Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos informacinės sistemos veiklos tęstinumo valdymo plano
5 priedas

ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ VALDYMO IR PRANEŠIMO NACIONALINIAM KIBERNETINIO SAUGUMO CENTRUI TVARKA

1. Elektroninės informacijos saugos incidentų valdymo ir pranešimo Nacionaliniam kibernetinio saugumo centrui tvarka nustato Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos (toliau – VAT) elektroninės informacijos saugos incidentų valdymo ir pranešimo Nacionalinio kibernetinio saugumo centrui apie įvykusius elektroninės informacijos saugos incidentus tvarką.

2. Apie elektroninės informacijos saugos incidentus Nacionaliniam kibernetinio saugumo centrui (toliau – Centras) praneša VAT informacinės sistemos (toliau – VATIS) saugos įgaliotinis:

2.1. didelio poveikio elektroninės informacijos saugos incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;

2.2. vidutinio poveikio elektroninės informacijos saugos incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;

2.3. nereikšmingo poveikio elektroninės informacijos saugos incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

3. Centras informuojamas apie didelio ar vidutinio poveikio elektroninės informacijos saugos incidentus VATIS saugos įgaliotinio pranešimu, kuriame nurodoma:

3.1. elektroninės informacijos saugos incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Valstybinės augalininkystės tarnybos prie Žemės ūkio ministerijos informacinės sistemos veiklos tęstinumo valdymo plano (toliau – Valdymo planas) 6 priede pateiktus kriterijus;

3.2. trumpas elektroninės informacijos saugos incidento apibūdinimas;

3.3. tikslus laikas, kada elektroninės informacijos saugos incidentas įvyko ir buvo nustatytas;

3.4. elektroninės informacijos saugos incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne);

3.5. tikslus laikas, kada bus teikiama elektroninės informacijos saugos incidento tyrimo ataskaita.

4. Asmenys, kuriems Valdymo plane nėra nustatytos pareigos pranešti apie elektroninės informacijos saugos incidentus turi teisę savanoriškai pranešti Centrui apie elektroninės informacijos saugos incidentus ir taikytas elektroninės informacijos saugos ų incidentų tyrimo ar valdymo priemones šio priedo 6 punkte nurodytais kontaktais.

5. Kai būtina informuoti visuomenę siekiant išvengti elektroninės informacijos saugos incidento arba valdyti vykstantį elektroninės informacijos saugos incidentą, Centras, pasikonsultavęs su VAT, informuoja visuomenę apie pavienius elektroninės informacijos saugos incidentus arba reikalauja, kad tai padarytų VAT.

6. Apie elektroninės informacijos saugos incidentus Centras turi būti informuojamas naudojantis Kibernetinio saugumo informaciniu tinklu, nesant tokios galimybės – Centro nurodytais kontaktais (tel. 1843, el. p. cert@nksc.lt).

7. Įvykus elektroninės informacijos saugos incidentui, vadovaujamasi Valdymo planu.

8. Elektroninės informacijos saugos incidento tyrimo metu VAT Centrui teikia elektroninės informacijos saugos incidento tyrimo ataskaitas:

8.1. apie didelio poveikio elektroninės informacijos saugos incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki elektroninės informacijos saugos incidentas suvaldomas ar pasibaigia;

8.2. apie vidutinio poveikio elektroninės informacijos saugos incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki elektroninės informacijos saugos incidentas suvaldomas ar pasibaigia;

8.3. apie didelio ar vidutinio poveikio elektroninės informacijos saugos incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

9. Centrui teikiant didelio ar vidutinio poveikio elektroninės informacijos saugos incidento tyrimo ataskaitą nurodoma VAT žinoma informacija:

9.1. elektroninės informacijos saugos incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Valdymo plano 6 priede pateiktus kriterijus;

9.2. ryšių ir informacinės sistemos, kurioje nustatytas elektroninės informacijos saugos incidentas, tipas (elektroninių ryšių tinklas, VATIS, tarnybinė stotis ir panašiai);

9.3. elektroninės informacijos saugos incidento veikimo trukmė;

9.4. elektroninės informacijos saugos incidento šaltinis;

9.5. elektroninės informacijos saugos incidento požymiai;

9.6. elektroninės informacijos saugos incidento veikimo metodas;

9.7. galimos ir (ar) nustatytos elektroninės informacijos saugos incidento pasekmės;

9.8. elektroninės informacijos saugos incidento poveikio pasireiškimo (galimo išplitimo) mastas;

9.9. elektroninės informacijos saugos incidento būsena (aktyvus, pasyvus);

9.10. priemonės, kuriomis elektroninės informacijos saugos incidentas nustatytas;

9.11. galimos ir (ar) taikomos elektroninės informacijos saugos incidento valdymo priemonės;

9.12. tikslus laikas, kada bus teikiama pakartotinė elektroninės informacijos saugos incidento tyrimo ataskaita.

10. Įvertinus, kad savarankiškai ištirti ar suvaldyti elektroninės informacijos saugos incidento per dvylika valandų negalės, ne vėliau kaip per dvidešimt keturias valandas valandas nuo šių aplinkybių nustatymo VAT kreipiasi pagalbos į Centrą.

11. Didelio ar vidutinio poveikio elektroninės informacijos saugos incidentų tyrimas baigiamas ir elektroninės informacijos saugos incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta elektroninės informacijos saugos incidento poveikis VATIS ir (ar) atkuriama įprasta VATIS veikla, atitinkanti Plane nustatytus kriterijus.

12. Ne vėliau kaip per aštuonias valandas nuo elektroninės informacijos saugos incidento suvaldymo ar pasibaigimo informuojami VATIS paslaugų gavėjai, jeigu elektroninės informacijos saugos incidento poveikis jiems padarė arba gali ateityje padaryti žalos.

13. Centro nurodymu tiriant ir valdant pavojingą elektroninės informacijos saugos incidentą, ne rečiau kaip kas keturias valandas VAT teikia Centrui atnaujintą informaciją apie pavojingo

elektroninės informacijos saugos incidento valdymo būklę, kurią sudaro šio priedo 9 punkte nurodyta informacija. Centras, atsižvelgdamas į VAT teikiamą informaciją, turi teisę perimti pavojingo elektroninės informacijos saugos incidento tyrimą ir (ar) valdymo organizavimą.

14. Centrui perėmus tirti ir (ar) organizuoti pavojingo elektroninės informacijos saugos incidento valdymą,VAT:

14.1. nuolat renka, apdoroja informaciją, susijusią su elektroninės informacijos saugos incidentu, ir ne rečiau kaip kas keturias valandas ją teikia Centrui;

14.2. ne rečiau kaip kas keturias valandas teikia Centrui informaciją apie atliktus elektroninės informacijos saugos incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus, kurią sudaro šio priedo 9 punkte nurodyta informacija;

14.3. vykdo Centro nurodymus, susijusius su elektroninės informacijos saugos incidento tyrimu ir (ar) valdymo organizavimu, ir dalyvauja elektroninės informacijos saugos incidento valdymo procese, taikydami elektroninės informacijos saugos saugumo užtikrinimo priemones.

_____