



**VALSTYBINĖS KELIŲ TRANSPORTO INSPEKCIJOS
PRIE SUSISIEKIMO MINISTERIJOS
VIRŠININKAS**

ĮSAKYMAS

**DĖL ŪKIO SUBJEKTŲ, SUSIJUSIŲ SU KELIŲ TRANSPORTU, STEBĖSENOS IR
INFORMAVIMO VALSTYBĖS INFORMACINĖS SISTEMOS „VEKTRA“ DUOMENŲ
SAUGOS NUOSTATŲ PATVIRTINIMO**

2015 m. kovo 2 d. Nr. 2B-37
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7 ir 11 punktais:

1. T v i r t i n u Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ duomenų saugos nuostatus (pridedama).

2. S k i r i u Informacinių technologijų skyriaus patarėją Gintarą Serbentą Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ saugos įgaliotiniu.

3. Į p a r e i g o j u saugos įgaliotinį iki 2015 m. liepos 1 d. su Lietuvos Respublikos vidaus reikalų ministerija suderinti naujos redakcijos Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos informacinių sistemų naudotojų administravimo taisyklių ir Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos informacinių sistemų veiklos tęstinumo valdymo plano projektus.

4. P r i p a ž i s t u netekusiais galios:

4.1. Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. lapkričio 10 d. įsakymą Nr. 2B-435 „Dėl Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ duomenų saugos nuostatų patvirtinimo“;

4.2. Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos viršininko 2012 m. rugpjūčio 20 d. įsakymą Nr. 2B-333 „Dėl Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. lapkričio 10 d. įsakymo Nr. 2B-435 „Dėl Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ duomenų saugos nuostatų patvirtinimo“ pakeitimo“.

5. Šis įsakymas nustatyta tvarka skelbiamas Lietuvos Respublikos teisės aktų registre ir Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos interneto svetainėje.

Inspekcijos viršininkas

Vidmantas Žukauskas

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2015 m. sausio 27 d. raštu Nr. 1D-1027

PATVIRTINTA
Valstybinės kelių transporto inspekcijos
prie Susisiekimo ministerijos viršininko
2015 m. kovo 2 d. įsakymu Nr. 2B-37

ŪKIO SUBJEKTŲ, SUSIJUSIŲ SU KELIŲ TRANSPORTU, STEBĖSENOS IR INFORMAVIMO VALSTYBĖS INFORMACINĖS SISTEMOS „VEKTRA“ DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ (toliau – IS „Vektra“) elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir supažindinimo su saugos dokumentais principus.

2. Saugos nuostatų tikslas – sudaryti sąlygas tinkamam tarnybinių stočių, kompiuterių tinklo, kompiuterizuotų darbo vietų techninės ir programinės įrangos veikimui ir saugiam šios įrangos naudojimui, saugiu automatišku būdu tvarkyti IS „Vektra“ elektroninę informaciją ir užtikrinti elektroninės informacijos konfidencialumą, prieinamumą ir vientisumą. IS „Vektra“ elektroninės informacijos saugai užtikrinti kompleksiskai naudojamos administracinės, techninės ir programinės priemonės.

3. Saugos nuostatuose vartojama sąvoka **IS „Vektra“ naudotojas** – Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos (toliau – Inspekcija) valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

4. Kitos Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Saugos reikalavimų aprašas), ir aktuoliuose Lietuvos standartuose LST ISO/IEC 27002, LST ISO/IEC 27001 vartojamas sąvokas.

5. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

- 5.1. elektroninės informacijos konfidencialumas;
- 5.2. elektroninės informacijos vientisumas;
- 5.3. elektroninės informacijos prieinamumas;
- 5.4. IS „Vektra“ veiklos tęstinumas;
- 5.5. asmens duomenų apsauga.

6. IS „Vektra“ valdytojas ir tvarkytojas yra Inspekcija (Švitrigailos g. 42, LT-03209 Vilnius, Lietuva).

7. IS „Vektra“ valdytojo ir tvarkytojo funkcijos, teisės ir pareigos nurodytos Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ nuostatuose, patvirtintuose Valstybinės kelių transporto inspekcijos prie Susisiekimo ministerijos viršininko 2011 m. rugsėjo 16 d. įsakymu Nr. 2B-340 „Dėl Ūkio subjektų, susijusių su kelių transportu, stebėsenos ir informavimo valstybės informacinės sistemos „Vektra“ nuostatų patvirtinimo“.

8. IS „Vektra“ saugos įgaliotinio funkcijos ir atsakomybė:

8.1. teikia IS „Vektra“ valdytojui pasiūlymų dėl:

8.1.1. IS „Vektra“ administratoriaus paskyrimo ir reikalavimų administratoriaus veiklai nustatymo;

8.1.2. informacinių technologijų saugos atitikties vertinimo atlikimo Saugos reikalavimų aprašo 43 punkte nurodytoje metodikoje nustatyta tvarka;

8.1.3. saugos dokumentų priėmimo ir (ar) keitimo;

8.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS „Vektra“, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

8.3. informuoja IS „Vektra“ valdytoją ir kompetentingas institucijas apie neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią IS „Vektra“ saugą;

8.4. teikia IS „Vektra“ naudotojams ir IS „Vektra“ administratoriui privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

8.5. pagal kompetenciją kitiems IS „Vektra“ valdytojo ir IS „Vektra“ tvarkytojo valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, duoda privalomus vykdyti nurodymus ir pavedimus, būtinus saugos politikos įgyvendinimui;

8.6. organizuoja IS „Vektra“ saugos rizikos įvertinimą;

8.7. organizuoja IS „Vektra“ naudotojų ir IS „Vektra“ administratoriaus mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas;

8.8. atlieka kituose teisės aktuose jam priskirtas kitas funkcijas;

8.9. įgyvendindamas elektroninės informacijos saugą, negali atlikti IS „Vektra“ administratoriaus funkcijų ir yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.

9. IS „Vektra“ administratoriaus funkcijos ir atsakomybė:

9.1. registruoja IS „Vektra“ naudotojus IS „Vektra“ testavimo ir (ar) darbinėje aplinkoje, jiems suteikia prisijungimo vardus ir slaptažodžius (identifikavimo duomenis), teises ir leidžiamus veiksmus IS „Vektra“ (autorizavimo duomenis);

9.2. organizuoja IS „Vektra“ konfigūravimą, įskaitant saugų IS „Vektra“ įjungimą ir išjungimą;

9.3. vykdo IS „Vektra“ sudedamųjų dalių (kompiuterizuotų darbo vietų, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, bylų serverių, kompiuterių tinklo programinės ir duomenų perdavimo įrangos) veikimo koordinavimą, stebi IS „Vektra“ sudedamųjų dalių sąrankos (kaip vienos visumos) veikimą ir veikimo būklę, nustato IS „Vektra“ pažeidžiamas vietas;

9.4. ne rečiau kaip vieną kartą per metus ir (arba) po IS „Vektra“ pokyčio patikrina (peržiūri) IS „Vektra“ sąranką ir IS „Vektra“ būsenos rodiklius; tvarko IS „Vektra“ sąrankos sąrašus ir versijas;

9.5. vykdo centralizuotą IS „Vektra“ programinės įrangos diegimą ir atnaujinimą; vykdo teisės aktų ir kitų dokumentų, susijusių su IS „Vektra“ veikimu, atnaujinimą;

9.6. moko IS „Vektra“ naudotojus, juos konsultuoja;

9.7. dalyvauja valdant IS „Vektra“ pokyčius, pagal kompetenciją juos įgyvendina;

9.8. dalyvauja atkuriant IS „Vektra“ elektroninius duomenis iš duomenų atsarginių kopijų;

9.9. perkelia elektroninius duomenis į IS „Vektra“ duomenų archyvą ir tvarko elektroninių duomenų perkėlimo įrašų žurnalą;

9.10. naikina elektroninius duomenis IS „Vektra“ duomenų archyvuose ir tvarko elektroninių duomenų naikinimo įrašų žurnalą;

9.11. tvarko IS „Vektra“ eksploatacijos žurnalą;

9.12. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su IS „Vektra“ saugos užtikrinimu;

- 9.13. nuolat teikia informaciją saugos įgaliotiniui dėl IS „Vektra“ saugos užtikrinimo;
- 9.14. atlieka kitų informacinių sistemų saugą reglamentuojančių teisės aktų nustatytas funkcijas;
- 9.15. atlieka kitas IS „Vektra“ valdytojo, IS „Vektra“ saugos įgaliotinio pavestas funkcijas;
- 9.16. atsako už nepertraukiamą IS „Vektra“ veikimą.
10. Saugų IS „Vektra“ duomenų tvarkymą reglamentuoja:
- 10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
- 10.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;
- 10.3. Saugos reikalavimų aprašas;
- 10.4. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Gairių aprašas);
- 10.5. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;
- 10.6. aktualūs Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai standartai, nustatantys saugų elektroninės informacijos tvarkymą;
- 10.7. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“;
- 10.8. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Gairių aprašo 4.2.3, 4.2.4 ir 4.2.7 punktų nuostatomis, IS „Vektra“ tvarkoma elektroninė informacija priskirtina svarbios elektroninės informacijos kategorijai. Atsižvelgiant į elektroninės informacijos svarbos kategoriją ir vadovaujantis Gairių aprašo 5.2 punkto nuostata, IS „Vektra“ priskiriama antrajai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų kategorijai.
12. Vadovaujantis Saugos nuostatų 10.7 punkte nurodyto teisės akto 11.3 punkto nuostatomis, IS „Vektra“ asmens duomenų tvarkymas automatinio būdu priskiriamas trečiajam saugumo lygiui.
13. IS „Vektra“ rizikos įvertinimas (toliau – rizikos įvertinimas) atliekamas vadovaujantis šiomis nuostatomis:
- 13.1. atliekamas ne rečiau kaip kartą per vienus metus, jeigu teisės aktai nenustato kitaip;
- 13.2. neeilinis rizikos įvertinimas atliekamas padarius esminius IS „Vektra“ funkcinis pakeitimus arba kai įvyksta dideli Inspekcijos organizaciniai pokyčiai, arba atsiranda naujų informacinių technologijų saugos srities reikalavimų, arba po didelio masto saugos incidentų, kai nustatoma naujų rizikos formų;
- 13.3. atliekant rizikos įvertinimą, vadovujamasi Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Saugos nuostatų 10.6 punkte nurodytais standartais, geriausiomis praktikomis (COBIT ar kitomis) ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais;
- 13.4. taikoma detali rizikos analizės strategija, kokybiniai rizikos analizės metodai;
- 13.5. įvertinami svarbiausi saugos rizikos veiksniai: subjektyvūs netyčiniai vidiniai ir išoriniai, subjektyvūs tyčiniai vidiniai ir išoriniai, nenugalima jėga (*force majeure*).

14. Rizikos įvertinimas atliekamas vadovaujantis šiais kriterijais:

- 14.1. organizacijos valdymo ir veiklos sutrikdymas;
- 14.2. asmens duomenų saugumas;
- 14.3. teisės aktų reikalavimų laikymasis;
- 14.4. finansiniai nuostoliai;
- 14.5. tarptautiniai santykiai;
- 14.6. viešosios paslaugos;
- 14.7. reputacija.

15. Rizikos įvertinimas apima:

- 15.1. vertinamų informacinių išteklių sąrašo sudarymą ir šių informacinių išteklių savybių nustatymą (įtaka, priklausomybė, vieta, už saugų tvarkymą atsakingi asmenys ir kt.);
- 15.2. galimų grėsmių sąrašo sudarymą;
- 15.3. galimų grėsmių priskyrimą kiekvienam informaciniam ištekliui;
- 15.4. potencialaus įvykio kiekvienai informacinio išteklio ir grėsmės porai tikimybės nustatymą;
- 15.5. rizikos priimtimumo nustatymą;
- 15.6. liekamosios rizikos apskaičiavimą;
- 15.7. rekomendacijų rizikai mažinti pateikimą.

16. Rizikos įvertinimą atlieka saugos įgaliotinis arba sutartiniais pagrindais samdomi

trejieji asmenys.

17. Pagrindinės IS „Vektra“ saugos rizikos mažinimo priemonės pateikiamos IS „Vektra“ rizikos įvertinimo ataskaitoje, kurią iki IS „Vektra“ valdytojo nurodytos datos rengia IS „Vektra“ saugos įgaliotinis. IS „Vektra“ saugos įgaliotinis dalyvauja rengiant IS „Vektra“ rizikos įvertinimo ataskaitą, jei rizikos įvertinimą atlieka trečioji šalis.

18. IS „Vektra“ valdytojas, atsižvelgęs į rizikos įvertinimo ataskaitą, jei prireikia, tvirtina IS „Vektra“ saugos rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų priemonių poreikis saugos rizikos valdymo priemonėms įgyvendinti.

19. Už IS „Vektra“ saugos rizikos vertinimo organizavimą ir atlikimą atsakingas IS „Vektra“ saugos įgaliotinis.

20. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, IS „Vektra“ informacinių technologijų saugos atitikties vertinimas atliekamas ne rečiau kaip kartą per vienus metus, jei teisės aktai nenustato kitaip:

20.1. IS „Vektra“ informacinių technologijų saugos atitikties vertinimą atlieka IS „Vektra“ valdytojo sudaryta darbo grupė; prireikus IS „Vektra“ informacinių technologijų saugos atitikties vertinimą pagal sutartį gali atlikti tretieji asmenys;

20.2. atliekant IS „Vektra“ informacinių technologijų saugos atitikties vertinimą tikrinama, kaip IS „Vektra“ veikimas atitinka Saugos nuostatų, kitų elektroninės informacijos saugą reglamentuojančių teisės aktų ir dokumentų reikalavimus;

20.3. tikrinamas įdiegtos antivirusinės programos ir apsaugos nuo nepageidaujamos programinės įrangos filtravimo sistemos naudojimas, centralizuotas jų valdymas ir atnaujinimas;

20.4. tikrinamas programinės įrangos, programinės įrangos sertifikatų ir licencijų naudojimas;

20.5. tikrinamas IS „Vektra“ naudotojų kompiuterizuotų darbo vietų (ne mažiau kaip 10 procentų) naudojimas;

20.6. tikrinamas tarnybinių stočių ir komunikacinės įrangos naudojimas;

20.7. tikrinamas duomenų bazių atsarginių kopijų ir archyvų darymas;

20.8. tikrinamas pasirengimas atkurti IS „Vektra“ veiklą duomenų saugos incidento atveju;

20.9. tikrinama, kaip IS „Vektra“ naudotojams suteiktos teisės IS „Vektra“ atitinka naudotojų atliekamas funkcijas.

21. Įvertinusi IS „Vektra“ informacinių technologijų saugos atitiktį, darbo grupė parengia informacinių technologijų saugos atitikties vertinimo ataskaitą ir, jei reikia, pastebėtų trūkumų šalinimo planą, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus IS „Vektra“ valdytojas.

22. Elektroninės informacijos saugos priemonėms parinkti taikomi šie principai:

22.1. parenkamos priemonės, kurios leidžia užtikrinti patalpų saugą;

22.2. parenkamos priemonės, kurios leidžia užtikrinti kompiuterinės ir programinės įrangos veikimo saugą;

22.3. parenkamos priemonės, kurios leidžia užtikrinti kompiuterių tinklų veikimo saugą;

22.4. parenkamos priemonės, kurios leidžia užtikrinti IS „Vektra“ naudotojų mokymą ir informavimą apie elektroninių duomenų tvarkymo saugą.

23. Elektroninės informacijos saugos priemonės turi garantuoti:

23.1. elektroninių duomenų saugą jų tvarkymo ir (ar) perdavimo ryšio kanalais metu;

23.2. elektroninių duomenų saugą nuo nesankcionuoto ar neteisėto tvarkymo, perdavimo ryšio kanalais ir (ar) kitokio pažeidimo.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Programinės įrangos, skirtos IS „Vektra“ apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

24.1. tarnybinėse stotyse ir kompiuterizuotose darbo vietose privalo būti įdiegta centralizuotai valdoma apsauga nuo kenksmingos programinės įrangos;

24.2. tarnybinės stotys ir kompiuterizuotos darbo vietos turi būti apsaugotos nuo brukalų ir nepageidaujamo turinio laiškų;

24.3. kompiuterizuotose darbo vietose turi būti įdiegtos priemonės, ribojančios atminties raktų (USB) ir kitų išorinių laikmenų naudojimą;

24.4. apsaugai nuo kenksmingos programinės įrangos naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas;

24.5. apsaugos nuo kenksmingos programinės įrangos sistema privalo automatiškai elektroniniu paštu informuoti atsakingus darbuotojus apie kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos nuo kenksmingos programinės įrangos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

25. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

25.1. IS „Vektra“ veikti naudojama tik legali programinė įranga;

25.2. IS „Vektra“ naudotojų kompiuterizuotose darbo vietose draudžiama naudoti programinę įrangą, nesusijusią su tiesiogine jų veikla ir funkcijomis;

25.3. programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų;

25.4. programinę įrangą diegia, šalina ir konfigūruoja tik atitinkami administratoriai;

25.5. kompiuterizuotos darbo vietos, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami.

26. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliojimų serverių (angl. *proxy*) ir kita) programinės įrangos naudojimo nuostatos:

26.1. IS „Vektra“ naudojami kompiuterių tinklai nuo kitų kompiuterių tinklų privalo būti atskirti tinklo užkardomis;

26.2. IS „Vektra“ naudojamame kompiuterių tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos;

26.3. viešuoju kompiuterių tinklu gaunamas duomenų srautas privalo būti filtruojamas;

26.4. turi būti naudojama programinė įranga, leidžianti atlikti IS „Vektra“ naudojamų kompiuterių tinklų monitoringą ir užtikrinanti šių tinklų saugos prevencines priemones;

26.5. už saugų Inspekcijos teritorinio kompiuterių tinklo veikimą atsako šio tinklo administratorius.

27. Kompiuterizuotų darbo vietų, kuriose veikia IS „Vektra“, saugaus naudojimo nuostatos ir reikalavimai:

27.1. kompiuterizuota darbo vieta privalo būti naudojama tik su IS „Vektra“ ir su kitomis Inspekcijoje naudojamomis informacinėmis sistemomis pagal naudotojo kompetenciją susijusioms funkcijoms vykdyti;

27.2. stacionariuosiuose ir nešiojamuosiuose kompiuteriuose IS „Vektra“ įjungimo metu turi būti naudojamas IS „Vektra“ naudotojo identifikavimas. Kompiuterizuotų darbo vietų įjungimo metu turi būti naudojamas įjungimo (angl. *power on*) slaptažodis;

27.3. IS „Vektra“ naudotojo, atliekančio kontrolę keliuose ar vežėjų įmonėse, nešiojamajam kompiuteriui prieiga prie IS „Vektra“ suteikiama specialiu tuneliu (VPN), praleidžiančiu tik tam tikru būdu šifruotus duomenų paketus; nešiojamieji kompiuteriai prieigai prie IS „Vektra“ parengiami IS „Vektra“ valdytojo nurodymu.

28. Saugaus elektroninės informacijos teikimo ir gavimo metodai:

28.1. duomenys IS „Vektra“ perduodami naudojant TCP/IP protokolą realiu laiku („On-line“ režimu);

28.2. iš duomenų gavėjų elektroniniai duomenys gaunami pagal asmens duomenų teikimo sutartyse ar duomenų teikimo sutartyse numatytas elektroninių duomenų perdavimo technologijas, jų šifravimo mechanizmus, specifikacijas ir kitas sąlygas; duomenų gavėjų prieigą prie IS „Vektra“ kontroliuoja Inspekcijos teritorinio kompiuterių tinklo užkarda.

29. Nustatomi šie pagrindiniai atsarginių elektroninių duomenų kopijų darymo ir atkūrimo reikalavimai:

29.1. turi būti sudaromi IS „Vektra“ elektroninių duomenų, kurių kopijos daromos, sąrašai;

29.2. elektroninių duomenų atsarginės kopijos ir archyvai turi būti daromi ir duomenys iš jų atkuriami vadovaujantis IS „Vektra“ valdytojo patvirtinta tvarka;

29.3. elektroninių duomenų atsarginės kopijos turi būti daromos automatiškai kiekvieną dieną nuo tarnybinių stočių patalpų nutolusiose patalpose esančiame elektroninių duomenų kopijų darymo įrenginyje;

29.4. elektroniniai duomenys į duomenų archyvą perkeliami, pasibaigus duomenų saugojimo IS „Vektra“ laikui;

29.5. elektroninių duomenų atsarginėms kopijoms daryti turi būti naudojama speciali programinė įranga;

29.6. už elektroninių duomenų atsarginių kopijų ir elektroninių duomenų archyvų darymą yra atsakingi tarnybinių stočių ir IS „Vektra“ administratoriai pagal kompetenciją; už elektroninių duomenų naikinimą – IS „Vektra“ duomenų valdymo įgaliotinis ir IS „Vektra“ administratorius.

IV. REIKALAVIMAI PERSONALUI

30. IS „Vektra“ naudotojai turi turėti ne prastesnius darbo su kompiuteriu įgūdžius, nei numatyta jų pareigybių aprašymuose.

31. Saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų panaudojimo ypatumus, žinoti elektroninės informacijos saugos principus bei saugos užtikrinimo metodus, kitus su informacinių sistemų saugiu veikimu susijusius teisės aktus, turėti darbo organizavimo gabumų.

32. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

33. IS „Vektra“ administratorius privalo gerai žinoti kompiuterizuotos veiklos procesus, elektroninės informacijos saugos užtikrinimo metodus ir principus, būti susipažinęs su naudojamų duomenų bazių organizavimo principais, gebėti jas administruoti, žinoti tarnybinių stočių veikimo principus.

34. IS „Vektra“ naudotojai ir IS „Vektra“ administratorius turi būti susipažinęs su Saugos nuostatais bei kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais (toliau – saugos dokumentai) ir sutikę laikytis jų reikalavimų.

35. IS „Vektra“ naudotojai turi būti išmokyti dirbti su IS „Vektra“. Mokymai gali būti centralizuoti, kai juos organizuoja ir veda IS „Vektra“ administratorius, arba individualūs, kai juos organizuoja ir veda IS „Vektra“ tvarkytojo paskirtas asmuo arba IS „Vektra“ administratorius.

36. Elektroninės informacijos saugos mokymai IS „Vektra“ naudotojams ir IS „Vektra“ administratoriui turi būti rengiami ne rečiau kaip vieną kartą per metus.

V. IS „VEKTRA“ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. IS „Vektra“ naudotojų ir IS „Vektra“ administratoriaus supažindinimą su saugos dokumentais atlieka saugos įgaliotinis:

37.1. rašytine forma (per dokumentų valdymo sistemą, raštu, elektroniniu paštu ar kitomis rašytinėmis priemonėmis) supažindina IS „Vektra“ naudotojus ir IS „Vektra“ administratorių su saugos dokumentais, jų pakeitimais ir (ar) negaliojimu;

37.2. supažindinimą su saugos dokumentais atlieka per 3 darbo dienas nuo saugos dokumento įsigaliojimo datos;

37.3. IS „Vektra“ naudotojų ir IS „Vektra“ administratoriaus susipažinimo su saugos dokumentais faktas registruojamas Inspekcijos informacinių sistemų naudotojų susipažinimo su saugos dokumentais žurnale, kuris tvarkomas vadovaujantis Inspekcijos viršininko patvirtintu dokumentacijos planu;

37.4. IS „Vektra“ naudotojų ir IS „Vektra“ administratoriaus sutikimą laikytis saugos dokumentų reikalavimų atitinka jų pasirašymas Inspekcijos informacinių sistemų naudotojų susipažinimo su saugos dokumentais žurnale;

37.5. po susipažinimo su saugos dokumentais fakto užregistravimo Inspekcijos informacinių sistemų naudotojų susipažinimo su saugos dokumentais žurnale datos telefonu, elektroniniu paštu ar susitikimo metu gali patikrinti saugos dokumentų supratimo žinias; gali organizuoti saugos dokumentų žinių patikrinimo egzaminą.

38. Pakartotinai IS „Vektra“ naudotojai ir IS „Vektra“ administratorius su saugos dokumentais supažindinami iš esmės pasikeitus saugos dokumentams ir (arba) padažnėjus elektroninės informacijos saugos incidentų.

39. IS „Vektra“ naudotojai ir IS „Vektra“ administratorius nuolat turi būti informuojami apie saugos problemas (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

VI. BAIGIAMOSIOS NUOSTATOS

40. Saugos įgaliotinis, IS „Vektra“ tvarkytojas, IS „Vektra“ naudotojai, IS „Vektra“ administratorius, pažeidę Saugos nuostatų ar kitų saugos politiką reglamentuojančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.
