Žmogaus audinių, ląstelių ir organų
donorų bei recipientų registro veiklos
tęstinumo valdymo plano
5 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO IR NACIONALINIO KIBERNETINIO SAUGUMO CENTRO PRIE KRAŠTO APSAUGOS MINISTERIJOS INFORMAVIMO TVARKOS APRAŠAS

1. Kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos informavimo tvarkos aprašas reglamentuoja kibernetinių incidentų valdymo ir pranešimo apie kibernetinius incidentus tvarką.

2. Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – Centras) pranešama apie Žmogaus audinių, ląstelių ir organų donorų bei recipientų registre (toliau – Registre) įvykusius:

2.1. didelės reikšmės kibernetinį incidentą – ne vėliau kaip per vieną valandą nuo jo nustatymo;

2.2. vidutinės reikšmės kibernetinį incidentą – ne vėliau kaip per keturias valandas nuo jo nustatymo;

2.3. nereikšmingą kibernetinį incidentą – periodiškai kievieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

3. Pranešime apie didelės ir vidutinės reikšmės kibernetinį incidentą nurodoma:

3.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

3.2. trumpas kibernetinio incidento apibūdinimas;

3.3. tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

3.4. kibernetinio incidento kategorija;

3.5. kibernetinio incidento šalinimo tvarka (nurodoma, ar tai prioritetas, ar ne);

3.6. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

4. Pranešime apie nereikšmingą kibernetinį incidentą pateikiama apibendrinta informacija apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

5. Centrui pateikiama kibernetinio incidento tyrimo ataskaita apie:

5.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

5.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ir pasibaigia;

5.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

6. Centrui teikiant didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitą nurodoma Registro valdytojui ir (ar) tvarkytojui žinoma informacija:

6.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

6.2. Registro, kuriame nustatytas kibernetinis incidentas, tipas (informacinė sistema, elektroninių ryšių tinklas, tarnybinė stotis ir panašiai);

6.3. kibernetinio incidento veikimo trukmė;

6.4. kibernetinio incidento šaltinis;

6.5. kibernetinio incidento požymiai;

6.6. kibernetinio incidento veikimo metodas;

6.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

6.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

6.9. kibernetinio incidento būsena (aktyvus, pasyvus);

6.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

6.11. galimos kibernetinio incidento valdymo priemonės;

6.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Nacionalinio kibernetinių incidentų valdymo plano 23 punktu.

7. Įvertinus, kad negalima savarankiškai ištirti ar suvaldyti kibernetinio incidento per dvylika valandų, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo turi būti kreiptasi pagalbos į Centrą.

8. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigiusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinių sistemų veikla, atitinkanti Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2000 m. rugpjūčio 23 d. nutarimu Nr. 961 „Dėl Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro įsteigimo ir jo nuostatų patvirtinimo“, nustatytus reikalavimus.

9. Ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo turi būti informuojami ryšių ir Registro teikiamų paslaugų gavėjai, jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir Registro teikiamų paslaugų gavėjui.

10. Tais atvejais, kai Centro nurodymu toliau tiriamas ir valdomas pavojingas kibernetinis incidentas, ne rečiau kaip kas keturias valandas teikiama Centrui atnaujinta informacija apie pavojingo kibernetinio incidento valdymo būklę, kurią sudaro Nacionalinio kibernetinių incidentų valdymo plano 24 punkte nurodyta informacija.

11. Centrui perėmus tirti ir (ar) organizuoti pavojingo kibernetinio incidento valdymą, privaloma:

11.1. nuolat rinkti, apdoroti informaciją, susijusią su kibernetiniu incidentu, ir ne rečiau kaip kas keturias valandas ją teikti Centrui;

11.2. ne rečiau kaip kas keturias valandas teikti Centrui informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus, kurią sudaro Nacionalinio kibernetinių incidentų valdymo plano 24 punkte nurodyta informacija;

11.3. vykdyti Centro nurodymus, susijusius su kibernetinio incidento tyrimu ir (ar) valdymo organizavimu, ir dalyvauti kibernetinio incidento valdymo procese, taikant kibernetinio saugumo užtikrinimo priemones.

12. Gavus iš Centro, Valstybinės duomenų apsaugos inspekcijos, Lietuvos policijos (toliau kartu – KIVT institucijos), kitų juridinių asmenų ar kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, informaciją apie galimą kibernetinį incidentą Registre, turi būti imtasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti. Nenustačius kibernetinio incidento požymių, ne vėliau kaip per keturias valandas nuo pranešimo apie kibernetinį incidentą gavimo turi būti informuojamos KIVT institucijos.

13. Nacionaliniame kibernetinių incidentų valdymo plane nurodyta informacija, susijusi su kibernetiniais incidentais ir jų valdymu, turi būti perduodama per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, – kitomis saugiomis informacijos perdavimo priemonėmis.

14. Po kibernetinio incidento suvaldymo ar pasibaigimo turi būti atlikta jo analizė. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

15. Ištyrus Registre įvykusį kibernetinį incidentą, turi būti išanalizuota ir įvertinta visa informacija, susijusi su kibernetiniu incidentu, atlikti veiksmai ir panaudotos priemonės:

15.1. ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikiami kibernetinio incidento analizės rezultatai Centrui ir kibernetinio saugumo informaciniame tinkle paskelbiama susisteminta ir aktuali neįslaptinta informacija apie kibernetinio incidento nustatymą ir suvaldymą;

15.2. imamasi priemonių, kad būtų pašalintas ryšių ir Registro pažeidžiamumas;

15.3. įvertinama ryšių ir Registro rizika ir atitiktis Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

15.4. nustačius teisinio reglamentavimo spragų, pakeičiami vidiniai kibernetinio saugumo teisės aktai ir (ar) inicijuojami kitų institucijų priimtų teisės aktų pakeitimai.

16. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami konkrečiai kategorijai, nustatyti Nacionalinio kibernetinių incidentų valdymo plano priede.

_____