Regitra“ vidaus teisės aktuose.

3. Tvarkos aprašas parengtas vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu bei Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. Vadovaujantis minėtais teisės aktais, AB „Regitra“ yra priskiriama **esminių subjektų** kategorijai.

4. Tvarkos aprašas skirtas visiems AB „Regitra“ darbuotojams ir išorinių IT paslaugų teikėjams, kurie pagal savo funkcijas yra susiję su Tvarkos apraše apibrėžtais vaidmenimis. Su aktualiomis Tvarkos aprašo nuostatomis išoriniai IT paslaugų teikėjai supažindinami paslaugų teikimo sutarčių ar kitų rašytinių susitarimų pagrindu, įtraukiant į juos atitinkamus įsipareigojimus ir reikalavimus.

II SKYRIUS

SAUGUMO OPERACIJŲ CENTRO FUNKCIJOS IR ATSAKOMYBĖS

5. AB „Regitra“ SOC funkcijos ir atsakomybės:
 - 5.1. kibernetinių incidentų nustatymas;
 - 5.2. kibernetinių incidentų vertinimas;
 - 5.3. informavimas apie kibernetinius incidentus ir informacijos teikimas Nacionaliniam kibernetinio saugumo centrui;
 - 5.4. kibernetinių incidentų valdymas;
 - 5.5. komunikavimas apie kibernetinius incidentus su suinteresuotomis šalimis;
 - 5.6. įrodymų apie kibernetinius incidentus saugojimas;
 - 5.7. kibernetinių incidentų valdymo įgytos patirties vertinimas;
 - 5.8. proceso veiksmingumo išbandymų organizavimas ir įgyvendinimas bei šių išbandymų rezultatų ataskaitos rengimas;
 - 5.9. operacinių sistemų, tinklų, registrų ir IS, techninės įrangos žurnalinių įrašų saugojimas, fiksavimas ir analizė;
 - 5.10. įeinančio ir išeinančio tinklo duomenų srauto, antivirusinės programinės įrangos, įsibrovimų aptikimo ir prevencijos sistemos ar saugasienės (ugniasienės) žurnalinių įrašų saugojimas ir analizė;
 - 5.11. tinklų, registrų ir IS, konfigūracinių ir atsarginių kopijų failų prieigos ar pakeitimo veiksmų rinkimas.

III SKYRIUS

KIBERNETINIŲ INCIDENTŲ NUSTATYMAS IR VERTINIMAS

6. AB „Regitra“ turi būti naudojamos automatinės kibernetinių incidentų aptikimo/stebėjimo sistemos, pvz., antivirusinės apsaugos sistema, įsilaužimų aptikimo sistema (angl. *Intrusion Detection System, IDS*), įsilaužimų prevencijos sistema (angl. *Intrusion Prevention System, IPS*), ugniasienė ir kt.
7. AB „Regitra“ taip pat gali būti naudojami rankiniai kibernetinių incidentų aptikimo metodai:
 - 7.1. AB „Regitra“ IT pagalbos tarnyba, kurioje darbuotojai gali registruoti įvairaus pobūdžio kibernetinius incidentus;
 - 7.2. AB „Regitra“ darbuotojo pagrįsta nuomone, kad kažkas neįprasto vyksta su kompiuterine darbo vieta (KDV) ar (ir) AB „Regitra“ IS (pvz., žymus sulėtėjimas, dingsta seni ar atsiranda nauji failai ir pan.).
8. **Kibernetinis incidentas laikomas dideliu**, kai AB „Regitra“ patiria ar gali patirti didelių paslaugų teikimo sutrikimų ir kibernetinis incidentas atitinka bent vieną iš šių kriterijų:
 - 8.1. paslaugos trikdamos visoje Lietuvos teritorijoje ir (ar) bent vienoje Europos Sąjungos arba NATO šalyje;
 - 8.2. tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;
 - 8.3. paveiktų paslaugų gavėjų (tiek AB „Regitra“ darbuotojai, tiek AB „Regitra“ klientai) ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);
 - 8.4. paveikti 1000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti AB „Regitra“ saugomi paslaugų gavėjų duomenys;
 - 8.5. paveikta 25 procentai AB „Regitra“ kompiuterizuotų darbo vietų;

8.6. AB „Regitra“ nebegali užtikrinti teisės aktuose jos veiklai nustatytų reikalavimų įgyvendinimo;

8.7. prarasta arba atskleista valstybės paslaptį sudaranti informacija;

8.8. per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa, o finansinių nuostolių dydis siekia Tvarkos aprašo 8.9 papunktyje numatytas vertes;

8.9. AB „Regitra“ patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur, arba 5 procentų AB „Regitra“ praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

8.10. kai kibernetinis incidentas paveikė kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų:

8.10.1. galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;

8.10.2. galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur;

8.10.3. sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.

IV SKYRIUS

KIBERNETINIŲ INCIDENTŲ VALDYMAS

9. Kibernetinio incidento valdymo procese (toliau – INVP) dalyvaujančios rolės, atsakingi asmenys ir jų funkcijos pateiktos Tvarkos aprašo 10 punkto lentelėje.

10. Asmenys (įskaitant juridinius): Nacionalinis kibernetinio saugumo centras (NKSC); Valstybinė duomenų apsaugos inspekcija (VDAI); AB „Regitra“ duomenų apsaugos pareigūnas (DAP).

1 lentelė. INVP dalyvaujančių asmenų rolės.

| Rolės | Atsakomybės | Asmenys ar grupės |
|------------------------------|--|---|
| Kibernetinio INVP valdytojas | <ul style="list-style-type: none">• Tobulina ir prižiūri kibernetinio INVP.• Stebi kaip efektyviai ir našiai yra vykdomas INVP.• Teikia rekomendacijas dėl kibernetinio INVP tobulinimo.• Ruošia vadovybei informaciją, susijusią su kibernetinio INVP.• Esant būtinybei, informuoja NKSC ir/ar VDAI apie incidentą. | Kibernetinio saugumo vadovas ir/ar DAP |
| Naudotojas | <ul style="list-style-type: none">• Informuoja apie kreipinius, įvykius, kibernetinius incidentus ir problemas;• Teikia informaciją, reikalingą kreipinio, įvykio, incidento ir problemos sprendimui;• Vertina kreipinio, įvykio, incidento ir problemos sprendimą. | AB „Regitra“ darbuotojai, registruojantys kreipinius IT pagalbos tarnyboje. Nuolatinę priežiūrą vykdančios turintys naudotojai. |
| Sprendėjas | <ul style="list-style-type: none">• Priima ir registruoja kreipinius, įvykius, kibernetinius incidentus ir problemas; | IT pagalbos tarnybos specialistas. |

| | | |
|----------------|--|--|
| | <ul style="list-style-type: none"> • Atlieka pirminę kreipinių, įvykių, kibernetinių incidentų ir problemų peržiūrą ir klasifikavimą; • Analizuoja ir sprendžia kreipinius, įvykius, incidentus ir problemas, arba <ul style="list-style-type: none"> • Perduoda kreipinius, įvykius, kibernetinius incidentus ir problemas kitiems sprendėjams. | |
| Trečioji šalis | <ul style="list-style-type: none"> • Analizuoja ir sprendžia kreipinius, įvykius, kibernetinius incidentus ir problemas. | Išorės tiekėjai, atsakingi už konkretaus kreipinio, problemos ir kibernetinio incidento sprendimą. |

11. AB „Regitra“ kreipiniai, įvykiai, kibernetiniai incidentai ir problemos registruojami ir valdomi IT pagalbos tarnyboje.

12. Kibernetinio incidento metu, kai paveikiami asmens duomenys, nedelsiant informuojamas DAP ir jam pateikiama visa su kibernetiniu incidentu susijusi informacija. Tokiu atveju DAP turi teisę gauti visą su kibernetiniu incidentu susijusią informaciją, kad galėtų užtikrinti tinkamą asmens duomenų saugos pažeidimo užkardymą ir pranešimą apie jį.

13. Visi kibernetinio incidento sprendime dalyvaujantys asmenys turi užtikrinti, kad kibernetinio incidento sprendimo eiga būtų fiksuojama IT pagalbos tarnyboje ir apie ją būtų informuojamas kibernetinį incidentą registravęs asmuo.

14. Sprendžiant kibernetinius incidentus, būtina atsižvelgti į Tvarkos aprašo 20 punkte nurodytus laikus (24 val., 72 val.).

15. Kibernetinių incidentų valdymo tikslas – kaip įmanoma greičiau po incidento atstatyti AB „Regitra“ teikiamas paslaugas į normalią būseną ir tuo pačiu minimizuoti neigiamą incidento įtaką teikiamoms paslaugoms ir jų kokybei.

16. Kibernetinio saugumo vadovas, siekdamas efektyvaus kibernetinio incidento suvaldymo, turi teisę iš darbuotojų gauti visą su kibernetiniu incidentu susijusią informaciją bei pasitelkti Skaitmeninio ir informacijų technologijų departamento darbuotojus būtiniais kibernetinio incidento sustabdymo ir pasekmių pašalinimo veiksmais atlikti.

V SKYRIUS INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

17. AB „Regitra“ SOC informuoja NKSC apie kibernetinius incidentus juos registruodamas KSIS posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma).

18. AB „Regitra“ SOC, dėl kibernetinio incidento neturintis galimybes apie kibernetinius incidentus informuoti per Platformą, NKSC informuoja užpildydamas formą NKSC interneto svetainėje, siųsdamas informaciją apie kibernetinį incidentą NKSC nurodytu elektroninio pašto adresu arba telefonu.

19. Jeigu AB „Regitra“ SOC funkciją vykdo išorės paslaugų teikėjas, jis privalo visą informaciją apie nustatytą kibernetinį incidentą nedelsdamas perduoti AB „Regitra“ kibernetinio saugumo vadovui, kuris užtikrina, kad pranešimas apie kibernetinį incidentą būtų pateiktas NKSC Tvarkos aprašo 17–18 punktuose nustatyta tvarka.

20. **Pranešant apie didelį kibernetinį incidentą pateikiama:**

20.1. nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento – ankstyvasis perspėjimas, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

20.2. nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento – pranešimas apie kibernetinį incidentą, kuriame pagal galimybes atnaujinama Tvarkos aprašo 20.1 papunktyje nurodyta informacija ir nurodomas didelio kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jeigu tokių yra;

20.3. NKSC prašymu – tarpinė atitinkamų atnaujintų padėties duomenų ataskaita per NKSC nurodytą pateikimo terminą;

20.4. ne vėliau kaip per vieną mėnesį nuo šios Tvarkos aprašo 19.1 punkte nurodyto pranešimo apie kibernetinį incidentą pateikimo dienos – galutinė ataskaita, kurioje pateikiama ši informacija:

20.4.1. išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

20.4.2. grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo įvykti, rūšis;

20.4.3. taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės;

20.4.4. tarpvalstybinis kibernetinio incidento poveikis, jeigu toks buvo.

21. Jeigu šios Tvarkos aprašo 20.4 papunktyje nurodytos galutinės ataskaitos pateikimo metu kibernetinis incidentas tebevyksta, pateikiama pažangos ataskaita, o galutinė ataskaita – per vieną mėnesį nuo dienos, kai kibernetinis incidentas buvo suvaldytas.

20. Teikiant Tvarkos aprašo 20.4.2 papunktyje nurodytą informaciją, parenkama viena iš išvardytų kibernetinių grėsmių ir pagrindinių incidentų priežasčių, pateiktų šios Tvarkos aprašo priede.

21. AB „Regitra“ SOC arba AB „Regitra“ kibernetinio saugumo vadovas apie didelį kibernetinį incidentą nedelsiant informuoja AB „Regitra“ generalinį direktorių.

22. AB „Regitra“ SOC arba AB „Regitra“ kibernetinio saugumo vadovas apie kitus kibernetinius incidentus, neatitinkančius šios Tvarkos aprašo 9 punkto nuostatų (toliau – **nedidelis kibernetinis incidentas**), NKSC informuoja pateikdamas:

22.1. nedelsdamas, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kibernetinį incidentą momento, pranešimą apie nedidelį kibernetinį incidentą, jame pateikdamas Tvarkos aprašo 20.2 papunktyje nurodytą informaciją;

22.2. per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos galutinę ataskaitą apie nedidelį kibernetinį incidentą, joje pateikdamas Tvarkos aprašo 20.4 papunktyje nurodytą informaciją. Galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija.

23. Jei kibernetinis incidentas tęsiasi ilgiau nei vieną mėnesį, AB „Regitra“ kas mėnesį atnauja Tvarkos aprašo 20.2 papunktyje nurodytą informaciją.

24. AB „Regitra“ SOC arba AB „Regitra“ kibernetinio saugumo vadovas teikdamas NKSC informaciją apie kibernetinio incidento pradinį vertinimą, įvardija:

24.1. kokių paslaugų sutrikimų patyrė ar gali patirti AB „Regitra“ – nurodomos paslaugos ir sutrikimų apimtys;

- 24.2. kokių finansinių nuostolių patyrė ar gali patirti AB „Regitra“ – nurodomas nuostolių dydis;
- 24.3. ar kibernetinis incidentas paveikė arba gali paveikti kitus asmenis, sukeldamas turtinę arba neturtinę žalą, – jei taip, nurodomi asmenys ir žalos dydis;
- 24.4. neteisėtų ar piktavališkų veiksmų įrodymus (jei tokių yra);
- 24.5. ar incidentas suvaldytas;
- 24.6. kitą svarbią informaciją (pavyzdžiui, kibernetinio incidento vietą, tikslų nustatymo laiką).
25. AB „Regitra“ SOC renka ir saugo įrodymus, susijusius su kibernetinio incidento nustatymu ir tyrimu. Įrodymai apima, bet neapsiriboja:
- 25.1. ekrano vaizdai (angl. *screenshots*);
- 25.2. žurnalo įrašai (angl. *logs*);
- 25.3. situaciją paaiškinantys tekstiniai komentarai;
- 25.4. interneto nuorodos;
- 25.5. tinklo srauto failai (PCAP);
- 25.6. paveiktų sistemų konfigūraciniai failai;
- 25.7. kiti failai (pvz., įvairių šalių nacionalinių CSIRT komandų ataskaitos apie tam tikrus globalius incidentus).
26. Įrodymai, susiję su kibernetiniu incidentu, turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.
27. Kibernetinio incidento valdymo metu įgytos žinios ir patirtis turi būti dokumentuojama. Turi būti vykdoma analizė, nustatant, kas incidento valdymo metu buvo padaryta tinkamai, o kas – netinkamai. Jei kibernetinis incidentas įvyko dėl saugumo spragos, spraga turi būti pašalinta pagal AB „Regitra“ generalinio direktoriaus patvirtintą AB „Regitra“ techninių reikalavimų įgyvendinimo ir pažeidžiamumų valdymo tvarką. AB „Regitra“ SOC ir (ar) kibernetinio saugumo vadovas organizuoja įgytų žinių pasidalinimą su kitais darbuotojais, susijusiais su informacinėmis technologijomis.
28. Vieną kartą per metus kibernetinių incidentų valdymas yra aptariamas pagal AB „Regitra“ generalinio direktoriaus patvirtintą Informacijos saugumo valdymo sistemos veiksmingumo stebėsenos ir vertinimo tvarką.

VI SKYRIUS BAIGIAMOSIOS NUOSTATOS

29. Už Tvarkos aprašo vykdymo kontrolę atsako AB „Regitra“ kibernetinio saugumo vadovas.
30. AB „Regitra“ turi reguliariai planuoti ir vykdyti mokymus, susijusius su kibernetinių incidentų valdymu. Šie mokymai turi būti skirti darbuotojų kompetencijų didinimui, naujų grėsmių atpažinimui ir praktiniam šio Tvarkos aprašo taikymui įvairiose situacijose.
31. AB „Regitra“ SOC privalo kaupti ir saugoti visą informaciją apie įvykusius kibernetinius incidentus, įskaitant jų priežastis, pasekmes ir taikytus sprendimus. Ši informacija turi būti tvarkoma pagal AB „Regitra“ dokumentų valdymo ir duomenų apsaugos reikalavimus.
32. AB „Regitra“ SOC surinktą informaciją apie įvykusius incidentus nuolatos analizuoja, o išmoktas pamokas pagal galimybes sistemingai pritaiko AB „Regitra“ veikloje, siekdamas sumažinti incidentų pasikartojimo tikimybę.
33. Jei tinklų ir informacinių sistemų paslaugas, susijusias su kibernetinių incidentų valdymu, teikia paslaugų teikėjai, tai už sutarties vykdymą atsakingas AB „Regitra“ darbuotojas užtikrina, kad tokie paslaugų teikėjai būtų supažindinti su Tvarkos aprašu.
34. Remdamasi analizuotais incidentais, išmoktomis pamokomis ir mokymų metu gauta informacija, AB „Regitra“ kibernetinio saugumo vadovas privalo periodiškai peržiūrėti ir atnaujinti Tvarkos aprašą, užtikrindamas jos efektyvumą ir atitikimą besikeičiančioms grėsmėms.

35. Kibernetinio saugumo vadovas turi parengti ketvirtines ataskaitas apie įvykusius incidentus ir mokymų rezultatus, kurios pristatomos atsakingiems asmenims ar vadovybei.

36. Kibernetinio saugumo vadovas turi skatinti darbuotojus aktyviai dalyvauti mokymuose, pranešti apie pastebėtas grėsmes ir teikti pasiūlymus, kaip būtų galima tobulinti kibernetinių incidentų valdymą.

KIBERNETINIŲ GRĖSMIŲ IR PAGRINDINIŲ INCIDENTŲ PRIEŽASTYS

1. Nepageidaujamų laiškų ir (ar) klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*) ir (ar) tinklų informacinės sistemos veiklos trikdymas.
2. Kenkimo programinė įranga (angl. *malicious software / code*): programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie tinklų ir informacinės sistemos, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti skaitmeninius duomenis, panaikinti ar apriboti galimybę jais naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešus skaitmeninius duomenis tokios teisės neturintiems asmenims ir kuri identifiukuota kaip:
 - 2.1. pažangi kenkimo programinė įranga (angl. *advanced persistent threat, APT*);
 - 2.2. tinklų ir informacinės sistemos duomenis šifruojantis ir naikinantis (angl. *wiper*) ar išpirkos reikalaujantis programinis kodas (angl. *ransomware*);
 - 2.3. tinklų ir informacinės sistemos dalys, aktyviai kontroliuojamos įsibrovėlių;
 - 2.4. kenkimo programinės įrangos platinimas;
3. Informacijos rinkimas (angl. *information gathering*): žvalgyba ar kita įtartina veikla, manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie tinklų ir informacinės sistemos ir (ar) kitą svarbią informaciją;
4. Mėginimas įsilaužti (angl. *intrusion attempts*). Mėginimas įsilaužti arba sutrikdyti tinklų ir informacinės sistemos veikimą išnaudojant žinomas spragas (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*), kurie gali būti skirstomi į:
 - 4.1. išnaudojama viena ar kelios nežinomos spragos (angl. *zero day*);
 - 4.2. tinklų ir informacinės sistemos žvalgyba ar kita kenkimo veikla (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita);
 - 4.3. išnaudojamos žinomos ir viešai publikuotos spragos;
5. Įsilaužimas (angl. *intrusions*). Sėkmingas įsilaužimas ir (ar) neteisėtas tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*), kuris skirstomas taip:
 - 5.1. veiksmai prieš tinklų ir informacinę sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti tinklų ir informacinės sistemos naudotojų pasitikėjimą jais;

5.2. gaunama neteisėta prieiga prie tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos;

6. Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*): veiksmai, kuriais trikdoma tinklų ir informacinės sistemos veikla, teikiamos paslaugos (angl. *DoS, DDoS*), tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos ir (ar) jos teikiamas paslaugas, kuris skirstomas taip:

6.1. teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas;

6.2. teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui;

7. Tiekimo grandinės atakos (angl. *supply chain attack*): išnaudojama trečiųjų šalių, teikiančių paslaugas tinklų ir informacinės sistemos valdytojui ir (ar) tvarkytojui, infrastruktūra, siekiant įgauti ar turėti įtaką paslaugos gavėjo tinklų ir informacinės sistemos infrastruktūrai;

8. Informacijos turinio saugumo pažeidimai (angl. *information content security*): neteisėta prieiga prie informacijos, galinčios turėti įtakos tinklų ir informacinės sistemos veiklai ir (ar) teikiamoms paslaugoms, ar jos neteisėtas keitimas;

9. Neteisėta veikla, sukčiavimas (angl. *fraud*): vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai;

10. Kitos grėsmės ar priežastys.

| DETALŪS METADUOMENYS | |
|--|--|
| Dokumento sudarytojas (-ai) | AB "REGITRA", Liepkalnio g. 97A, 02121 Vilnius, Lietuva (2026-02-14 00:42:44) |
| Dokumento pavadinimas (antraštė) | DĖL AKCINĖS BENDROVĖS „REGITRA“ KIBERNETINIŲ INCIDENTŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO |
| Dokumento rūšys | - |
| Dokumento registracijos data ir numeris | 2025-10-14 Nr. 1V-181 |
| Dokumento gavimo data ir dokumento gavimo registracijos numeris | - |
| Dokumento specifikacijos identifikavimo žymuo | ADOC-V1.0 |
| Parašo paskirtis | Pasirašymas |
| Parašą sukūrusio asmens vardas, pavardė ir pareigos | Rytis Polikauskas, Generalinis direktorius |
| Parašo sukūrimo data ir laikas | 2025-10-14 08:52:42 (GMT+03:00) |
| Parašo formatas | XAdES-A |
| Laiko žymoje nurodytas laikas | 2025-10-14 08:52:55 (GMT+03:00) |
| Informacija apie sertifikavimo paslaugos teikėją | EID-SK 2016,2.5.4.97=#160e4e545245452d3130373437303133,AS Sertifitseerimiskeskus,EE |
| Sertifikato galiojimo laikas | 2024-08-15 15:37:05–2029-08-14 23:59:59 |
| Parašo paskirtis | Registravimas |
| Parašą sukūrusio asmens vardas, pavardė ir pareigos | Regitra DVS, Sistema |
| Parašo sukūrimo data ir laikas | 2025-10-14 08:53:02 (GMT+03:00) |
| Parašo formatas | XAdES-EPES |
| Laiko žymoje nurodytas laikas | - |
| Informacija apie sertifikavimo paslaugos teikėją | RCSC IssuingCA-2,RCSC,VI Registru Centras - i.k. 124110246,LT |
| Sertifikato galiojimo laikas | 2024-06-28 14:53:25–2027-06-28 14:53:25 |
| Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti | - |
| Pagrindinio dokumento priedų skaičius | 1 |
| Pagrindinio dokumento pridedamų dokumentų skaičius | - |
| Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas | DocLogix v12.8.7.0 |
| Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data) | Tikrinant dokumentą nenustatyta jokių klaidų (2026-02-14 00:42:44) |
| Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas | 2026-02-14 00:42:44 atspausdino Jonas Piliponis |
| Paieškos nuoroda | - |
| Papildomi metaduomenys | - |