MYKOLO ROMERIO UNIVERSITETO
VALSTYBINIO VALDYMO FAKULTETO
TEISINĖS INFORMATIKOS KATEDRA

REGINA KRANAUSKIENĖ
ELEKTRONINĖS VALDŽIOS ADMINISTRAVIMAS
Studijų knygelės Nr. 036611

INFORMACIJOS SAUGUMO VALDYMAS X ORGANIZACIJOJE

Magistro baigiamasis darbas

Darbo vadovas prof. Rimantas Petrauskas
Konsultantas Žydrūnas Paškauskas

Vilnius
2004

TURINYS

ĮVADAS

Siekdama tapti Europos Sąjungos nare ir įsilieti į išsivysčiusių Europos šalių bendriją, Lietuvos Respublikos Vyriausybė parengė Lietuvos informacinės visuomenės plėtros strateginį planą[1], suderintą su Europos Sąjungos veiklos planu eEurope 2005: „Informacinė visuomenė visiems“ ir šalims kandidatėms parengtu informacinės plėtros veiksmų planu *eEurope+*. Šiame plane numatyta užtikrinti informacinių technologijų saugumą valstybės institucijose ir įstaigose.

Atsižvelgdama į jai iškeltus uždavinius, tais pačiais metais Vyriausybė patvirtino Informacijos technologijų saugos valstybinę strategiją[2], kurios tikslas, vadovaujantis tarptautiniais standartais, Ekonominio bendradarbiavimo ir plėtros organizacijos, NATO ir Europos Tarybos direktyvomis ir rekomendacijomis, Europolo ir Šengeno informacinių sistemų, prie kurių stengsis prisijungti ir Lietuva, reikalavimais, teisiškai reglamentuoti bendruosius duomenų saugos reikalavimus.

Įmonės ir valstybinės įstaigos tapo potencialiais įvairiausių atakų rengėjų taikiniais, kurių motyvacija labai skirtinga – nuo asmeninės nuoskaudos iki kriminalinės veiklos.

Daugybė tyčinių ir atsitiktinių saugos pažeidimų kyla iš vidaus – tat prielaida, kad pakankamą saugą garantuoja stipri perimetro kontrolė, nepasiteisino.

Informacijos ir procesų, pagrįstų informacinių technologijų naudojimu, konfidencialumas, autentiškumas, vientisumas, privalomumas ir patikimumas daugumos didelių organizacijų veiklai yra kritiniai veiksniai – daugeliu atvejų tai reglamentuoja teisiniai ir administraciniai reikalavimai.

„Informacijos saugumo užtikrinimas:

- turėtų būti suprantamas ne kaip galutinis rezultatas, o greičiau kaip kontroliuojamas ir valdomas **procesas**;
- yra svarbi ir neatskiriama vidinių organizacijos kontrolės procesų dalis, jis apima visą organizaciją ir turi būti nagrinėjamas visos jos **veiklos** kontekste;
- prasideda nuo jo svarbos suvokimo ir žinojimo. Bendras informacijos saugumo klausimų suvokimo organizacijoje lygis tiesiogiai priklauso nuo **organizacijos vadovybės** suvokimo lygio.“

[1] Lietuvos Respublikos Vyriausybės 2001 m. rugpjūčio 10 d. nutarimas Nr. 984 “Dėl Lietuvos informacinės visuomenės plėtros strateginio plano patvirtinimo” // Valstybės žinios. 2001, Nr. 71-2534.
[2] Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 “Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo” // Valstybės žinios. 2001, Nr. 110-4006.

Taip teigia Informacinių sistemų audito ir valdymo asociacija (ISACA) – tarptautinė informacinių technologijų specialistų asociacija, veikianti daugiau nei 100 šalių ir vienijanti virš 28 tūkstančių narių.[3]

Išnagrinėjus Lietuvos Respublikoje galiojančius teisės aktus, kuriais nustatyti duomenų saugos informacinėse sistemose organizavimo ir organizacinių priemonių reikalavimai valstybinėms institucijoms, galima konstatuoti, kad teisinė bazė šiuo klausimu dar nepakankama.

Lietuvos Respublikoje galiojantys teisės aktai reikalauja užtikrinti duomenų saugą ir įpareigoja prisitaikyti prie jau nustatytų ar naujai priimamų, tačiau daugeliu atvejų tarpusavyje nesuderintų, nuostatų.

Teisės akto, kuris vieningai būtų taikomas visiems be išimties duomenims bei apibrėžtų ir aiškiai susietų visai šiai duomenų visumai turimus taikyti duomenų saugos informacinėse sistemose organizacinių priemonių principus ar standartus, procedūras, arba pateiktų atitinkamas nuorodas, nėra.

Organizacijoje apsiribojant ir laikantis vien tik teisės aktų reikalavimų jos veiklos saugaus ir patikimo funkcionavimo užtikrinimo srityse nebus pasiektas efektyvus duomenų saugos ir patikimumo organizavimas ir valdymas.

Komercinės informacinių technologijų paslaugas teikiančios įmonės, siūlydamos organizacijoms saugos užtikrinimo dokumentus (IT saugos politiką, saugos architektūrą ir t.t.), naudojasi daugiausia tarptautiniais standartais (pvz., ISO 17799[4]), kurie jau patvirtinti ir Lietuvos standartais. Tie dokumentai labai dažnai būna mažai nutolę nuo pažodinio standartų vertimo į lietuvių kalbą, ir visai netinkami tvirtinti organizacijos vadovo įsakymu.

Viešojo administravimo institucijai iškyla problema, kaip pasinaudoti komercinių įmonių parengtais projektais, pripažintais standartais, ir, nenusižengus galiojantiems teisės aktams, sukurti organizacijoje saugumo valdymo struktūrą ir patvirtinti informacijos saugumo politiką arba nuostatus, kuriais galėtų vadovautis organizacijos vadovybė ir darbuotojai, užtikrindami savo veiklos tolydumą ir nenutrūkstamumą.

Autorės magistro baigiamojo darbo tikslas – išnagrinėti Lietuvos ir Europos Sąjungos teisės aktų keliamus reikalavimus informacijos saugumo užtikrinimui viešojo administravimo institucijoje, pateikti savo siūlymus, kokia turėtų būti organizacijos informacijos saugumo valdymo struktūra, strategija ir politika, jų įgyvendinimo administracinės, organizacinės ir technologinės priemonės.

Darbas yra aktualus, nes didėjant informacijos išteklių reikšmei kiekvienos organizacijos išteklių struktūroje, kylant jų saugumo užtikrinimo vis didesniam poreikiui ir teisės aktų

[3]Informacinių sistemų audito ir valdymo asociacija // http://www.isaca.lt/lt/naujienos/?news_id=News192.
[4]LST ISO?IEC 17799:2000 „Informacijos technologija. Praktiniai informacijos valdymo principai“.

reikalavimams, informacijos saugumo valdymui konkrečioje organizacijoje skiriamas per mažas dėmesys, metodinė medžiaga yra išbarstyta ir nenuosekli, specialistai yra labai siauros kvalifikacijos, dažniausiai techninės, o vadybininkai mažai susipažinę su informacinėmis technologijomis.

Darbe autorė rėmėsi Lietuvos ir ES teisės aktais, tarptautiniais ir Lietuvos standartais, užsienio ir šalies mokslininkų pranešimais, straipsniais, konferencijų medžiaga. Buvo naudojami dokumentų analizės, lyginimo, modeliavimo, sisteminės analizės metodai.

Baigiamojo darbo uždaviniai:

- išnagrinėti Lietuvos ir ES teisės aktus, reglamentuojančius informacijos saugumo užtikrinimo reikalavimus;
- įvardyti, kas sudaro organizacijos informacijos išteklius, informacijos saugumo lygius;
- pateikti organizacijos saugumo valdymo struktūros modelį;
- išsamiai išnagrinėti ir pasiūlyti informacijos saugumo užtikrinimo priemones.

Pirmoje darbo dalyje nagrinėjama informacija, informacijos išteklių ir saugumo samprata, antroje dalyje analizuojami teisinio reguliavimo ir reglamentavimo informacijos turinio apsaugos ir saugumo klausimai, trečioje dalyje siūlomas organizacijos saugumo valdymo struktūros modelis, ketvirtoje ir penktoje dalyje nagrinėjami informacijos saugumo planavimo ir valdymo klausimai.

I. INFORMACIJA, INFORMACIJOS IŠTEKLIŲ IR SAUGUMO SAMPRATA

1. Informacijos samprata, klasifikavimo kriterijai

Prieš imantis analizuoti informacijos saugumo klausimus, būtina išsiaiškinti, kas yra informacija apskritai ir kas yra ta informacija, kurią kiekviena organizacija pasiryžusi saugoti. Autorei teko susipažinti su dideliu kiekiu mokslinės, metodinės ir dalykinės literatūros, ir ji laiko reikalinga pažymėti, kad informacijos apibrėžimų yra daug, dažnai jos sąvoką lemia mokslo šaka. Tiksliųjų mokslų atstovai ir technologai informacijos neskiria nuo duomenų ir šia sąvoka remiasi nagrinėdami informacijos (duomenų) kodavimą, perdavimą ir priėmimą. Sociologai, psichologai informaciją supranta kaip bendravimo rezultatą ir domisi jos pažinimu, interpretavimu, dažnai skirtingai suvokdami tos pačios informacijos prasmę. Politologai informaciją sieja su valdžia ir nagrinėja jos paskirstymą arba neteisėtą nuslėpimą. Verslo vadybos specialistai sutinka, kad informacija gali būti prekė, bet keista prekė – pardavus ją, savininkas jos nepraranda, bet ji gali būti prarasta už dyka ir žaibiškai.

Informacijos ir komunikacijos mokslų atstovai informacijos sąvoką dažnai nagrinėja santykyje „duomenys – informacija – žinios“.

Duomenys – tai ženklai, simboliai, neapdorota, nesutvarkyta ir neįvertinta informacija. Informacija – tai, kas suvokiama, vartojama ir tampa žiniomis. Negalima nustatyti tikros ribos, kada duomenys virsta informacija, o ši – žiniomis ir, atvirkščiai, žinios virsta informacija. Informacijos terminų standartas ISO 2382 informacijos sąvoką apibrėžia taip: informacija vadinamos žinios apie faktus, įvykius, daiktus, procesus, idėjas, sąvokas ir kitus objektus, kurios tam tikrame kontekste turi kokią nors prasmę[5].

Lietuvių kalboje duomenys kildinami iš žodžio „duoti“[6], t.y. kas yra duota, kuo galima remtis. Informacija – žinios arba reikšmė, kurią supranta žmonės, sužinoję duomenis.

Tarptautinių žodžių žodynas žodį „informacija“ aiškina taip: 1. mokslinės, visuomeninės, politinės, techninės žinios, perduodamos vienų asmenų kitiems žodžiu, raštu arba žiniasklaidos priemonėmis (per spaudą, radiją, televiziją, kiną, kompiuterių tinklus); 2. duomenų, žinių kokiu nors klausimu visuma; 3. įstaigos, organizacijos skyrius, teikiantis žinias, nurodantis, paaiškinantis[7].

Šiame darbe autorė, kaip tiksliųjų mokslų atstovė, irgi nenorėtų informacijos griežtai atskirti nuo duomenų. Ar duomenų bazė, išeinant iš jos pavadinimo, yra tik duomenų sankaupa? Autorė mano, kad ne. Vienas, atskirai paimtas duomenų bazės laukas, – tai tikrai duomenys, kurie individui nieko nesako, bet visas duomenų bazės įrašas, ar net keli kartu paimti laukai gali pateikti išsamią informaciją apie konkretų asmenį, jei nagrinėjama duomenų bazė yra, pvz., organizacijos personalo registras.

Toliau šiame darbe autorė laikys, kad duomenys yra informacijos dalis.

2. Informacijos išteklių samprata ir pagrindinės koncepcijos

Šiuolaikinėje informacinėje visuomenėje informacija yra tokie patys ištekliai (turtas, angl.*asset*), kaip ir finansai, žmogiškieji ištekliai ar žaliavos ir inventorius (fiziniai ištekliai). Informacija, kalbant vadybiniais terminais, turi vertę (produktyvumas, valdymo procesų palaikymas ir konkurencinė vertė), kainuoja pinigus (kaupti, saugoti, apdoroti ir skleisti), galima apibrėžti kokybę (savalaikiškumas, tikslumas, pateikimo forma), ją galima kontroliuoti.

Negana to, kad pačią informaciją, kaip turtą, būtina saugoti, reikia saugoti ir turtą, susijusį su ja. Tokį turtą galima būtų skirstyti į[8]:

[5] E. Janiūnienė. Biblioteka – žinių institucija // Informacijos mokslai. 2001, Nr. 17.
[6] Dabartinės lietuvių kalbos žodynas. –Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2000.
[7] Tarptautinių žodžių žodynas. –Vilnius: Alma littera, 2003.

[8] LST ISO?IEC 17799:2000 „Informacijos technologija. Praktiniai informacijos valdymo principai“.

- pačią informaciją (duomenų bazės ir duomenų rinkmenos, IT sistemos dokumentai, vartotojo instrukcijos ir procedūrų aprašymai, mokymo medžiaga, priežiūros ir palaikymo procedūros, veiklos tolydumo planai, apsaugos priemonių aprašymai, archyvo informacija);
- programinę įrangą (taikomosios programos, IT sistemų valdymo ir vystymo programos, kitų paslaugų programos);
- fizinę įrangą: kompiuterio įranga (procesoriai, monitoriai, nešiojamieji kompiuteriai, modemai), ryšių įranga (trasuotuvai, automatiniai linijų komutatoriai, fakso aparatai, autoatsakikliai, kabeliai), magnetinės duomenų laikmenos (juostos ir diskai), kita techninė įranga (maitinimo šaltiniai, oro kondicionavimo įtaisai), specialūs baldai, patalpos;
- paslaugas (skaičiavimo ir ryšių paslaugos, šildymas, apšvietimas, elektros tiekimas ir kt.).

Kiekvienoje organizacijoje būtina turėti tokio turto sąrašus, šiam turtui priskiriant reikšmes pagal turto svarbą organizacijai. Geriausia tai išreikšti saugumo terminais: potencialiais žalingais poveikiais, atsirandančiais dėl informacijos ar kito IT sistemos turto atskleidimo, modifikavimo, neprieinamumo ar sunaikinimo. Turto nustatymas ir įvertinimas yra svarbus rizikų nustatymo faktorius.

Pradinius duomenis turtui įvertinti turi pateikti turto savininkai ir vartotojai. Turtui priskirta reikšmė turi atspindėti turto įsigijimo ir priežiūros išlaidas bei potencialiai žalingą poveikį organizacijos veiklai, atsirandantį praradus slaptumą, vientisumą, prieinamumą, atsakingumą, tapatumą ir patikimumą. Nėra lengva nustatyti turto finansinę vertę. Įvertinimo skalė gali būti: nereikšmingas – mažai reikšmingas – vidutiniškai reikšmingas – gana reikšmingas – labai reikšmingas.

3. Informacijos apsaugos esmė ir savybių analizė

Daugelis šalių perėjo nemažai žingsnių link informacijos ir duomenų perdavimo apsaugos: (1) dėmesio problemai skyrimas ir visapusiškas nagrinėjimas; (2) valstybės vadovo paskirtas vadovavimas šiai sričiai; (3) nacionalinio projekto derinimas su visais sąveikaujančiais sektoriais; (4) įstatymų, sustiprinančių vyriausybinius įsipareigojimus ir valdymą, leidyba[9].

Teisės aktai, ES ir Lietuvoje reglamentuojantys informacijos apsaugą ir kontrolę, pateikti kitame skyriuje. Kiekviena organizacija privalo jų laikytis ir tinkamai saugoti informaciją. Tam būtinas organizacijoje turimos informacijos klasifikavimas pagal slaptumą ir prieinamumą.

[9] World Public Sector Report 2003: E-government at the Crossroads. United Nations, New York, 2003, P.110-122.

Vadovaudamasi Valstybės ir tarnybos paslapčių įstatymu[10], Visuomenės informavimo įstatymu[11], Lietuvos Respublikos Vyriausybės nutarimu patvirtinta Lietuvos Respublikos įslaptintos informacijos apsaugos tvarka[12], autorė siūlo organizacijoje turimą informaciją suskirstyti į keturias kategorijas:

- I kategorija – valstybės paslaptį sudaranti informacija. Valstybės paslaptis – politiniai, ekonominiai, kariniai, teisėtvarkos, mokslo ir technikos duomenys, kurių praradimas ar neteisėtas atskleidimas gali pažeisti Lietuvos Respublikos suverenitetą, gynybinę ar ekonominę galią, pakenkti Lietuvos Respublikos konstitucinei santvarkai, politiniams interesams, sukelti pavojų žmogaus gyvybei ir sveikatai, jo konstitucinėms teisėms. Ši informacija žymima slaptumo žymomis „Visiškai slaptai“, „Slaptai“, „Konfidencialiai“, ji naudojama, tvarkoma, kontroliuojama ir saugoma, vadovaujantis Valstybės ir tarnybos paslapčių įstatymu, Lietuvos Respublikos Vyriausybės nutarimu patvirtinta Lietuvos Respublikos įslaptintos informacijos apsaugos tvarka, atitinkamais organizacijos vadovų išleistais norminiais teisės aktais;
- II kategorija – tarnybos paslaptį sudaranti informacija. Tarnybos paslaptis – politiniai, ekonominiai, kariniai, teisėtvarkos, mokslo ir technikos duomenys, kurių platinimas ribojamas dėl valstybės bei jos institucijų interesų, taip pat siekiant apsaugoti žmogaus konstitucines teises. Ši informacija žymima slaptumo žyma „Riboto naudojimo“. Ji naudojama, tvarkoma, kontroliuojama ir saugoma, vadovaujantis Valstybės ir tarnybos paslapčių įstatymu, Lietuvos Respublikos Vyriausybės nutarimu patvirtinta Lietuvos Respublikos įslaptintos informacijos apsaugos tvarka, atitinkamais organizacijos vadovų išleistais norminiais teisės aktais;
- III kategorija – viešai neskelbtina ir neteiktina informacija. Tai informacija, nesudaranti valstybės ir tarnybos paslapties, tačiau jos skelbimas ribojamas teisės aktų nustatyta tvarka. Į šią informacijos kategoriją pakliūna ir organizacijos personalo asmens duomenys, ir komercinė ūkio subjektų informacija, prieinama organizacijai, pačios organizacijos detalūs finansų ir apskaitos duomenys, vidaus audito tarnybos darbo dokumentai ir pan. Su šia informacija darbuotojai gali susipažinti ir naudotis tarnyboje jų pareigybių aprašymuose nurodytoms funkcijoms atlikti;
- IV kategorija – viešoji informacija. Tai visa informacija, kuri nepriklauso kitoms trims kategorijoms, išvardintoms anksčiau. Ši informacija gali būti skelbiama internete bei kitomis *multimedia* priemonėmis.

[10] Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios. 1999, Nr. 105-3019.
[11] Lietuvos Respublikos visuomenės informavimo įstatymas // Valstybės žinios. 1996, Nr. 71-1706.
[12] Lietuvos Respublikos Vyriausybės 2000 m. balandžio 27 d. nutarimas Nr. 462 “Dėl Lietuvos Respublikos įslaptintos informacijos apsaugos tvarkos patvirtinimo” // Riboto naudojimo

Vykdydamas Informacijos technologijų saugos valstybinės strategijos įgyvendinimo planą[13], 2003 m. sausio 27 d. Lietuvos Respublikos vidaus reikalų ministras savo įsakymu Nr. 1V-33 patvirtino Informacijos klasifikavimo pagal duomenų grupes rekomendacijas[14]. Šios rekomendacijos ne klasifikuoja informaciją, bet nustato kategorijas informacinėms sistemoms pagal duomenų grupių savybių įtaką konkrečiai informacinei sistemai. Čia apibrėžiamos trys duomenų savybės: vientisumas, konfidencialumas ir prieinamumas, o duomenų grupėmis laikomi logiškai tarpusavyje susiję informacinės sistemos duomenys. Trys pirmosios kategorijos suteikiamos informacinėms sistemoms, kurių duomenis pagal viešumo apribojimą galima priskirti pirmoms trims autorės išskirtoms informacijos kategorijoms. Ketvirtoji kategorija pagal šias rekomendacijas priskirtina ne pačiai informacinei sistemai, bet atskiriems informacinės sistemos duomenims, neatitinkantiems pirmųjų trijų kategorijų. Tokiu būdu minėtose rekomendacijose klasifikavimo objektai skiriasi ne tik nuo nurodytų pavadinime, bet ir tarpusavyje. Autorės nuomone, minėtas rekomendacijas reikėtų patikslinti.

II. TEISINIO REGULIAVIMO IR REGLAMENTAVIMO INFORMACIJOS TURINIO APSAUGOS IR SAUGUMO KLAUSIMAIS ANALIZĖ

1. ES teisės aktų analizė

1. 1981 m. **Konvencija dėl asmenų apsaugos** ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108), kuri nurodo, kad automatizuotai tvarkomi asmens duomenys turi būti gauti ir tvarkomi sąžiningai ir teisėtai, saugomi konkrečiam ir teisėtam tikslui ir nenaudojami kitu šiam tikslui prieštaraujančiu būdu, ne pernelyg didelės apimties, negu reikalauja konkretus tikslas, laikomi ne ilgiau, nei tai yra reikalinga tam tikslui, dėl kurių duomenys buvo saugomi. Lietuvos Respublikos Seimas šią konvenciją su pataisomis, priimtomis Europos Tarybos Ministrų Komiteto 1999 m. birželio 15 d. Strasbūre, ratifikavo 2001 m. vasario 20 d. įstatymu Nr. IX-189.

2. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva **95/46/EB** dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo reikalauja, kad valstybės narės užtikrintų fizinių asmenų teises ir laisves, susijusias su asmens duomenų tvarkymu, ir ypač jų privatumo teisę, siekiant užtikrinti laisvą asmens duomenų srautą Bendrijoje.

3. 1997 m. Europos Parlamento ir Tarybos direktyva **97/66/EB** dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje nurodo, kad valstybės narės privalo

[13] Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 "Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo" // Valstybės žinios. 2001, Nr. 110-4006.

prižiūrėti atsakomybės nuostatų laikymąsi ir sankcijas, išplečia duomenų apsaugos ribas, įtraukdama juridinius asmenis.

4. 1998 m. birželio 22 d. Europos Parlamento ir Tarybos direktyva **98/34/EB** nustato informacijos teikimo tvarką techninių standartų ir reglamentų bei taisyklių, reglamentuojančių informacinės visuomenės paslaugas.

5. 1999 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva **1999/5/EB** dėl radijo ryšio įrenginių ir telekomunikacijų galinių įrenginių bei abipusio jų atitikties pripažinimo patvirtina priemones, kurios reikalauja iš gamintojų, gaminančių kai kurių tipų įrangą elektroninių ryšių paslaugoms, įtraukti į įrenginių konstrukciją apsaugos priemones, užtikrinančias abonentų ir naudotojų asmens duomenų ir privatumo apsaugą.

6. 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (**Elektroninės komercijos direktyva**).

7. 2001 m. lapkričio 23 d. **Konvencija dėl elektroninių nusikaltimų** reikalinga, kad būtų sustabdyti veiksmai, nukreipti prieš kompiuterinių sistemų, tinklų ir kompiuterinių duomenų konfidencialumą, vientisumą ir prieinamumą, taip pat kad nebūtų leista netinkamai naudoti tokių sistemų, tinklų ir duomenų.

8. Europos Parlamento ir Tarybos direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (2002/58/EB **Direktyva dėl privatumo ir elektroninių ryšių,** direktyvos **97/66/EB** nauja redakcija). Direktyva nurodo, kad paslaugų teikėjai, jeigu reikia, kartu su tinklo teikėju turėtų imtis tinkamų priemonių savo paslaugų saugumui užtikrinti, ir pranešti abonentams apie kiekvieną tinklo saugumo pažeidimo specifinę riziką.

2. Lietuvos Respublikos teisės aktų analizė

9. Elektroninių duomenų teisinę apsaugą reglamentuoti pradėjo 1996 m. sausio 30 d. Lietuvos Respublikos **kompiuterių programų ir duomenų bazių teisinės apsaugos įstatymas** Nr. I-1188, kurio galiojimą sustabdė 1999 m. gegužės 18 d. Lietuvos Respublikos **autorių teisių ir gretutinių teisių** įstatymas Nr. VIII-1185, kurio 30-32 straipsniai reguliuoja kompiuterių programų atgaminimo, adaptavimo ir dekompiliavimo teises bei duomenų bazių naudojimą.

10. 1996 m. birželio 11 d. Lietuvos Respublikos **asmens duomenų teisinės apsaugos įstatymas** Nr. I-1374 (2003 m. sausio 21 d. įstatymo nauja redakcija). Įstatymas nustato fizinių asmenų, kaip duomenų subjektų, teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę, tvarkant asmens duomenis. Asmens duomenys gali būti renkami

[14] Lietuvos Respublikos vidaus reikalų ministro 2003 m. sausio 27 d. įsakymas Nr. 1V-33 "Dėl informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo" // Valstybės žinios. 2003, Nr. 77-3541.

tik apibrėžtais ir teisėtais tikslais, tokios apimties, kuri būtina asmens duomenims tvarkyti. Įstatymas reguliuoja asmens duomenų saugojimą ir teikimą, duomenų saugumui būtinas priemones. Išankstinę duomenų patikrą atlieka Valstybinė duomenų apsaugos inspekcija, kuriai ir pavesta prižiūrėti ir kontroliuoti šio įstatymo vykdymą.

11. 1996 m. liepos 2 d. Lietuvos Respublikos **visuomenės informavimo įstatymas** Nr. I-1418, kuris reglamentuoja, kokia informacija yra vieša ir galima skelbti, ir kokia yra neskelbtina.

12. 1996 m. rugpjūčio 13 d. Lietuvos Respublikos **valstybės registrų įstatymas** Nr. I-1490, kuris nustato registrų steigimo, tvarkymo, naudojimo, pertvarkymo ir likvidavimo tvarką, valstybės registrų tvarkymo įstaigų, joms vadovaujančių ir jų priežiūrą atliekančių institucijų, valstybės registrams duomenis teikiančių bei valstybės registrų duomenis naudojančių juridinių ir fizinių asmenų pareigas ir teises, šių teisių apsaugą, juridinių ir fizinių asmenų, kurių duomenys yra registro objektas, pareigas ir teises, šių teisių apsaugą.

13. 1996 m. lapkričio 29 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 1418 patvirtino Valstybės kadastrų, klasifikatorių, registrų steigimo, projektavimo ir reorganizavimo tvarką bei Lietuvos Respublikos **valstybės registro tipinius nuostatus**.

14. 1997 m. vasario 17 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 122 patvirtina pirmuosius **Valstybinės duomenų apsaugos inspekcijos** (toliau – Inspekcija) nuostatus. Inspekcijos nuostatai tvirtinami dar kelis kartus, keičiant Inspekcijos priklausomybę ministerijoms, paskutinį kartą jie patvirtinami 2001 m. rugsėjo 25 d. nutarimu Nr. 1156. Svarbiausieji Inspekcijos veiklos tikslai yra plėtoti duomenų apsaugą, prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais ir užtikrinti duomenų subjekto teisių apsaugą. Svarbiausieji Inspekcijos uždaviniai – prižiūrėti ir kontroliuoti LR asmens duomenų teisinės apsaugos įstatymo vykdymą, vykdyti nacionalinės Šengeno informacinės sistemos asmens duomenų tvarkymo teisėtumo kontrolę ir įgyvendinti LR telekomunikacijų įstatymo 49-56 straipsnių, Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis nuostatas.

15. 1997 m. gegužės 22 d. Lietuvos Respublikos **operatyvinės veiklos įstatymas** (jį pakeitė 2002 m. birželio 20 d. įstatymas Nr. IX-965), kuris reglamentuoja operatyvinės informacijos panaudojimą ir atskleidimą.

16. 1997 m. liepos 4 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 726 įsteigė **Valstybės registrą - valstybės registrų sąrašą** ir patvirtino jo nuostatus.

17. 1997 m. liepos 7 d. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės įsakymas Nr. 35, patvirtinęs **Reikalavimus dokumentų saugykloms**.

18. 1997 m. rugsėjo 4 d. Lietuvos Respublikos Vyriausybė nutarimas Nr. 952 „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“ (2002 m. gruodžio 31 d. nauja redakcija). Nutarimu patvirtinami **bendrieji duomenų saugos reikalavimai**. Šie reikalavimai taikomi duomenų bazėms, kurias tvarko valstybės registrų tvarkymo įstaigos, asmens duomenų valdytojai, kitų valstybės ir savivaldos informacinių sistemų duomenų valdytojai bei duomenų tvarkymo įstaigos. Duomenų valdytojas turi dvi teisines organizacines pareigas, kurias atlikdamas privalo atsižvelgti į rekomenduojamus Lietuvos standartus atitinkančius tarptautinius standartus ISO/IEC „Informacijos technologija. Saugumo technika“: suformuluoti specialius duomenų apsaugos priemonių reikalavimus (duomenų klasifikavimą pagal slaptumo laipsnį, duomenų apsaugos lygmenį, galimus pažeidimų rizikos veiksnius) ir informacinės sistemos nuostatuose nustatyti duomenų apsaugos įgyvendinimo tvarką bei priemones.

19. 1999 m. lapkričio 25 d. Lietuvos Respublikos **valstybės ir tarnybos paslapčių įstatymas** Nr. VIII-1443 (2003 m. gruodžio 16 d. nauja redakcija). Naujos redakcijos 8 skirsnis reguliuoja automatizuotų duomenų apdorojimo sistemų ir tinklų, kuriuose yra saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, apsaugą, leidimų apdoroti įslaptintą informaciją ADA sistemomis ir tinklais išdavimą.

20. 2000 m. kovo 27 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 349 įsteigė **Asmens duomenų valdytojų valstybės registrą** ir patvirtino jo nuostatus. 2002 m. vasario 20 d. nutarimu Nr. 262 šį registrą reorganizavo, kad jis galėtų veikti Lietuvai tapus Europos Sąjungos nare, ir iš naujo patvirtino jo nuostatus bei Asmens duomenų valdytojų pranešimo apie duomenų tvarkymą automatiniu būdu tvarką.

21. 2000 m. liepos 11 d. priimtas **Elektroninio parašo įstatymas**. Jis reglamentuoja elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, nustato sertifikavimo paslaugas ir reikalavimus jų teikėjams bei elektroninio parašo priežiūros institucijos teises ir funkcijas.

22. 2000 m. rugpjūčio 30 d. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės įsakymas Nr. 19 „Dėl Lietuvos Respublikos **įslaptintų dokumentų apskaitos**, raštvedybos organizavimo, tvarkymo bei kontrolės taisyklių patvirtinimo“. Šios taisyklės nustato bendruosius reikalavimus, kaip rengti, įforminti, tvarkyti, naikinti ir saugoti dokumentus, kuriuose yra valstybės ar tarnybos paslaptį sudarančios informacijos, bei reglamentuoja įslaptintų dokumentų raštvedybos organizavimo ir kontrolės tvarką.

23. 2000 m. rugsėjo 26 d. Lietuvos Respublikos Seimas priėmė naują **Baudžiamąjį kodeksą**. Kodekse atsirado iš esmės naujas XXX skyrius „**Nusikaltimai informatikai**“, numatantis atsakomybę už kompiuterinius nusikaltimus: 196 straipsnis – už kompiuterinės informacijos sunaikinimą ar pakeitimą, 197 straipsnis – už kompiuterinės programos sunaikinimą ar pakeitimą ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymą, 198 straipsnis – už kompiuterinės informacijos pasisavinimą ir skleidimą, 198^1 – už neteisėtą prisijungimą prie kompiuterio ar kompiuterinio tinklo ir 198^2 – už neteisėtą disponavimą įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis, skirtais nusikaltimams daryti.

24. 2001 m. sausio 31 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 112 patvirtino **Valstybės valdžios, valdymo ir savivaldybių institucijų, turinčių teisę 2001 m. neatlygintinai gauti valstybės kadastrų, klasifikatorių ir registrų duomenis, sąrašą**. Šiuos duomenis institucijos turi teisę gauti tik tiesioginėms jų funkcijoms vykdyti. 2001 m. lapkričio 5 d. nutarimu Nr. 1299 šios tvarkos galiojimas buvo pratęstas iki 2004 m. imtinai.

25. 2001 m. vasario 28 d. Lietuvos Respublikos Vyriausybė nutarimu Nr. 228 patvirtino **Duomenų teikimo duomenų subjektui atlyginimo tvarką** ir Duomenų surinkimo iš registruotų duomenų valdytojų atlyginimo tvarką (Duomenų teikimo duomenų subjektui atlyginimo taisyklių naują redakciją patvirtino 2004 m. birželio 2 d. nutarimas Nr. 676). Šios taisyklės reglamentuoja duomenų teikimo duomenų subjektui atlyginimą, kai duomenų valdytojas ar duomenų tvarkytojas ne pirmą kartą per kalendorinius metus teikia duomenis duomenų subjektui, vadovaudamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 19 straipsnio 2 dalimi.

26. Informacijos saugumo svarbą Lietuvos valstybės institucijose nurodė **Informacijos technologijų saugos valstybinė strategija**, patvirtinta 2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625.

27. Vadovaudamasi šia strategija, Lietuvos Respublikos Vyriausybė 2002 m. gruodžio 31 d. nutarimu Nr. 2105 patvirtino **naują Bendrųjų duomenų saugos reikalavimų redakciją**, kurioje nurodė šių reikalavimų tikslą – sudaryti sąlygas saugiai tvarkyti automatizuotu būdu duomenis valstybės registruose ir kitose valstybės informacinėse sistemose.

28. Vykdydamas Informacijos technologijų saugos valstybinės strategijos įgyvendinimo planą, Lietuvos Respublikos vidaus reikalų ministras 2003 m. sausio 27 d. įsakymu Nr. 1V-33 patvirtino **Informacijos klasifikavimo pagal duomenų grupes rekomendacijas**, kuriose duomenų svarbumą apibrėžia informacinės sistemos kategorija, nustatoma pagal informacinės sistemos duomenų grupes ir tų grupių savybių įtaką informacinės sistemos darbui.

29. Įgyvendindama Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ (nauja redakcija patvirtinta 2002 m. gruodžio 31 d. nutarimu Nr. 2105) 3 punktą, Vidaus reikalų ministerija parengė ir 2003 m. liepos 16 d. Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-272 patvirtino **Tipinius duomenų saugos nuostatus**, kuriuose nurodė, kad valstybės registro ar kitos valstybės institucijos informacinės sistemos valdytojas, vadovaudamasis šiais nuostatais rengia ir suderinęs su Vidaus reikalų ministerija tvirtina savo informacinės sistemos duomenų saugos nuostatus, kurie kartu su rengtinomis detaliomis instrukcijomis, procedūrų aprašymais ir saugaus darbo su duomenimis tvarkos taisyklėmis apibrėžia informacinės sistemos saugumo politiką.

30. Lietuvos Respublikos Vyriausybė 2004 m. balandžio 19 d. nutarimu Nr. 451 patvirtino **Valstybės informacinių sistemų steigimo ir įteisinimo taisykles**, pagal kurias informacinės sistemos steigėjas derinančioms organizacijoms turi pateikti sistemos nuostatų projektą, o Vidaus reikalų ministerijai ir šios sistemos duomenų saugos nuostatus, parengtus pagal aukščiau nurodytus Tipinius duomenų saugos nuostatus.

31. Asmenims, atsakingiems už konkrečių organizacijų informacijos technologijų saugumą, problemų sprendimo vadovu tapo **Lietuvos standartas „Informacijos technologija. Informacijos technologijų saugumo valdymo gairės“**, lietuviškoji Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės elektrotechnikos komisijos (IEC) 1-ojo jungtinio technikos komiteto parengto techninio pranešimo ISO/IEC TR 13335:1996 versija. Šis standartas turi 5 dalis.

32. Kiekvienos organizacijos, nusiteikusios pas save užtikrinti informacijos saugumą, parankine knyga tapo 2002 m. liepos 1 d. įsigaliojęs **Lietuvos standartas „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“**, tapatus tarptautiniam standartui ISO/IEC 17799:2000, kurį Lietuvos standartizacijos departamentas patvirtinimo būdu perėmė iš Tarptautinės standartizacijos organizacijos ir Tarptautinės elektrotechnikos komisijos. Savo ruožtu, šis tarptautinis standartas yra parengtas pagal Didžiosios Britanijos standartą BS 7799.

III. ORGANIZACIJOS SAUGOS VALDYMO STRUKTŪRA

Sena Max Webber’io biurokratinė organizacijos valdymo sistema visai netinka organizacijos saugos valdymui. Šiai funkcijai vykdyti organizacijai per brangu kurti centralizuotą hierarchinę sistemą. Daug efektingiau panaudoti darbą grupėje, „punktyrinį“ vadovavimą, nuolatinį

mokymąsi ir kvalifikacijos kėlimą (*long life learning)*, kas yra būdinga šiuolaikinei žiniomis ir informacija grindžiamai valdymo aplinkai[15].

Viešojo administravimo žinovai teigia, kad tradicinė biurokratinė centralizuota organizacija turėtų transformuotis į lanksčių kolektyvų tinklą, o mažėjant hierarchinėms sąveikoms vis didesnę reikšmę įgyja horizontalios sąveikos[16].

Tuo labiau, kad organizacijos saugos valdymui reikalingi įvairių sričių specialistai, o dažniausiai – kelių specialybių „hibridai“, kurių tiesioginis viršininkas gali neturėti jokių vienos iš šių specialybių žinių. Todėl organizacijoje vis didėja poreikis specialistų (vadovų), turinčių mažiau „objektyviųjų žinių, o daugiau žinojimo organizavimo, komunikacijos ir vadybos žinių“[17].

Atsižvelgdama į tai ir vadovaudamasi Informacijos technologijų saugos valstybine strategija[18], kuri numato duomenų saugos įgaliotinių pareigybių įvedimą, Bendraisiais duomenų saugos reikalavimais[19], reikalaujančiais organizacijoje paskirti asmenį, atsakingą už saugumo politikos įgyvendinimą, ir Tipiniais duomenų saugos nuostatais[20], autorė siūlo tokį organizacijos saugos valdymo modelį, kurio schema pateikta 1 priede.

Bendrai organizacijos saugai valdyti sukuriamas nuolatinis Saugos administravimo komitetas (toliau – Komitetas), kuriam vadovauja organizacijos direktoriaus pavaduotojas – vyriausiasis saugos administratorius. Komiteto nariais paskiriami Informacinių sistemų tarnybos atstovas – IT saugos administratorius, vyriausiasis darbuotojų saugos ir sveikatos inspektorius, įslaptintų dokumentų apyvartos saugos administratorius, fizinės saugos administratorius. Komitetas tiesiogiai vadovauja Saugos administravimo pakomitečiams, sukurtiems kiekvienoje organizacijos tarnyboje (jie gali būti kuriami ir didesniuose skyriuose, jei tam yra poreikis). Pakomitetis atsakingas už saugą savo tarnybos veiklos zonoje.

Komiteto nuostatuose nurodoma, kad svarbiausi Komiteto uždaviniai – analizuoti ir vertinti saugos padėtį, Lietuvos ir ES teisės aktų laikymąsi organizacijoje, nustatyti atitinkamų vidaus teisės aktų reikalingumą ir jų parengimą saugos srityje, rengti organizacijos saugos viziją ir strategiją bei koordinuoti jų įgyvendinimą organizacijoje. Komiteto funkcijos, vykdant šiuos uždavinius:

---

[15] R. Petrauskas. Informacinių technologijų taikymas viešajame administravime. –Vilnius:LTU, 2001, P.15.
[16] J. Lakis. Permainos ir iššūkiai organizacijų vidaus administravimo srityje // Viešoji politika ir administravimas: LTU, KTU, 2003 (6), P.65-67.
[17] A. Augustinaitis. Informacijos visuomenės profesionalumo kriterijai // Informacijos mokslai.2001,Nr.16, P.17-30.
[18] Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 “Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo” // Valstybės žinios. 2001, Nr. 110-4006.
[19] Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2105 “Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose" pakeitimo” // Valstybės žinios. 2003, Nr. 2-45.
[20] Lietuvos Respublikos vidaus reikalų ministro 2003 m. liepos 16 d. įsakymas Nr. 1V-272 “Dėl Tipinių duomenų saugos nuostatų patvirtinimo” // Valstybės žinios. 2003, Nr. 76-3511.

- vertinti saugos padėtį organizacijoje;
- organizuoti su sauga susijusios politikos kūrimą;
- plėsti saugos standartų įgyvendinimą;
- užtikrinti nenumatytų atvejų planavimą;
- informacinių sistemų saugos architektūros laikymąsi;
- periodiškai peržiūrėti rizikos veiksnius, grėsmes ir pažeidžiamumus; aprobuoti tinkamų apsaugos priemonių, užtikrinančių priimtiną rizikos lygį, atsižvelgiant į turimus finansinius ir žmogiškuosius išteklius, pasirinkimą;
- užtikrinti, kad saugos incidentai būtų identifikuoti, sekami ir laiku išspręsti;
- garantuoti pakomitečių narių (saugos personalo) valdymą, apmokymą, reikalingų priemonių ir įgaliojimų suteikimą;
- visų organizacijos darbuotojų supažindinimą su saugos politika ir reikalavimais, saugant informacijos išteklius,

kaip ir nurodyta tarptautiniuose informacinių sistemų audito reikalavimuose[21].

IV. INFORMACIJOS SAUGUMO PLANAVIMO ORGANIZACIJOJE PROBLEMOS IR TURINYS

1. Vartojamų sąvokų unifikavimo problema ir reikšmė informacijos saugumo planavimui

Prieš tai esančiame skyriuje buvo kalbama apie bendros organizacijos saugos valdymą. Į tai įeina ir informacijos technologijų saugos administravimas. Kaip IT sauga siejasi su informacijos saugumu? Tuo labiau, kad literatūroje labai dažnai šios sąvokos keičiamos viena kita, kartais minimos abi kartu ir t.t. Lietuvos standarte LST ISO/IEC TR 13335-1:2000 „Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų sąvokos ir modeliai“ informacijos technologijų saugumas apibrėžiamas kaip visi aspektai, susiję su slaptumo, vientisumo, prieinamumo, atsakingumo, tapatumo ir prieinamumo apibrėžimu, įgyvendinimu ir palaikymu. Apibrėžimas visai nesusietas su tuo, kas saugoma. Kitas apibrėžimas – informacijos technologijų saugumo politika – apibūdinama, kaip taisyklės, direktyvos ir praktinės priemonės, kurios nusako, kaip turtas, taip pat ir slapta informacija, yra valdomas, saugomas ir perduodamas organizacijos ir jos **informacijos technologijų** sistemų viduje[22]. O jau Lietuvos standarte LST ISO/IEC 17799:2000 „Informacijos technologija. Praktiniai informacijos valdymo principai“ kalbama vien tik apie informacijos saugumą, kuris

[21] John Kramer. The CISA Prep Guide: Mastering the Certified Information Systems Auditor, 4 chapter, Protection of Information Assets. 2003, Wiley Publishing, Inc.Indianapolis, Indiana, P.184-185.
[22] LST ISO/IEC TR 13335-1:2000 „Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų sąvokos ir modeliai“. P.1.

apibrėžiamas, kaip informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas[23]. Turint omeny, kad informacinės technologijos – tai techninė ir programinė įranga, naudojama įmonės duomenims, informacijai ir žinioms kaupti, perduoti, apdoroti ir skleisti, galima sakyti, kad IT sauga apima ir informacijos, esančios IT sistemų viduje, saugumą. Tuo labiau, kad daugelis saugos komponentų užtikrinami IT priemonėmis.

Kartais literatūroje ar Lietuvos teisės aktuose sutinkama sąvoka „Duomenų sauga“ (2003 m. liepos 16 d. Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-272 patvirtinti Tipiniai duomenų saugos nuostatai). Išeinant iš to, kad duomenys yra informacijos sudėtinė dalis, kaip buvo išnagrinėta pirmame šio darbo skyriuje, sąvoką „Duomenų sauga“ galima traktuoti adekvačiai sąvokai „Informacijos saugumas“.

2. Informacijos saugumo organizacijoje tikslų ir strategijos nustatymo problema

Tikslas nustato, kas turi būti pasiekta, strategija numato, kaip šiuos tikslus pasiekti, o politika numato, ką reikia padaryti. Strategija – veiksmai ir sprendimai bei organizacijos sąveika su aplinka ilgu laikotarpiu. Politika – nuostatų ir strategijų visuma tikslui pasiekti.

Organizacijos saugos politika apima visos organizacijos principus ir direktyvas, joje turi atsispindėti platesnės politikos aspektai, susiję su individo teisėmis, legalumo reikalavimais ir standartais. Organizacijos IT saugumo politikoje turi atsispindėti bendrieji saugumo principai ir bendrieji IT sistemų naudojimo organizacijos viduje saugumo klausimai.

Bendriausias IT saugos tikslas – garantuoti, kad organizacija galėtų veikti, esant priimtino lygio rizikoms. Joks saugumas negali būti absoliučiai efektyvus, todėl svarbu planuoti žalos padarinių atkūrimo veiklą po nepageidaujamo incidento ir sudaryti saugumo struktūrą, apribojančią žalos dydį.

Būtina užtikrinti šešis saugumo aspektus:

- Slaptumą – savybė, kad informacija neprieinama ar neatskleidžiama nelegaliems individams, esybėms ar procesams;
- Vientisumą – savybė, kad duomenys nebuvo pakeisti ar sunaikinti nelegaliu būdu (duomenų vientisumas) ar savybė, kad sistema nustatytu būdu atlieka numatytas funkcijas, kad yra neįmanomas sąmoningas ar atsitiktinis nelegalus manipuliavimas sistema (sistemos vientisumas);
- Prieinamumą – savybė būti prieinamu ir naudojamu legaliems vartotojams;
- Atsakingumą – savybė, kuri garantuoja, kad veiksmų atlikėjai vienareikšmiškai gali būti nustatyti;

[23] LST ISO?IEC 17799:2000 „Informacijos technologija. Praktiniai informacijos valdymo principai“. P.1.

- Tapatumą – savybė, kuri garantuoja, kad subjekto ar šaltinio tapatumas tikrai yra toks, kaip teigiama. Tapatumas siejamas su vartotojais, procesais, šaltiniais sistemomis ir informacija;
- Patikimumą – savybė, kad elgesys ar rezultatas atitiks tai, ko tikimasi[24].

IT sistemų saugumas – daugiamatė problema, todėl būtina atsižvelgti į

- aplinką, kurioje slypi, nuolat besikeičiančios ir tik dalinai žinomos grėsmės;
- organizacijos turtą;
- šio turto pažeidžiamumą;
- turtui apsaugoti ir grėsmių nepageidaujamiems poveikiams mažinti pasirinktas apsaugos priemones;
- apsaugos priemones, kurios modifikuoja rizikas;
- liekamąsias, organizacijai priimtinas rizikas.

Būtiną saugumo lygį apibrėžia IT saugumo tikslai, kuriuos organizacijai reikia pasiekti. Kad būtų galima įvertinti šiuos saugumo tikslus, reikia išnagrinėti turtą ir jo reikšmę organizacijai. Tai iš esmės priklauso nuo to, kiek svarbios yra informacijų technologijos organizacijos veiklai, pačių IT kaina sudaro tik dalį jų reikšmės. Norint nustatyti, kaip organizacijos veikla priklauso nuo IT, reikia atsakyti į tokius klausimus:

- kokios yra svarbios ar labai svarbios veiklos sritys, kurios neįmanomos be IT?
- kokias užduotis įmanoma atlikti tik su IT?
- kokie esminiai sprendimai priklauso nuo IT pateikiamos informacijos tikslumo vientisumo ar prieinamumo arba nuo šios informacijos atnaujinimo?
- kokia slapta informacija turi būti apsaugota?
- kokios yra nepageidaujamo saugumo incidento pasekmės organizacijai?

Reikia nepamiršti, kad planuojant tam tikrą organizacijos veiklą, šiuo atveju, informacijos saugumo užtikrinimą, iškyla tam tikri apribojimai:

- organizaciniai (pvz., geranoriškas vadovybės palaikymas, resursų skyrimas ir t.t.);
- finansiniai (apsaugos priemonė neturi būti brangesnė nei saugomas turtas, neturi būti viršytas numatytas biudžetas ir t.t.);
- aplinkos (disponuojamos erdvės dydis, klimato, geografinės sąlygos);
- personalo (pakankama kompetencija, skiriami ištekliai, tiek žmonių, tiek darbo laiko ir t.t.);
- laiko (administracijos ar aukščiau stovinčios organizacijos nustatyti terminai, patogiausias IT sistemos būvio laikotarpis ir t.t.);

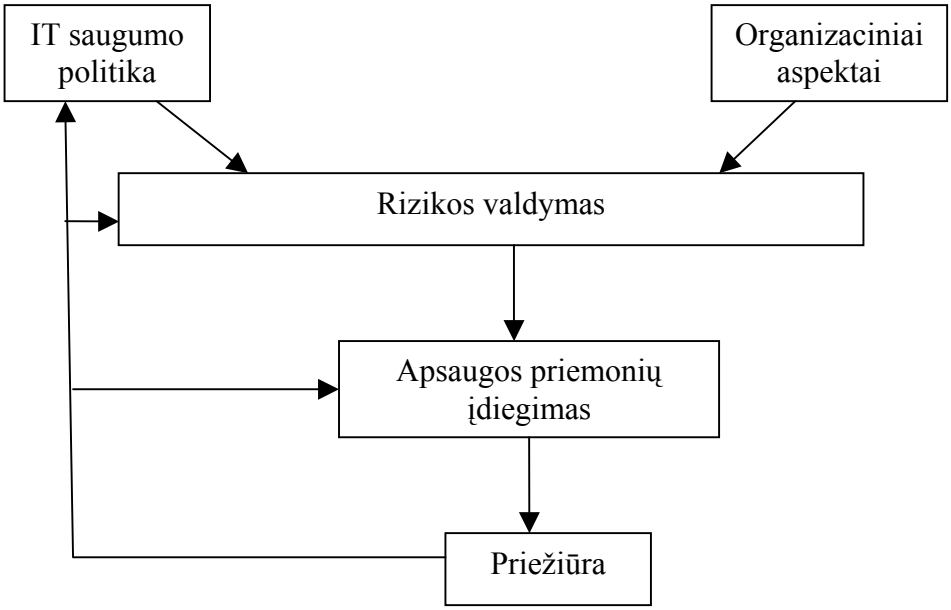
- teisiniai (būtinumas saugoti asmens duomenis, ūkio subjektų komercinę informaciją, reikalauja priešgaisrinės apsaugos taisyklės ir t.t.);
- techniniai (pvz., programų ar kompiuterinės įrangos nesuderinamumas);
- kultūriniai/socialiniai (reikia atsižvelgti į organizacijos tradicijas, darbuotojų sąmoningumą).

Visi su IT sistemų saugumu susiję veiksmai yra efektyviausi tada, kai jie atliekami tolygiai visoje organizacijoje nuo kiekvienos IT sistemos būvio ciklo pradžios. IT sistemos būvio ciklas gali būti suskirstytas į tris pagrindines fazes, kurios visos susijusios su IT saugumu:

- planavimas: į IT saugumo poreikius turi būti atsižvelgiama visais planavimo ir sprendimų priėmimo momentais;
- įgijimas: IT saugumo reikalavimai turi būti integruoti į sistemų projektavimo, plėtojimo, pirkimo, atnaujinimo ar kitokio konstravimo procesus;
- naudojimas: IT saugumas turi būti integruotas į naudojimo aplinką, juo turi būti pasirūpinta, kai naudojama sistema keičiama arba, kai atsiranda nauji naudojimo aplinkos pokyčiai.

3. Informacijos saugumo planavimo procesas

Planuojant būtina įjungti mąstymo procesus[25] ir juos pavaizduoti loginių schemų pagalba. Pradėti lengviausia nuo abstrakčios schemos:



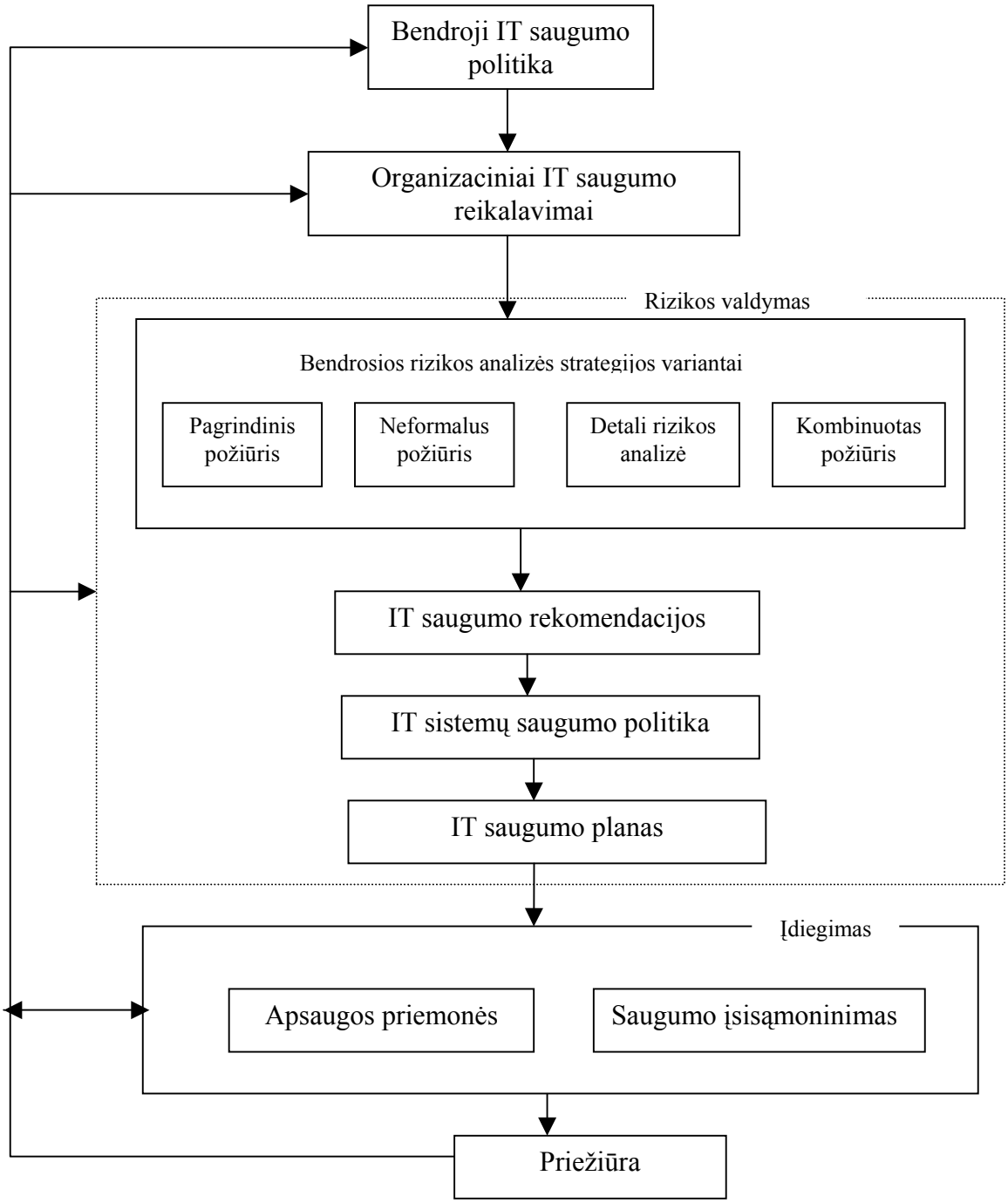
1 schema. IT saugumo valdymo procesas

[24] Visos sąvokos pateiktos iš LST ISO/IEC TR 13335-1:2000 „Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų sąvokos ir modeliai“, P.1-2.
[25] Eliyahu M. Goldratt. Tikslas II. Sėkmė priklauso ne nuo laimės.

Turėdami abstrakčią schemą, kurioje pavaizduoti pagrindiniai saugumo valdymo elementai, ir žinodami IT saugumo valdymo funkcijas:

- organizacinių IT saugumo tikslų, strategijos ir politikos nustatymas;
- organizacinių IT saugumo reikalavimų nustatymas;
- grėsmės IT turto saugumui organizacijos viduje nustatymas ir analizė;
- rizikos nustatymas ir analizė;
- atitinkamų saugumo priemonių specializavimas;
- efektyviai apsaugančių informaciją ir paslaugas organizacijos viduje priemonių įdiegimo ir naudojimo priežiūra;
- saugumo įsisąmoninimo programos plėtojimas ir diegimas;
- incidentų atskleidimas ir reakcija į juos;

galime 1 schemą pavaizduoti detaliau:



2 schema. IT saugumo planavimo ir valdymo apžvalga

Šioje schemoje išvardinti veiksmai ir funkcijos turi būti suderinti su organizacijos stiliumi, dydžiu ir struktūra, taip pat su jos veiklos pobūdžiu.

Ypač svarbu pasirinkti tokią rizikos valdymo strategiją, kuri labiausiai tiktų organizacijos aplinkai ir būtų efektyvi, naudojant tam tikras lėšas ir laiką. Daryti išsamią visų sistemų apžvalgą išteklių ir laiko atžvilgiu nėra efektyvu, tačiau negalima iš viso nekreipti dėmesio į rimtas grėsmes. Požiūris, kuriuo pasiekiama abiejų šių kraštutinumų pusiausvyra, reikalauja, kad būtų

daromos IT sistemų saugumo poreikių bendro lygio apžvalgos ir šiuos poreikius atitinkančios detalios analizės.

Kai kuriais atvejais organizacija gali nutarti nenaudoti jokių apsaugos priemonių arba atidėti jų įdiegimą. Jeigu toks sprendimas yra priimtas, administracija turi visiškai suprasti, kokios rizikos egzistuoja ir kokie žalingi poveikiai yra su jomis susiję, taip pat kiek tikėtini yra nepageidaujami įvykiai. Stokojant šių žinių, organizacija netyčia gali pažeisti įstatymus, kitus teisės aktus, ir jos veiklai gali grėsti potencialūs nuostoliai.

Kaip nurodyta 2 schemoje bendrosios rizikos analizės strategiją galima rinktis iš keturių variantų.

Pagrindinis požiūris. Pasirenkamos apsaugos priemonės, kuriomis pasiekiamas visų sistemų bazinis apsaugos lygis. Šios apsaugos priemonės gali būti perimtos ir prisitaikytos iš kitų organizacijų, tokių kaip tarptautinių ir nacionalinių standartų organizacijų. Šio požiūrio pranašumai:

- nereikia naudoti išteklių detaliai rizikos analizei, paprastai pagrindinėms apsaugos priemonėms nustatyti nereikia didelių išteklių, apsaugos priemonių parinkimo kaštai ir laikas sumažėja;
- tos pačios priemonės gali būti pritaikytos daugeliui sistemų.

Jei daugelis organizacijos sistemų veikia bendroje aplinkoje ir jei veiklos poreikiai panašūs, parinkti pagrindines apsaugos priemones gali būti efektyvus lėšų naudojimo požiūriu sprendimas. Šis požiūris turi ir trūkumų:

- jeigu pagrindinis lygis nustatytas per aukštas, kai kurioms sistemoms tai gali būti per brangu arba pernelyg varžyti jų veiklą;
- jei pagrindinis lygis per žemas, kai kurioms sistemoms gali neužtekti saugumo;
- jei sistema atnaujinama, gali būti sunku nustatyti, ar pradinės pagrindinės apsaugos priemonės dar tebėra pakankamos.

Neformalus požiūris. Neformali analizė nesiremia struktūrizuotais metodais, joje naudojamos individų žinios ir patirtis. Šio varianto pranašumas toks:

- neformaliai analizei atlikti nereikia įgyti papildomų įgūdžių,
- ji atliekama greičiau, negu detali rinkos analizė.

Šis požiūris gali būti tinkamas mažoms organizacijoms ir lėšų atžvilgiu efektyvus. Jo trūkumai:

- padidėja tikimybė neatsižvelgti į kai kurias rizikas ar svarbias sritis;
- rezultatams gali turėti įtakos subjektyvūs požiūriai ir įsitikinimai;
- pasirenkamos apsaugos priemonės menkai pagrindžiamos, todėl gali būti sunku pateisinti išlaidas joms.

Detali rizikos analizė. Atliekama detali visų sistemų rizikos analizė, kuri apima turto ir jo reikšmingumo, grėsmių šiam turtui lygio ir turto pažeidžiamumų nustatymą. Detali rizikos analizė gali būti daug sąnaudų reikalaujantis procesas, todėl jis reikalauja rūpestingo ribų nustatymo ir nuolatinio vadovybės dėmesio. Šio varianto pranašumas tokie:

- nustatomas kiekvienos sistemos saugumui tinkamas saugumo lygis;
- pateikia detalią informaciją, kuri praverčia atsinaujinant sistemoms.

Pagrindinis šio požiūrio trūkumas – jis reikalauja palyginti daug laiko ir lėšų.

Kombinuotas požiūris. Iš pradžių, naudojantis bendro lygio rizikos analize, nustatomos tos sistemos, kurioms gresia didelė rizika arba kurios yra gyvybiškai svarbios veiklai. Remiantis analizės rezultatais sistemos suskirstomos į reikalaujančias detalios rizikos analizės, kad būtų pasiekta tinkama apsauga, ir į tas, kurioms pakanka pagrindinės apsaugos.

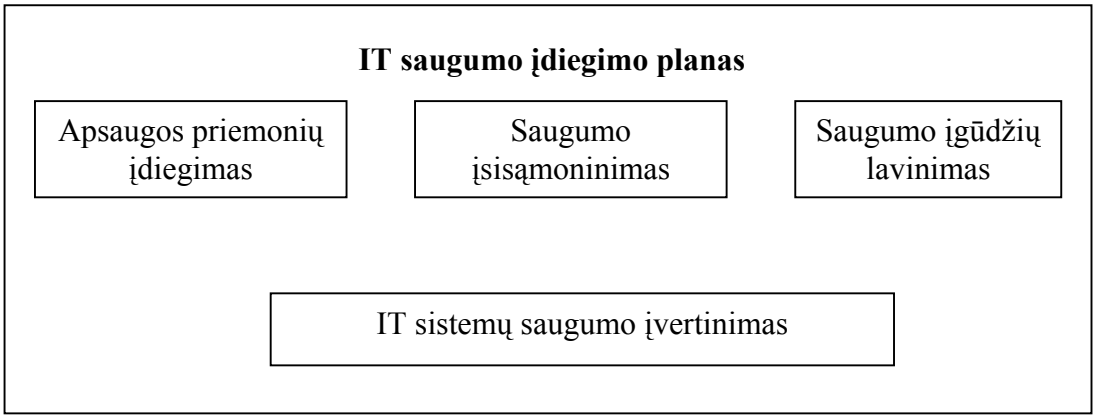
Šiame variante derinami geriausi pagrindinio požiūrio ir detalios rizikos analizės bruožai. Taigi, apsaugos priemonėms nustatyti reikalingas laikas ir pastangos mažinamos, tuo pat metu užtikrinant, kad visos sistemos yra tinkamai apsaugotos. Šio požiūrio pranašumai:

- prieš panaudojant ženklius išteklius reikalingą informaciją surinkus paprastos bendro lygio apžvalgos būdu, labiau tikėtina, kad rizikos valdymo programa bus priimta;
- gali būti įmanoma betarpiškai susidaryti organizacinį saugumo programos vaizdą, kuris gali būti panaudotas planuojant;
- ištekliai ir pinigai gali būti panaudoti, kur naudingiausia, ir į sistemas, kurioms gresia didžiausia rizika, gali būti atsižvelgiama iš anksto.

Pagrindinis šio požiūrio trūkumas – analizuojant bendro lygio riziką, į kai kurias sistemas, kurioms reikia detalios rizikos analizės, gali būti neatsižvelgta, tačiau bet kuriuo atveju tokios sistemos bus apsaugotos pagrindinėmis apsaugos priemonėmis.

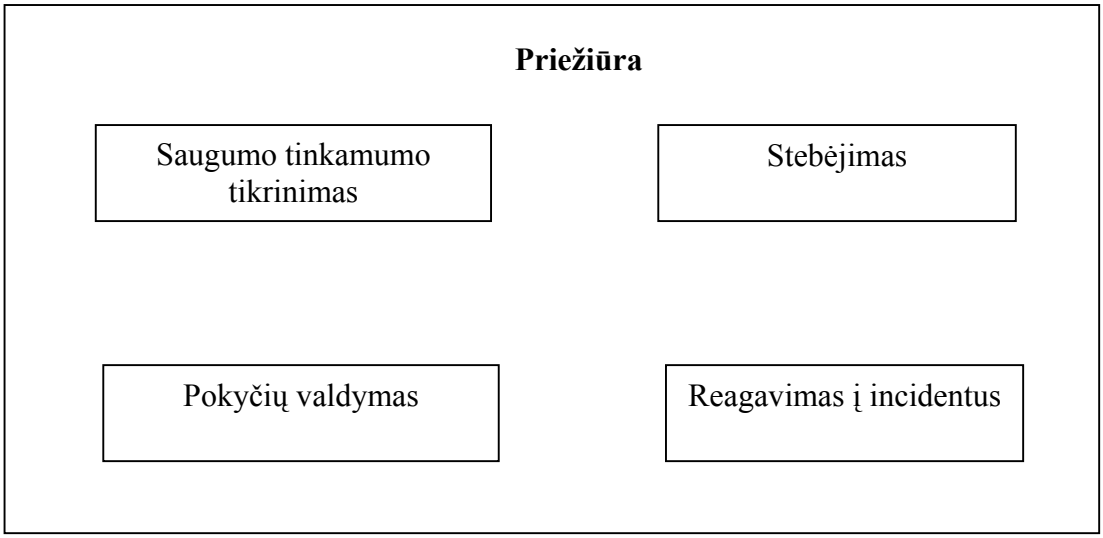
Daugeliu atvejų šis variantas pateikia išlaidų atžvilgiu efektyviausią požiūrį, daugeliui organizacijų jis yra rekomenduotinas rizikos analizės būdas. Autorė taip pat renkasi šitą būdą, nes jos organizacijoje yra įvairia veikla užsiimančių tarnybų ir įvairaus jautrumo saugai sistemų.

Esant poreikiui galimas 2 schemoje pavaizduoto IT saugumo valdymo plano detalizavimas. Pavyzdžiui, įdiegimo etapą galima pavaizduoti taip:



3 schema. IT saugumo įdiegimo planas

Lygiai taip pat galima detalizuoti ir IT saugumo priežiūrą:



4 schema. IT saugumo priežiūra

Kitame skyrelyje bus kalbama apie informacijos saugumo dokumentą – IT saugumo architektūrą, kuriame aptariamos techninės apsaugos priemonės, nors į netechninius aspektus irgi atsižvelgiama. Toliau galimi ir kiti dokumentai – stambaus masto projektavimo dokumentas, detalaus projektavimo dokumentas ir kiti, bet autorė šiame darbe jų nenagrinės.

4. Informacinių technologijų saugumo architektūra

Dėl technologinių inovacijų spartos, didesnio funkcionalumo bei tarpusavio ryšių IT sprendimai darosi vis sudėtingesni, todėl dažnai būna neįmanoma iš anksto – prieš įdiegiant ir naudojant IT sistemas – išsamiai įvertinti riziką. Būtinybė naudoti išorinius šaltinius, tokius kaip

duomenų perdavimo tinklai, projektavimo ir techninės priežiūros partnerių paslaugos, ryšys su mobiliomis ar nuotolinėmis darbo vietomis (kompiuteriais) išoriškai prisijungiant ir viešosios paslaugos, tokios kaip internetas, sukuria papildomą didelę grėsmę. Dėl bendrų standartų stokos IT nėra vientisa, sudaryta iš atskirų fragmentų, todėl saugos nepakankamumas ir trūkumai ilgą laiką gali būti nepastebėti.

Dėl šių priežasčių yra gyvybiškai svarbu sukurti tokią IT saugumo architektūrą, kuri būtų pagrįsta nedideliu projektavimo principų skaičiumi ir būtų įgyvendinta naudojant visapusiškai tarpusavyje sąveikaujančių sprendimų ir priemonių kompleksą. IT saugumo architektūra gali būti naudojama plėtojant naujas sistemas ir darant reikšmingus pakeitimus esamose sistemose.

IT saugumo architektūra yra naudojama kaip saugumo elementų struktūros ir loginio grupavimo apibrėžimo priemonė. Į ją įeina elementai, garantuojantys informacijos konfidencialumą ir užtikrinantys, kad visa prieiga prie kompiuterinių išteklių yra teisėta ir autentifikuota. Specifiniai architektūros tikslai – stiprinti atskirų taikomųjų programų ir informacijos vientisumą, neprieštaringumą ir konfidencialumą. Visi šie atributai yra būtina efektyvios ir visapusiškos saugos prielaida. Mes turime pasitikėti visomis sistemos vietomis, per kurias vartotojams teikiama prieiga prie sistemos, o ne vien tomis vietomis, kuriose laikoma informacija ir programiniai įrankiai.

IT saugumo architektūroje aprašoma, kokiu būdu IT sistemos saugumo reikalavimai turi būti patenkinti. Remiantis rizikos analizės rezultatais, joje saugumo reikalavimai paverčiami techninių saugumo paslaugų rinkiniu, taikomu tai sistemai, kuri šiuos reikalavimus turi atitikti. Nors architektūra gali būti kuriama naudojantis daugeliu skirtingų perspektyvų ir požiūrių, turi būti atsižvelgiama į vieną pagrindinį principą. Vienodo saugumo sferoje (srityje, kurioje galioja tie patys ar panašūs saugumo reikalavimai ir apsaugos priemonės) saugumo problema neturi padaryti žalos kitos vienodo saugumo sferos saugumui.

IT saugumo architektūra paprastai susideda iš vienos ar daugiau saugumo sferų. Saugumo sferos turi būti susietos su organizacijos veiklos sferomis. Šios veiklos sferos gali atitikti atskirus funkcinius veiklos padalinius (atsiskaitymų, raštvedybos paslaugų klientams skyrius). Saugumo sferos skirstomos pagal vieną ar daugiau požymių:

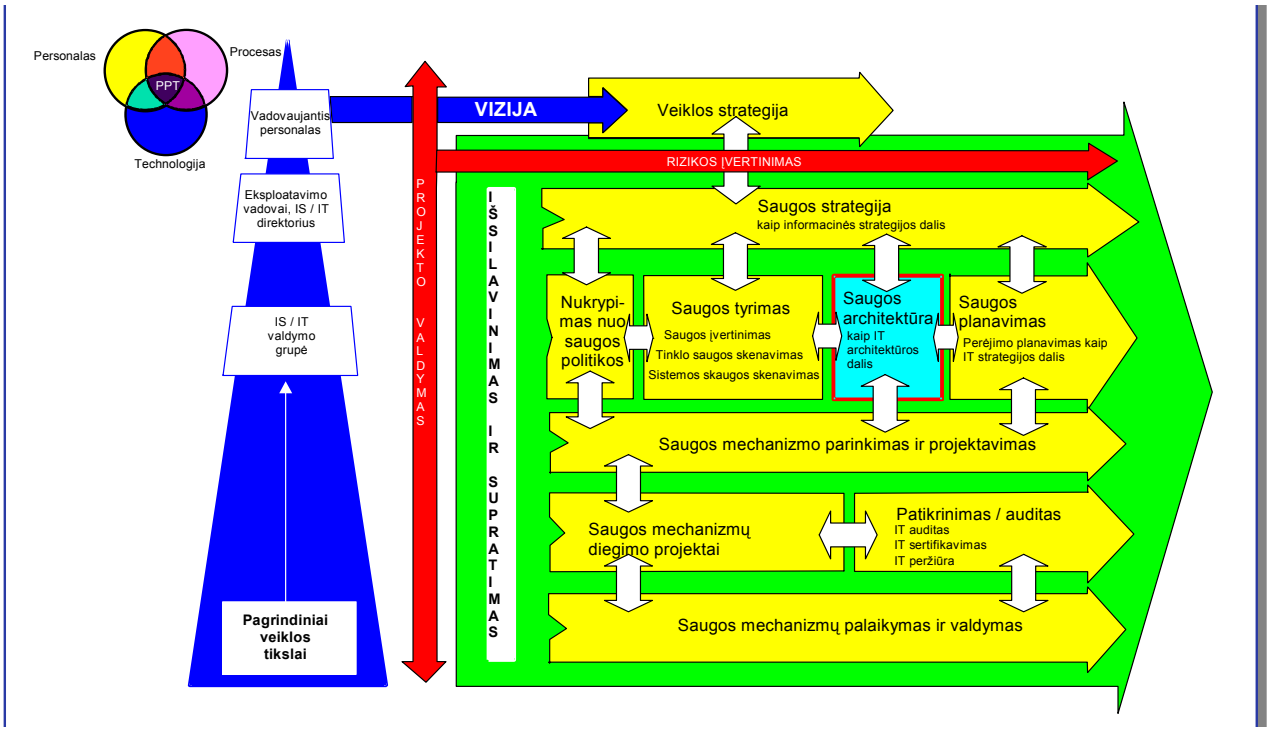
- informacijos, naudojamos veikloje, lygius, kategorijas ir rūšis;
- operacijas, atliekamas veiklos sferos viduje;
- susijusias interesų bendruomenes sferos viduje;
- ryšius su kitomis sferomis ir aplinkomis;
- interesų bendruomenės reikalaujamų funkcijų rūšis ar informacijos prieinamumą.

Konstruojant IT saugumo architektūrą, reikia atsižvelgti į šiuos dalykus:

- vienodo saugumo sferų tarpusavio ryšius ir priklausomybes;

- tarpusavio ryšių ir priklausomybių išdavas, silpninančias saugumo paslaugas;
- ypatingas paslaugas ar atsargumo priemones, reikalingas koreguoti, kontroliuoti ar priešintis, turint galvoje silpnas vietas.

IT saugumo architektūra kiek įmanoma mažiau turi trukdyti vartotojams, tuo pačiu garantuojant, kad aplinka yra optimaliai apsaugota.



5 schema. IT saugumo architektūros priklausomybė nuo kitų procesų

5 schemoje parodyta, kaip IT saugumo architektūra priklauso nuo kitų organizacijoje vykstančių procesų. Ją inicijuoja ir skatina saugumo politika ir veiklos strategija, į kurias nukreiptas grįžtamasis ryšys saugumo architektūrai vystantis ir keičiantis. Saugumo architektūra daro poveikį saugumo tyrimams, kurie pateikia saugumo būsenos įvertinimą. Taip pat saugumo architektūra inicijuoja ir skatina kitus saugumo planavimo procesus ir iniciatyvas. Svarbiausia yra tai, kad saugumo architektūra pateikia struktūrą, rekomendacijas ir pradinį planą visiems saugumo technologijos aspektams – nuo konkrečių priemonių pasirinkimo iki infrastruktūros projektavimo ir saugumo sistemos funkcionavimo. Įdiegtos taikomosios programos turi būti suderintos su saugumo architektūra.

Gera IT saugumo architektūra turi atitikti tokius reikalavimus:

- visos apsaugos priemonės pagrįstos organizacijos veiklos rizikos įvertinimo išvadomis;
- visos su saugumu susijusios funkcijos turi būti valdomos ir kontroliuojamos centralizuotai;

- apsaugos priemonių pasiekti rezultatai turi būti aiškiai matomi;
- saugumo sistema neturi būti labai sudėtingai organizuota;
- galimos prisitaikymo ir išplėtojimo galimybės, pasikeitus saugos poreikiams;
- visuotinė unifikuota metodika, pagrįsta aiškia, moduline, kelių sluoksnių ir kelių lygių metodika;
- reagavimas į incidentus realiuoju laiku ir kitos krizių valdymo galimybės;
- nenumatytų veiklos atvejų planavimo, žinių ir mokymo funkcinės galimybės;
- aiškios procedūros, atsakomybė ir jos ribos;
- apsaugos priemonės turi būti sertifikuotos arba parinktos *best praktice* principu, t.y. technologijos turi būti jau kur nors pasiteisinusios.

V. ORGANIZACIJOS INFORMACIJOS SAUGUMO VALDYMAS

Kaip matyti 2 schemoje IT saugumo valdymas apima saugumo reikalavimų analizę, plano, kaip atitikti šiuos reikalavimus sudarymą, plano įgyvendinimą, taip pat įdiegto saugumo palaikymą ir administravimą. Procesas prasideda organizacijos saugumo tikslų ir strategijos nustatymu ir bendrosios IT saugumo politikos plėtojimu.

Svarbi IT saugumo valdymo dalis yra rizikų įvertinimas ir nustatymas, kaip jas galima sumažinti iki priimtino lygio. Būtina atsižvelgti į veiklos tikslus, taip pat į organizacinius ir aplinkos aspektus bei kiekvienos IT sistemos specifinius poreikius ir rizikas.

Įvertinus IT sistemų ir paslaugų saugumo reikalavimus, patartina pasirinkti bendrosios rizikos analizės strategiją. Vidutinio dydžio organizacijai, turinčiai skirtingo saugumo funkcijų padalinius, rekomenduojamas kombinuotas požiūris, kuris numato bendro lygio visų IT sistemų rizikos analizę, nustatant aukšto rizikos lygio informacines sistemas. Tada šioms sistemoms atliekama detali rizikos analizė, o likusioms sistemoms taikomas pagrindinis požiūris. Po aukšto rizikos lygio sistemų detalios turto, grėsmių ir pažeidžiamumų analizės atliekama išsami rizikos analizė, palengvinanti parinkti efektyvias, atitinkančias įvertintas rizikas apsaugos priemones. Naudojant šį variantą, rizikos valdymo procesas koncentruojamas ten, kur yra reikšmingiausios rizikos ar didžiausi poreikiai, o visa programa tampa laiko ir išlaidų požiūriu efektyvesnė.

Įvertinus rizikas, kiekvienai IT sistemai nustatomos atitinkamos apsaugos priemonės, mažinančios rizikas iki priimtino lygio. Šios apsaugos priemonės įdiegiamos, kaip numatyta IT saugumo plane. Įdiegimas turi būti pagrįstas saugumo įsisąmoninimo ir įgūdžių lavinimo programa, kuri yra svarbi efektyviam apsaugos priemonių funkcionavimui.

IT saugumo valdymas apima nuolatinės priežiūros veiksmus, kurie gali pakeisti ankstesnius rezultatus ir sprendimus. Priežiūros veiksmai yra šie: palaikymas, saugumo tinkamumo tikrinimas, pokyčių valdymas, stebėjimas ir reagavimas į incidentus.

1. Organizacijos informacijos saugumo politika

Nagrinėjant informacijos saugumo planavimą IT saugumo politika buvo tik paminėta. Šiame skirsnyje autorė šį būtiną informacijos saugumo valdymui dokumentą aptars plačiau. Nustačius IT saugumo tikslus ir numačius bei suderinus su vadovybe jų įgyvendinimo strategiją, formuojama IT saugumo politika, kuri įforminama, kaip saugos dokumentas ir tvirtinama organizacijos vadovybės. Dokumentą rengia arba koordinuoja jo parengimą bei aprobavimą nuolatinis Saugos administravimo komitetas. Politikos išplėtojimui ir efektyviam įgyvendinimui reikalinga visų organizacijos grandžių vadovybės parama ir supratimas.

Bendrojoje IT saugumo politikoje būtinai turi būti nusakyti šie dalykai:

- taikymo sritis ir paskirtis;
- saugumo tikslai, atsižvelgiant į teisinius įsipareigojimus bei veiklos tikslus;
- IT saugumo organizacija ir infrastruktūra;
- organizacijos priimtas rizikos valdymo požiūris;
- organizacijos informacijos apžvalga, vertės ir jautrumo lygiai;
- grėsmių, pažeidžiamumų ir rizikų apžvalga, siekiamas liekamųjų rizikų lygis;
- visos bendrosios naudojimosi kontrolės taisyklės (loginė kontrolė, taip pat fizinė naudojimosi pastatais, kabinetais, sistemomis bei informacija kontrolė);
- organizacijos požiūris į saugumo įsisąmoninimą ir įgūdžių lavinimą;
- bendros saugumo tikrinimo ir palaikymo procedūros;
- bendri personalo saugumo klausimai;
- priemonės, kuriomis atitinkami asmenys informuojami apie saugumo politiką;
- veiklos tolydumas, atsitiktinumų planavimas ir padėties atkūrimas;
- politika išorinių šaltinių atžvilgiu;
- politikos peržiūrėjimo aplinkybės;
- politikos pokyčių kontroliavimo metodai;
- požiūris į priežiūros veiksmus: saugumo tinkamumo tikrinimas, apsaugos priemonių stebėjimas, reagavimas į su saugumu susijusius incidentus, IT sistemos veikimo stebėjimą.

Atsižvelgiant į saugumo tikslus ir šiems tikslams pasiekti organizacijos priimtą strategiją, pasirenkamas atitinkamas IT saugumo politikos detalumo lygis.

Saugos politikos dokumente naudojami terminai: saugos politika, standartai, procedūros ir nuorodos. Toliau nurodysime jų formuluotes ir ryšį tarp jų.

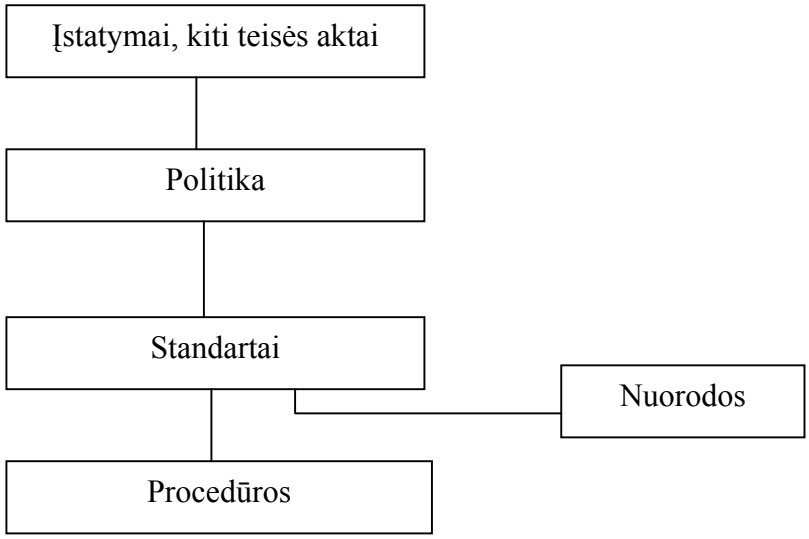
Saugos politika yra aukšto lygio organizacijos įsitikinimų, tikslų ir siekių formuluotė, politikos formuluotė turi būti glausta ir aiški, susidedanti iš formuluočių apie:

- informacijos saugumo reikalavimus organizacijoje;
- kontrolės mechanizmus, reikalingus informacijai saugoti;
- visų darbuotojų atsakomybę už informacijos saugumą;
- kas yra atsakingas už konkrečią informacijos saugumo sritį;
- numatomas pasekmes ir elgesį.

Saugos politika nėra konkretus ir išsamus tam tikro klausimo ir visų etapų, reikalingų taikant šią politiką, aprašymas. Technologijas ir metodus, reikalingus IT sistemoms apsaugoti nurodo **saugos standartai**.

Saugos procedūros paprastai padeda laikytis taikomos politikos ir standartų. Tai yra smulkiai nurodyti veiksmai, kuriuos turi atlikti IT sistemos vartotojai, administratoriai ar kiti asmenys, siekdami įvykdyti tam tikrą užduotį.

Saugos nuorodomis stengiamasi pateikti alternatyvas ir pasiūlymus, kaip padidinti saugos kontrolės lygį, kai tai yra reikalinga. Standartų laikytis yra privaloma, nuorodos yra tik pasiūlymai. Kiekvienas turi spręsti pats, ar jam jų laikytis.



6 schema. Tarpusavio ryšys

Toliau dar didesnio aiškumo dėlei pateiksime pavyzdžius.

1 lentelė. Politikos, standartų, procedūrų ir nuorodų pavyzdžiai

Dokumentas	***Formuluotė***
Politika	Darbuotojai gali naudotis elektroniniu paštu, kuris bus kontroliuojamas. Internetu naudotis galima tik darbo reikalais.

Standartai	Elektroninio pašto vartotojo programa – EXCHANGE. Interneto naršyklė – NETSCAPE. Visas išsiunčiamas paštas koduojamas algoritmu RC4.
Procedūros	Leidžiamos naudotis interneto svetainės nurodytos specialiame sąraše. Visas gaunamas paštas tikrinamas dėl virusų. Draudžiami gautų laiškų priedai su failų plėtiniais EXE.
Nuoroda	Vartotojas jam skirtą pašto dėžutę išvalo ne rečiau, kaip kartą per savaitę.

Saugos politika pagal organizacijos poreikį gali būti suskirstyta į atskirus politikos komponentus, kurie taip pat turi savo formuluotes ir rekomendacijas, pagrįstas veiklos standartais bei plačiai paplitusiais geriausio praktinio taikymo pavyzdžiais. Siūloma tokia saugos politikos komponentų struktūra:

- politikos formuluotė – trumpas politikos tam komponentui išdėstymas;
- politikos tikslas;
- politikos apimtis (ribos, kam politika taikoma);
- politikos laikymasis (aprašomi konkretūs bendrieji kontrolės mechanizmai ar elgesio variantai, taikomi siekiant laikytis politikos);
- politikos nesilaikymo pasekmės, skiriami nusižengimo lygiai.

Už konkrečius nusižengimo lygius skiriamos nuobaudos. Siūlomos nuobaudos:

- pirmo lygio nusižengimas – pažeidėjas informuojamas apie politikos nesilaikymą ir perspėjamas;
- antro lygio nusižengimas – pažeidėjas gauna papeikimą;
- trečio lygio nusižengimas – pažeidėjui taikomos sankcijos (pvz., perkėlimas į žemesnes, mažiau apmokamas pareigas);
- ketvirto lygio nusižengimas – pažeidėjas atleidžiamas iš darbo.

Pateiksime kelis tokių saugos politikos komponentų pavyzdžius.

PAŠALINIŲ ASMENŲ PRIEIGA.

Politikos formuluotė. Turi būti griežtai kontroliuojama pašalinių asmenų prieiga prie IT sistemų. Turi būti įvertinta rizika, siekiant nustatyti, kokių reikia imtis saugos priemonių ir tinkamų kontrolės mechanizmų.

Tikslas. Nesant tinkamos pašalinių asmenų prieigos prie IT sistemų kontrolės, visa informacinė infrastruktūra yra neapsaugota nuo piktnaudžiavimo. Būtina įvykdyti rizikos įvertinimą, siekiant nustatyti riziką ir saugos valdymo mechanizmus, kurie yra reikalingi tokiai kontrolei.

Apimtis:

- samdytiems iš pašalės techninės ir programinės įrangos priežiūros darbuotojams;

- valymo, maitinimo, apsaugos ir kitų įmonių teikiamų paslaugų personalui;
- studentams praktikantams ir kitiems trumpam laikui paskirtiems darbuotojams;
- konsultantams ir rangovams.

Politikos laikymasis. Prieiga prie fizinių įrenginių, loginė prieiga prie informacinių sistemų ir tinklų bus griežtai kontroliuojama. Tai apima šiuos dalykus:

- pašalinių asmenų logines užklausas turi apdoroti nuoseklus ir audituojamas procesas;
- pašalinių asmenų prieiga turi būti leidžiama tik tuo atveju, kai yra pagrįstas veiklos poreikis ir galima susidoroti su rizika, nustatyta rizikos įvertinimo metu;
- visi pašaliniai asmenys turi būti pasirašę sutartis su organizacija, užtikrinančias saugos politikos ir standartų laikymąsi;
- jei reikia, prieš pasirašant sutartį pašaliniai asmenys turi įrodyti, kad gali užtikrinti saugos politikos laikymąsi;
- nuolatinio Saugos administravimo komiteto kontroliuojama saugos darbo grupė arba rangovas turi atlikti rizikos įvertinimą, kad būtų nustatytos saugos priemonės ir nurodyti tinkami kontrolės mechanizmai, padedantys susidoroti su nustatyta rizika.

Politikos nesilaikymo pasekmės:

- prieigos suteikimas pašaliniam asmeniui be atitinkamo įgaliojimo yra antro lygio nusižengimas, jei nusižengiama pirmą kartą;
- jeigu organizacijoje nėra atliktas pašalinių asmenų prieigos rizikos įvertinimas ir kilo nenumatytas incidentas, laikoma, kad Komitetas neatlieka savo pareigų.

PRIEIGA IŠ TINKLO IŠORĖS

Politikos formuluotė. Turi būti imtasi tinkamų ir nuoseklių saugumo priemonių leidžiant prieigą fiziniams ir juridiniams asmenims iš kitų, organizacijos tinklo atžvilgiu išorinių, vietų.

Tikslas. Būtina kontroliuoti užklausas, siekiančias prieigos prie organizacijos tinklo sistemų iš išorinių vietų. Tai gali būti užklausos iš darbuotojų namų, mobiliųjų įrenginių, kitų organizacijų, rangovų darbo vietų ar kitų vietų, nepriklausančių organizacijos tinklui. Šie prisijungimai neturi kelti pavojaus organizacijos IT sistemų saugumui.

Apimtis. Prieiga iš tinklo išorės vadinama prieiga iš vietų, kurių neaptarnauja organizacijos tinklas. Tai gali būti pavieniai prisijungimai per modemą, kitos organizacijos tinklo ryšys, virtualus asmeninis tinklas ir visi kiti tokio pobūdžio ryšiai, inicijuojami ne iš organizacijos tinklo.

Politikos laikymasis. Prieiga prie organizacijos tinklo iš jam nepriklausančių vietų bus griežtai kontroliuojama saugos priemonėmis. Tai apima šiuos dalykus:

- visą prieigą iš tinklo išorės turi apdoroti nuoseklus ir audituojamas procesas;

- prieigai iš tinklo išorės tikrinti turi būti naudojami griežti autentiškumo nustatymo metodai;
- tarptinkliniai sujungimai su išoriniais, organizacijai nepriklausančiais tinklais, turi būti griežtai kontroliuojami, siekiant apriboti prieigą prie konkrečių funkcijų ir informacijos;
- visą prieigą iš tinklo išorės turi kontroliuoti ir valdyti Komiteto paskirtas informacijos saugos administratorius (-ai) ir programinė įranga;
- organizacijos tinklą draudžiama naudoti kaip tarpinį tinklą kitiems dviems išoriniams tinklams sujungti;
- turi būti parengtas standartizuotas prašymas prieigai iš tinklo išorės;
- turi būti vykdomas prieigos iš tinklo išorės stebėjimas, naudojamas potencialiam piktnaudžiavimui aptikti;
- prieigos iš tinklo išorės reikalavimai turi būti reguliariai peržiūrimi ir patikrinami, ar jie pakankamai aktualūs;
- ne visiškai atitinkantys pasikeitusias aplinkybes ar sutartis reikalavimai turi būti atnaujinami.

Politikos nesilaikymo pasekmės:

- prisijungimas prie organizacijos tinklo be atitinkamo leidimo yra antro lygio nusižengimas, jei nusižengiama pirmą kartą;
- administratoriai, prijungę organizacijai nepriklausančius asmenis ar kitas organizacijas prie organizacijos tinklo be atitinkamo įgaliojimo ir dokumentacijos, padaro antro lygio nusižengimą, jei nusižengiama pirmą kartą;
- naudojimasis kitų asmenų slaptažodžiais, slaptažodžių generatoriais ir kitomis prieigos iš tinklo išorės priemonėmis ne darbo tikslais arba tyčinis prieigos iš tinklo išorės priemonių suteikimas kitam asmeniui kvalifikuojamas kaip antro lygio nusižengimas, jei nusižengiama pirmą kartą;
- visi mėginimai įsilaužti ar apeiti organizacijos prieigos iš tinklo išorės saugos priemones kvalifikuojami kaip ketvirto lygio nusižengimas.

ORGANIZACIJOS TINKLO PRIEIGA

Politikos formuluotė. Turi būti imtasi tinkamų ir nuoseklių saugumo priemonių leidžiant prieigą prie visų organizacijos tinklo komponentų ir sistemų iš kitų prie šio tinklo prijungtų vietų.

Tikslas. Organizacijos tinklas sujungia visus organizacijos padalinius ir įgalina naudotis visa informacija. Bet kokia prieiga prie tinklo turi būti kontroliuojama, o visiems asmenims, besinaudojantiems šiuo tinklu, turi būti leidžiama pasiekti tik tą informaciją, kuria jie turi teisę

naudotis. Visa įranga gali būti jungiama prie tinklo tik gavus atitinkamą įgaliojimą. Savavališkai prijungta prie organizacijos tinklo įranga gali būti panaudota stebėti tinklo darbą ir rinkti slaptą informaciją.

Apimtis. Ši politika apima visų įrenginių fizinį ryšį su organizacijos tinklu ir prieigos teisių suteikimą asmenims, kurie kreipiasi į tinklą iš tiesiogiai prie šio tinklo prijungtų vietų. Tai negali būti nuotoliniai ryšiai komutuojama linija, virtualus asmeninis tinklas ir visi kiti tokio pobūdžio ryšiai.

Politikos laikymasis. Prieigos prie organizacijos tinklo valdymas privalo turėti šias savybes:

- prie tinklo be tam tikrų įgaliojimų negalima prijungti jokios įrangos;
- privaloma nustatyti slaptažodžių kūrimo standartus ir užtikrinti jų taikymą;
- vartotojams turi būti leidžiama pasiekti tik tą informaciją, kuriai jie turi teises;
- vartotojo prieigos teisės turi būti reguliariai peržiūrimos;
- vartotojų registracijos sąrašas turi būti periodiškai atnaujinamas;
- reikia laikytis standartų, skiriant pagrindinio administratoriaus (*root*) teises, tokia teisė turi būti suteikiama tik ribotam laikui;
- visi vartotojo statuso pasikeitimai turi tuoj pat atsispindėti jo prieigos teisėse;
- visi vartotojai turi būti registruojami tik pagal nuoseklią ir audituojamą procedūrą.

Politikos nesilaikymo pasekmės:

- neteisėtas įrangos prijungimas prie organizacijos tinklo yra kvalifikuojamas kaip pirmo lygio nusižengimas, jei nusižengiama pirmą kartą;
- politikos ir procedūrų, susijusių su *root* administratoriaus teisių suteikimu, nesilaikymas kvalifikuojamas kaip antro lygio nusižengimas, jei nusižengiama pirmą kartą;
- neteisėta prieiga prie organizacijos tinklo yra saugos įvykis, apie kurį privalu pranešti IT saugos administratoriui arba tiesioginiam vadovui, net jei tai atsitiko netyčia;
- tyčinės pastangos neleistinai gauti prieigą prie informacijos kvalifikuojamos kaip trečio lygio nusižengimas.

FIZINĖ SAUGA

Politikos formuluotė. Informacija turi būti fiziškai apsaugota nuo pažeidimų ar atskleidimo tais būdais, kurie atitinka jos slaptumo kategoriją.

Tikslas. Fizinės vietos, kur laikoma ar pasiekiama informacija turi būti apsaugotos tokiais būdais, kurie atitinka jos slaptumo kategoriją. Kompiuteriai, kuriuose elektroniniu pavidalu laikoma informacija, turi būti fiziškai pasiekiami tik įgaliotiems asmenims. Informacija, laikoma

kitomis formomis, pavyzdžiui, popieriuje, turi būti apsaugota nuo nesankcionuotos prieigos ir tokių pavojų, kaip gaisro, vandens ar pastato sugriuvimo.

Apimtis. Ši politika apima visas vietas, kuriose laikoma ar pasiekiama viešai nepriskirtina informacija.

Politikos laikymasis. Toliau pateikiami minimalūs reikalavimai fizinei informacijos saugai:

- IT sistemų darbo stotys (serveriai), kuriuose laikoma viešai nepriskirtina informacija, turi būti rakinamose patalpose, apsaugotose prieigos kontrolės sistemomis, praleidžiančiomis tik įgaliotus asmenis;
- informacija, laikoma popieriuje ir kitose materialiose laikmenose, turi būti laikoma vietose, į kurias gali įeiti tik įgalioti asmenys, ir jos po darbo valandų turi būti užrakinamos;
- atsarginių kopijų laikmenos turi būti archyvuojamos atskiroje saugioje vietoje;
- turi būti imtasi priimtinų apdairumo priemonių, siekiant išvengti žalos dėl gaisro, vandens, neteisėto įrangos ar informacijos pašalinimo, elektros dingimo;
- tinklo įranga ir kabeliai turi būti apsaugoti nuo nesankcionuotos prieigos;
- personaliniai kompiuteriai, kuriuose laikoma ar iš kurių pasiekiama viešai nepriskirtina informacija, juos įjungiant turi tikrinti vartotojo autentiškumą (pvz., per įkrovos slaptažodį) bei naudotų ekrano užsklandą, automatinį išsiregistravimą ar kitokius mechanizmus, kai kompiuteris trumpam laikui paliekamas be priežiūros;
- vietos, kurioje laikoma slapta informacija turi būti fiziškai atskirtos nuo viešai prieinamų vietų.

Politikos nesilaikymo pasekmės:

- darbuotojai, kurie neužtikrina, kad jų darbo vietos atitiktų šios politikos reikalavimus kvalifikuojami kaip įvykdę pirmo lygio nusižengimą.

PAREIGŲ ATSKYRIMAS

Politikos formuluotė. Saugos administravimo funkcijos turi būti atskirtos nuo sistemos plėtros ar kitų operacijų valdymo. Visi saugos administravimo procesai, turi būti suprojektuoti taip, kad joks pavienis asmuo negalėtų sukelti pavojaus saugos kontrolei.

Tikslas. Pareigų atskyrimas – tai principas, pagal kurį susijusių užduočių dalys paskiriamos vykdyti skirtingiems asmenims, kad nė vienas asmuo nevaldytų visų saugos komponentų ir negalėtų susilpninti saugos kontrolės.

Apimtis. Ši politika apima visus informacijos saugos kontrolės mechanizmus ir asmenis, susijusius su šių mechanizmų administravimu.

Politikos laikymasis. Informacijos saugos kontrolės mechanizmai, pvz., ugniasienės, įsibrovimo aptikimo sistemos, rizikos valdymo procesas, saugos principų įsisavinimo procesas ir kitos valdymo priemonės turi būti atskirtos nuo kitų funkcijų, pvz., programinės įrangos kūrimo, operacijų ir sistemų administravimo. Tai reiškia, kad asmenys, valdantys informacijos saugos kontrolės mechanizmus, ir asmenys, atliekantys kitas funkcijas, tokias kaip programinės įrangos kūrimas ar administravimas, turi būti skirtingi ir pavaldūs skirtingiems vadovams.

Politikos nesilaikymo pasekmės:

- jei asmuo nesilaiko procesų ar procedūrų, skirtų užtikrinti pareigų atskyrimą, tai kvalifikuojama kaip antro lygio nusižengimas;
- nuolatinio Saugos administravimo komiteto kontroliuojama saugos darbo grupė labai netinkamai atlieka savo pareigas, jei nėra sukurtos procedūros, užtikrinančios šios politikos vykdymą.

APSAUGA NUO KENKĖJIŠKOS PROGRAMINĖS ĮRANGOS

Politikos formuluotė. Turi būti taikomos apsauginės priemonės, skirtos aptikti kenkėjiškos programinės įrangos įsibrovimą ir apsisaugoti nuo jo. Visuose personaliniuose kompiuteriuose, prieš juos pajungiant prie organizacijos tinklo, turi būti įdiegta antivirusinė programinė įranga; virusų atpažinimo failai turi būti reguliariai atnaujinami; turi būti tikrinami serveriai, personaliniai ir nešiojami kompiuteriai; vartotojai neturi tyčia kurti, vykdyti, persiųsti ar įvesti save replikuojančio programinio kodo, sukurto daugintis, kenkti ar kitaip trukdyti kurio nors kompiuterio atminties, saugojimo, operacinės sistemos ar programinės įrangos darbui.

Tikslas. Apsauginės priemonės yra būtinos, siekiant apsisaugoti ir aptikti kenkėjiškos programinės įrangos įsibrovimą. Programinė įranga ir informacijos apdorojimo priemonės yra lengvai pažeidžiamos kenkėjiškos programinės įrangos, tokios kaip, kompiuteriniai virusai, tinklo „kirminai“, „Trojos arkliai“ ir loginės „bombos“. Vartotojus reikia supažindinti su pavojais, kuriuos kelia nelegali ar kenkėjiška programinė įranga. Reikia imtis apsaugos priemonių kompiuteriniams virusams personaliniuose kompiuteriuose aptikti ir nuo jų apsisaugoti.

Apimtis. Ši politika apima visą organizaciją.

Politikos laikymasis. Apsauga nuo kenkėjiškos programinės įrangos apima šiuos reikalavimus:

- turi būti laikomasi Keitimų valdymo proceso procedūrų (apie Keitimų valdymo procesą kalbėsime toliau), negalima diegti nelegalios programinės įrangos;
- turi būti įdiegta ir reguliariai atnaujinama antivirusinė programinė įranga;
- turi būti reguliariai peržiūrima programinė įranga ir duomenų turinys kritiškose organizacijos veiklai sistemose;

- turi būti tikrinami visi elektroniniai laiškai;
- visi darbuotojai turi būti išmokyti apsisaugoti nuo kompiuterinių virusų;
- turi būti laikomasi veiklos tolydumo plano, atkuriant sistemas po virusų atakos;
- turi būti užtikrinama, kad tikriems virusams nuo melagingų pranešimų apie virusus atskirti būtų naudojamasi tinkamais šaltiniais: patikimais žurnalais, patikimomis interneto svetainėmis ar antivirusinės programinės įrangos tiekėjais.

Politikos nesilaikymo pasekmės:

- informacijos saugos reikalavimų nesilaikymas bet kurios aukščiau minėtos veiklos metu yra kvalifikuojamas kaip pirmo lygio nusižengimas, išskyrus atvejus, kai pažeidžiamas įstatymas, tuomet baudžiama įstatymo numatyta tvarka.

ELEKTRONINIO PAŠTO SAUGA

Politikos formuluotė. Elektroninis paštas turi būti naudojamas tik darbo tikslais.

Tikslas. Elektroninis paštas yra veiklai gyvybiškai svarbi paslauga, todėl siekiama paaiškinti, kokie yra reikalavimai jo naudojimui.

Apimtis. Ši politika apima visą organizaciją.

Politikos laikymasis. Elektroninio pašto vartotojai turi žinoti šiuos reikalavimus ir laikytis jų:

- visi elektroniniai laiškai, siunčiami ir gaunami organizacijos elektroninio pašto sistema yra laikomi organizacijos dokumentais, gali būti peržiūrėti ir atskleisti bet kokiu tikslu, įskaitant jų atskleidimą teisėsaugos institucijoms;
- elektroninio pašto laiškai yra saugomi organizacijos tvarka nustatytą laiką;
- grasinančių, nepadorių ar kitokių visuotinai nepriimtinų laiškų siuntimas kvalifikuojamas kaip sunkus piktnaudžiavimas elektroninio pašto sistema;
- elektroninio pašto sistemos vartotojai privalo visada tinkamai identifikuoti save ir niekada neapsimesti kitu vartotoju;
- visi elektroninio pašto laiškai, ateinantys iš organizacijos tinklo išorės, turi būti tikrinami dėl kenkėjiškos programinės įrangos;
- darbuotojai neregistruojami elektroninio pašto vartotojais, jei jie nesusipažino su šiais reikalavimais ir raštu nepasižadėjo jų laikytis.

Politikos nesilaikymo pasekmės:

- toliau nurodomi pažeidimai kvalifikuojami kaip pirmo lygio nusižengimai, jei nusižengiama pirmą kartą: intensyvus naudojimas asmeniniais reikalais, nemandagių laiškų siuntimas;

- apsimetimas kitu vartotoju kvalifikuojamas kaip antro lygio nusižengimas, jei nusižengiama pirmą kartą. Pakartotinis apsimetimas jau kvalifikuojamas ne mažesniu kaip trečio lygio nusižengimu;
- viešai nepriskirtinos informacijos siuntimas už organizacijos ribų priklauso nuo siųstos informacijos slaptumo lygio. Kai kuriais atvejais tai gali būti įstatymo pažeidimas ir tuomet už tai baudžiama, kaip už nusikaltimą.

SLAPTAŽODŽIŲ VALDYMAS

Politikos formuluotė. Prieigai prie organizacijos IT sistemų kontroliuoti turi būti taikoma slaptažodžių valdymo programa.

Tikslas. Slaptažodžiai yra vienas iš pagrindinių priemonių vartotojo įgaliojimui naudotis kuria nors IT sistema patikrinti. Slaptažodžių tvarkymo sistemos turi suteikti efektyvias, dialogines priemones, užtikrinančias, kad naudojami tinkami slaptažodžiai.

Apimtis. Ši politika taikoma visoms organizacijos IT sistemoms.

Politikos laikymasis. Slaptažodžių valdymo procesas turi apimti šiuos reikalavimus:

- turi būti naudojami asmeniniai slaptažodžiai;
- leisti vartotojams pasirinkti ir keisti savo slaptažodžius bei naudoti patvirtinimo procedūrą;
- kur reikia, nustatyti priverstinį laikinų slaptažodžių pasikeitimą pirmojo registravimosi sistemoje metu;
- sudaryti ankstesnių slaptažodžių sąrašą ir neleisti jų naudoti pakartotinai;
- laikyti užšifruotus slaptažodžių failus atskirai nuo taikomosios programinės įrangos;
- programinės įrangos tiekėjo slaptažodžius pakeisti iškart po jos įdiegimo;
- turi būti sukurti tinkamų slaptažodžių ir slaptažodžių apdorojimo standartai.

Vartotojas privalo:

- užtikrinti slaptažodžių slaptumą;
- neužrašinėti slaptažodžių ant popieriaus, jei negali jo saugiai laikyti;
- keisti slaptažodžius visais atvejais, kai yra bet kokių požymių, kad nukentėjo sistemos ar slaptažodžių saugumas;
- pasirinkti tinkamus slaptažodžius pagal esamus standartus ir laikytis elgesio su jais taisyklių;
- keisti slaptažodžius po tam tikro laikotarpio ir nenaudoti senų;
- keisti laikinuosius slaptažodžius pirmojo registravimosi metu;
- neįtraukti slaptažodžių į automatinio registravimosi procesus, pvz., į makrokomandas ar funkcinį klavišą;

- bendrai nenaudoti asmeninių slaptažodžių.

Politikos nesilaikymo pasekmės:

- netinkamo slaptažodžio pasirinkimas ar elgesio su juo taisyklių pažeidimas yra kvalifikuojamas kaip pirmo lygio nusižengimas, jei nusižengiama pirmą kartą;
- slaptažodžio atskleidimas kitiems asmenims yra kvalifikuojamas kaip antro lygio nusižengimas, jei nusižengiama pirmą kartą.

Susipažinus su atskiromis saugumo sritimis, kaip prieiga prie organizacijos tinklo, fizinė sauga, personalo sauga ir kt. galima daryti išvadą, kad informacijos saugumo politika arba nuostatai – tai taisyklių, standartų, praktinio pritaikymo pavyzdžių rinkinys, reguliuojantis, kaip organizacija valdo, apsaugo ir skirsto jai priklausančią informaciją.

2. Organizacijos informacijos saugumo rizikos analizė

Prieš pradedant bet kokius rizikos analizės veiksmus, organizacija turi turėti šios analizės strategiją, kurios sudedamosios dalys (būdai, metodai ir kt.) turi būti įformintos dokumentais, kurie turi būti nurodyti IT saugumo politikoje. Organizacijoje turi būti susitarta dėl rizikos analizės metodo parinkimo priemonių ir kriterijų. Rizikos analizė turi garantuoti, kad pasirinktas požiūris tinka aplinkai ir sutelkia pastangas ten, kur jos iš tiesų reikalingos. Kadangi paprastai būna per brangu atlikti detalią visų IT sistemų rizikos analizę, taip pat neefektyvu skirti mažai dėmesio rimtoms grėsmėms, reikalinga pusiausvyra tarp šių variantų. Bendro lygio analizė, derinant ją su pagrindiniu požiūriu ir, kur reikia, su išsamia rizikos analize, daugumai organizacijų yra efektyviausias kelias. Apie tai jau buvo kalbėta IV skyriaus 3 skirsnyje „Planavimo procesas“.

Iš pradžių reikia atlikti pradinę bendro lygio rizikos analizę, kad būtų nustatyta, koks požiūris (pagrindinis ar išsami rizikos analizė) yra tinkamas kiekvienai IT sistemai. Per šią bendro lygio analizę nustatoma, kokią reikšmę IT sistemos ir jomis apdorojama informacija turi veiklai, taip pat nagrinėjamos rizikos organizacijos veiklos atžvilgiu. Pagrindas sprendimui dėl to, koks požiūris tinkamas kiekvienai IT sistemai, gali būti sudaromas nagrinėjant šiuos klausimus:

- veiklos tikslus, kuriuos, naudojant IT sistemą, reikia pasiekti;
- organizacijos veiklos priklausomumo nuo IT sistemų laipsnį, t.y., ar funkcijos, kurios yra iš esmės svarbios organizacijos efektyvios veiklos tąsai, priklauso nuo šių sistemų arba šiomis sistemomis apdorojamos informacijos slaptumo, vientisumo, prieinamumo, atsakingumo, tapatumo ir patikimumo;
- investicijų į IT sistemas lygį, plėtojimo, palaikymo ar sistemų pakeitimo terminais;

- IT sistemų turtą, kuris yra labai reikšmingas organizacijai.

Kai šie klausimai išnagrinėjami, priimti sprendimus paprastai būna lengva. Jeigu sistema yra svarbi organizacijos veiklai, jei sistemos pakeitimas daug kainuoja, arba jei turto atžvilgiu egzistuoja didelės rizikos, tai sistemai reikalinga išsami rizikos analizė.

Pagrindinės apsaugos tikslas yra įdiegti mažiausiai apsaugos priemonių visoms organizacijos IT sistemoms apsaugoti. Pagrindinio požiūrio taikymas sumažina organizacijos investicijas, reikalingas rizikos analizės apžvalgoms daryti. Atitinkamą pagrindinę apsaugą galima įdiegti naudojant apsaugos priemonių katalogus, kuriuose siūlomos IT sistemų apsaugos nuo pagrindinių grėsmių priemonės. Detalus grėsmių, pažeidžiamumų ir rizikų įvertinimas nėra būtinas.

Pagrindiniuose kataloguose gali būti išsamiai aprašytos apsaugos priemonės arba gali būti nusakytas saugumo reikalavimų rinkinys, susijęs su sistemai tinkama apsaugos priemone. Abu atvejai turi savų pranašumų. Abiejų rūšių katalogų galima rasti ISO/IEC TR 13335-4 prieduose. Vienas iš pagrindinio požiūrio tikslų – apsaugos priemonių suderinamumas organizacijos mastu; jį galima pasiekti abiem būdais.

Organizacija gali sudaryti savo pagrindinį požiūrį, derantį su jos tipine aplinka, derantį su jos aplinka ir jos veiklos tikslais.

Išsami reikalingų IT sistemų analizė apima su sistema susijusių rizikų nustatymą ir jų dydžių įvertinimą. Išsamios rizikos įvertinimo poreikis gali būti nustatomas be būtinų laiko ir piniginių sąnaudų, kai daromos visų sistemų bendro lygio apžvalgos, po to atliekant didelės rizikos arba veiklai iš esmės svarbių sistemų išsamią rizikos analizę.

Rizikos analizės metu nustatomi veiklai potencialiai žalingi nepageidaujamų įvykių poveikiai ir šių įvykių tikėtinumas. Nepageidaujami įvykiai gali padaryti žalos veiklai, darbuotojams arba kitam organizacijos turtui. Žalingas nepageidaujamo įvykio poveikis yra apibūdinamas galimomis žalomis turtui, su kuriuo susijusi rizika. Įvykio tikėtinumas priklauso nuo to, kiek turtas yra patrauklus potencialiam atakos šaltiniui, nuo grėsmių tikėtinumo ir nuo to, ar lengva pasinaudoti pažeidžiamumais. Rizikos analizės rezultatais remiamasi nustatant ir parenkant apsaugos priemones, kurias galima naudoti nustatytoms rizikoms sumažinti iki priimtino lygio.

Yra daug rizikos analizės atlikimo būdų: ir naudojant tikrinimo sąrašus, ir taikant struktūrine analize paremtus metodus. Gali būti naudojamos ir automatinės (naudojančios kompiuterius), ir žmonių rankomis valdomos priemonės. Svarbu, kad taikomi metodai būtų priimtini organizacijai. Iš kitos pusės, pirmą kartą atlikus išsamią sistemų rizikos analizę, apžvalgos rezultatai – turtas ir jo reikšmė, rizikos, pažeidžiamumai ir rizikos lygiai bei nustatytos apsaugos priemonės – turi būti išsaugoti duomenų bazėje. Akivaizdu, kad tai paprasčiau padaryti naudojantis metodais, paremtais programine įranga. Rezultatų vaizdavimas, kartais vadinamas

modeliu, gali būti efektyviai naudojamas, kai laikui bėgant įvyksta konfigūracijos, apdorojamos informacijos rūšies, grėsmių scenarijaus ir kiti pokyčiai. Kad būtų galima nustatyti poveikį būtinoms apsaugos priemonėms pakanka įvesti tik šiuos pokyčius. Be to, šie modeliai greitai gali būti panaudoti skirtingiems variantams nagrinėti, plėtojant naujas sistemas, taip pat naudojami kitoms panašioms sistemoms.

Kaip jau buvo nagrinėta šio darbo I skyriuje, organizacijoje turi būti išsiaiškinta, kas joje yra laikoma informacija, kokios yra jos slaptumo kategorijos (kaip ji gali būti klasifikuojama), koks kitas turtas (be informacijos) yra susijęs su organizacijos IT sistemomis, jo įvertinimas ir jo rūšių priklausomybės nustatymas. Toliau sektų grėsmių, pažeidžiamumų ir rizikų įvertinimas.

GRĖSMIŲ ĮVERTINIMAS. Grėsmė gali potencialiai padaryti žalos IT sistemoms ir įvertintam turtui. Grėsmių šaltinis gali būti žmonės arba gamta, grėsmės gali būti atsitiktinės ar tyčinės. Reikia nustatyti tiek atsitiktinių, tiek tyčinių grėsmių šaltinius ir įvertinti jų tikėtinumą.

Duomenys grėsmėms įvertinti turi būti gaunami iš turto savininkų ar vartotojų, personalo, įrenginių planavimo ir IT specialistų, taip pat iš žmonių, atsakingų už organizacijos apsaugą. Grėsmių vertinimui galima pasinaudoti grėsmių sąrašu, pateiktu ISO/IEC TR 13335-3 C priede.

Autorės nagrinėjamoje organizacijoje grėsmių vertinimui pasiūlyta atsižvelgti į tokias galimų grėsmių šaltinių rūšis:

- pavienius nusikaltimus;
- organizuotus nusikaltimus;
- įsilaužimus elektroninėmis priemonėmis;
- specialiųjų interesų grupes;
- vidinius vartotojus;
- pašalinius asmenis;
- privilegijuotus vartotojus;
- IT sistemų ir tinklo administratorius.

Nustatytos grėsmės, kurias gali sukelti šie grėsmės šaltiniai:

- slaptas komunikacijų tinklų informacijos (elektroninių laiškų, vartotojų identifikatorių, slaptažodžių ir kt.) perėmimas;
- taikomųjų programų paslaugų neprieinamumas;
- komunikacijų paslaugų neprieinamumas (maršrutizatorių ar kitų tinklo komponentų gedimai);
- duomenų, taikomųjų programų, sistemų, tinklų vientisumo pažeidimas (dėl sistemų ar tinklo komponentų konfigūravimo klaidų arba dėl kenksmingos programinės įrangos poveikio duomenims);

- komunikacijų parametrų nesankcionuoto keitimo;
- operatorių klaidos (nerūpestingai atliktas atsarginis kopijavimas ar duomenų atkūrimas iš atsarginių kopijų, šalinant gedimus);
- kenksminga programinė įranga, pakliuvusi į vidinius tinklus bei sistemas ir kelianti pavojų sistemų bei duomenų vientisumui;
- nesankcionuotas tinklų naudojimas (pvz., darbuotojo asmeninėms reikmėms);
- nesankcionuotas prisijungimas prie sistemų su konfidencialiais duomenimis;
- naudojimasis kito vartotojo duomenimis: identifikatoriumi, slaptažodžiu ir registravimosi sistemoje ar administratoriaus teisėmis;
- vartotojų teisių padidinimas ir netinkamas jų valdymas (pvz., nėra procedūrų, kurios užtikrintų kreipimosi teisių panaikinimą pasibaigus jų galiojimo laikui.

Kiekvienos konkrečios grėsmės laipsnis vertinamas pagal jos šaltinį ir sistemą, kuriai sukeliama grėsmė. Vertinant grėsmę, jai priskiriamas vienas iš šių laipsnių:

- **Aukštas (H)**.

Šaltinis turi svarbių motyvų ir susiklosto ypač palankios aplinkybės arba svarbūs motyvai derinami su tinkama vieta bei proga ir galimybe likti neatskleistam. Tokia grėsmė labai tikėtina tam tikrais laiko tarpais. Dažniausiai tokia grėsmė pasikartoja. Jei grėsmė tyčinė, jos šaltinis turi būti ypač kompetentingas, protingas ir (arba) turėti svarbių motyvų.

- **Vidutinis (M)**.

Šaltinis turi vidutinės svarbos arba svarbių motyvų ir yra palankios aplinkybės, tačiau nepalanki vieta ir nėra palankios progos. Tokia grėsmė pakankamai tikėtina. Paprastai galimi ne daugiau kaip keli pavieniai bandymai sukelti tokią grėsmę. Kalbant apie tyčines grėsmes, paprastai jų šaltiniai būna patyrę, bet nebūtinai kvalifikuoti specialistai. Jų motyvai būna vidutinės svarbos.

- **Žemas (L)**.

Motyvai nėra labai svarbūs arba, atsiradus progai, aplinkybės būna ypač nepalankios. Tokia grėsmė nelabai tikėtina, tačiau įmanoma. Jei grėsmė tyčinė, jos šaltinis paprastai nepatyręs arba atsitiktinis ir neturi aiškių motyvų.

Grėsmės laipsniai bus naudojami toliau, vertinant rizikos veiksnius.

PAŽEIDŽIAMUMŲ ĮVERTINIMAS. Šis įvertinimas apima silpnų vietų, kuriomis gali pasinaudoti grėsmė ir padaryti žalą turtui ir veiklai, nustatymą fizinėje aplinkoje, organizacijoje, procedūrose, personale, valdyme, administravime, kompiuterinėje, programinėje ir ryšių įrangoje. Pats pažeidžiamumo buvimas nesukelia žalos; kad taip būtų, turi būti grėsmė, galinti pasinaudoti pažeidžiamumu. Jei pažeidžiamumui nėra atitinkamos grėsmės, nereikia diegti apsaugos priemonės, tačiau jis turi būti atpažintas ir stebimas, ar neįvyko pokyčių. Reikia

pažymėti, kad netinkamai įdiegta arba blogai funkcionuojanti apsaugos priemonė pati gali būti pažeidžiamumas.

Pažeidžiamumai gali būti siejami su turto savybėmis ar požymiais, kurie gali būti naudojami ne taip arba ne tuo tikslu, kaip buvo numatyta turtą perkant ar sukuriant. Duomenys pažeidžiamumams įvertinti turi būti gaunami iš turto savininkų ir vartotojų, įrenginių specialistų ir IT sistemų kompiuterinės ir programinės įrangos ekspertų. Galima pasinaudoti pažeidžiamumų pavyzdžių sąrašu, pateiktu ISO/IEC TR 13335-3 D priede.

Autorės nagrinėjamoje organizacijoje pažeidžiamumai suskirstyti į 11 grupių pagal tai, su kuo jie yra susiję:

- su technine architektūra (trūksta ugniasienių, nėra apsaugos nuo kenksmingos programinės įrangos, nepakankama konfidencialių duomenų apsauga, nesustiprinta sistemų apsauga, nepakankamai kontroliuojama prieiga iš tinklo išorės);
- su konfidencialia informacija (konfidenciali informacija įvedama nesaugomose IT sistemos srityse);
- su tinklo sauga (nepakankamas sistemų ir tinklų valdymas);
- su vartotojų identifikavimu ir jų tapatumo nustatymu (nėra slaptažodžių tvarkymo procedūrų ir nekeliama jokių reikalavimų slaptažodžių kokybei ir galiojimo laikui, slaptažodžiai perduodami elektroniniu paštu nešifruotu tekstu, nėra vartotojų valdymo iš vieno centro, kai kuriose sistemose nenustatomas vartotojų tapatumas);
- su interneto naudojimu (jungiantis per HTTP ar FTP netikrinama, ar nėra kenksmingos programinės įrangos);
- su šifravimu (nėra šifravimo standarto, konfidencialūs duomenys prieš perduodant nešifruojami);
- su programinės įrangos produktų pasirinkimu ir kūrimu (nėra su sauga susijusių nurodymų pasirenkant produkto versiją ar kategoriją, neatsižvelgiama į programinės įrangos kūrimo saugos nurodymus, kad bandomosios ir gamybinės sistemos turi būti atskirtos);
- su konfigūravimo valdymu (nėra procedūrų, kurios apibrėžtų reikalaujamą minimalų konfigūruojamų komponentų saugos lygį);
- su keitimų valdymu (nėra keitimų valdymo procedūros);
- su saugos stebėjimu (nėra ugniasienių stebėjimo procedūros, serverių sistemose neregistruojama sistemų veikla ir neanalizuojami sistemų žurnalai, trūksta globalaus ir vietinio tinklo saugos stebėjimo);

- su nepakankamu registravimu (kai kuriose sistemose neregistruojama vartotojų veikla).

Kiekvieno pažeidžiamumo laipsnis įvertinamas pagal grėsmės galimybę. Gali būti priskiriamas vienas iš šių pažeidžiamumo laipsnių:

- **Aukštas (H)**.

Apsaugos priemonės nepakankamos, norint išvengti galimos žalos. Jei kiltų grėsmė, žala tikriausiai būtų padaryta.

- **Vidutinis (M)**.

Apsaugos priemonės įgyvendintos, bet ar jos gali užtikrinti apsaugą priklauso nuo grėsmės šaltinio sugebėjimų ir motyvų. Išlieka tikimybė, kad žala gali būti padaryta.

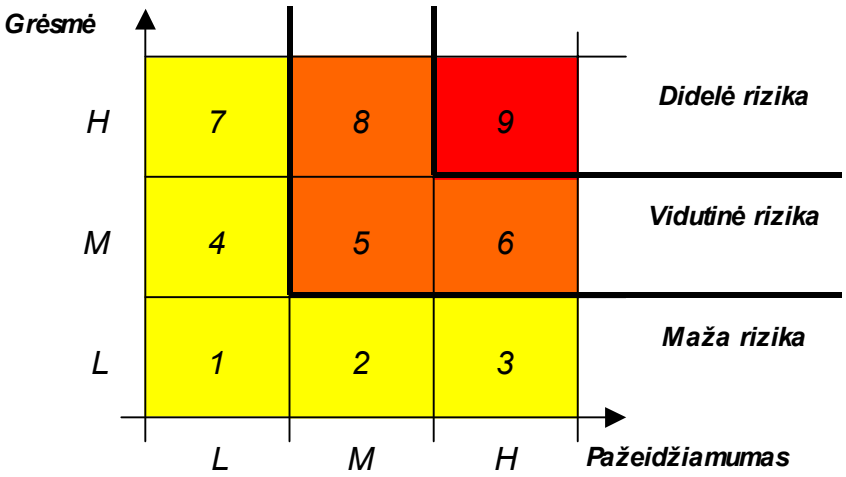
- **Žemas (L)**.

Apsaugos priemonės pakankamos, norint išvengti galimos žalos. Jei kiltų grėsmė, žala tikriausiai nebūtų padaryta..

Pažeidžiamumo laipsniai bus naudojami toliau, vertinant rizikos veiksnius.

RIZIKŲ ĮVERTINIMAS. Šio žingsnio tikslas – nustatyti ir įvertinti riziką, susijusią su IT sistemomis ir jų turtu, kad būtų galima nustatyti ir parinkti atitinkamas ir pateisintas apsaugos priemones. Rizika priklauso nuo turto reikšmingumo, grėsmių, galinčių padaryti žalingą poveikį veiklai, tikėtinumo, pasinaudojimo pažeidžiamumais paprastumo ir visų esamų ar planuotų apsaugos priemonių, galinčių sumažinti riziką.

Šiuos faktorius susieti galima įvairiais būdais. Pirmiausia įvertinamos grėsmės, kuri gali kilti sistemai, laipsnis. Paskui matuojamas sistemos pažeidžiamumas, esant grėsmei. Rizika nustatoma pagal galimos grėsmės laipsnį ir pažeidžiamumo šiai grėsmei laipsnį. Rizikos laipsnis įvertinamas pagal tokią schemą:



7 schema. Rizikos vertinimas

Galimi tokie rizikos laipsniai:

- **Aukštas (H)**.

Tai rizika, kuriai pašalinti būtina įdiegti papildomas apsaugos priemones.

- **Vidutinis (M)**.

Tai rizika, kuriai pašalinti reikalingos kokios nors apsaugos priemonės.

- **Žemas (L)**.

Tai rizikos lygis, kuris organizacijai yra priimtinas, ir apsaugos priemonės nediegiamos.

APSAUGOS PRIEMONIŲ NUSTATYMAS. Tinkamai apsaugai būtinų priemonių nustatymo pagrindas yra nustatyti rizikų laipsniai (dydžiai), jas vertinant. Vienas iš variantų gali būti pasirenkamas atsižvelgiant į apsaugos priemonių kainas. Apsaugos priemonių taikymas apima šias sritis: fizinę aplinką, personalą, administravimą, kompiuterinę ir programinę įrangą, ryšius.

Esamos ir planuotos apsaugos priemonės turi būti peržiūrimos, lyginant kaštus, įskaitant ir palaikymą bei pašalinimo galimybę arba pagerinimą, jeigu jos nėra pakankamai efektyvios. Yra daug galimybių sumažinti riziką: vengti jos, perkelti riziką apdraudžiant turtą, sumažinti grėsmes, pažeidžiamumus, sumažinti galimą poveikį, pastebėti nepageidaujamus įvykiu, reaguoti į juos, atkurti padėtį jiems įvykus. Kuri šių galimybių yra tinkamiausia, priklauso nuo aplinkybių.

Parenkant apsaugos priemones visada reikia siekti pusiausvyros tarp operacinių (netechninių) ir techninių apsaugos priemonių. Operacinės priemonės yra tos, kurios lemia fizinį, personalo ir administracijos saugumą.

Fizinis saugumas apima vidinių pastato sienų tvirtumą, durų rakinimą užraktais su kodais, ugnies gesinimo sistemas ir sargybinius. Personalo saugumas apima samdomo personalo tikrinimą (ypač toms pareigoms, kur reikalingas pasitikėjimas), personalo stebėjimą, saugumo įsisąmoninimo programas.

Procedūrinis saugumas apima saugaus operavimo procedūrų dokumentus, taikomųjų programų plėtojimo ir diegimo, taip pat reagavimo į incidentus procedūras. Dėl to labai svarbu, kad kiekvienai sistemai būtų sudaryta veiklos tąsos, apimant atsitiktinumų numatymą ir padėties po nepalankių įvykių atkūrimą, strategija ir planai. Plane turi būti išdėstytos pagrindinių funkcijų detalės ir padėties atkūrimo prioritetai, poreikiai ir organizacinės procedūros, kurias reikia atlikti, kai atsitinka nelaimė ar pertraukiamas paslaugos teikimas.

Techninis saugumas apima kompiuterinės ir programinės įrangos saugumą, taip pat ir ryšių apsaugos priemones. Šios apsaugos priemonės parenkamos atsižvelgiant į rizikas, kad būtų užtikrintas funkcionalumas ir patikimumas. Funkcionalumas aprėpia vartotojų identifikavimą ir tapatumo nustatymą, loginės priėmimo kontrolės reikalavimus, audito atlikimo, įėjimo į sistemą

saugumo poreikius, pranešimo tapatumo nustatymą, šifravimą ir taip toliau. Patikimumo reikalavimai pagrindžia pasitikėjimo saugumo funkcijomis lygį, taip pat tikrinimo apimtį ir rūšį, saugumo testavimą ir kitas priemones, reikalingas tam lygiui patvirtinti.

Parenkant apsaugos priemones tenka atsižvelgti į daugelį faktorių:

- apsaugos priemonių naudojimo paprastumą;
- suprantamumą vartotojui;
- vartotojui teikiamą pagalbą, kai jis atlieka savo funkcijas;
- atliekamų funkcijų rūšį – prevencija, sulaikymas, atskleidimas, padėties atkūrimas, korekcija, priežiūra, įsisąmoninimas.

Apskritai, apsaugos priemonė atlieka daugiau nei vieną šių funkcijų – kuo daugiau jų gali atlikti, tuo geriau. Nagrinėjant bendrąjį saugumą ar naudotinų apsaugos priemonių rinkinį, reikia palaikyti, jei įmanoma, pusiausvyrą tarp funkcijų rūšių. Tai padeda pasiekti, kad bendrasis saugumas būtų efektyvesnis ir veiksmingesnis.

Sėkmingai pasirinkus rizikos analizės strategiją, įvertinus grėsmes, pažeidžiamumus ir rizikos laipsnius, jau įdiegtas apsaugos priemones bei turimus finansinius išteklius, galima nustatyti organizacijai priimtino lygio riziką, tai mažai tikėtinų grėsmių pakankamai apsaugotoms silpnoms organizacijos vietoms tikimybė. Šis rizikos lygis turėtų būti organizacijos informacijos saugumo valdymo pagrindinis tikslas.

3. Organizacijos informacijos saugumo priežiūra

IT saugumo valdymui labai svarbu turėti gerai parengtą IT saugumo planą. Kiekvienas svarbus IT projektas negali vykti be tokio koordinuojančio ir suderinto su vadovybe ir atsakingais specialistais dokumento, o IT saugumas – tai ir yra svarbus ir didelis projektas, kurį organizacijai dažnai padeda vykdyti samdyti rangovai.

Kai IT saugumo planas pabaigiamas ir atsakingų asmenų pasirašomas, įdiegiamos apsaugos priemonės ir saugumo tinkamumas patikrinamas ir testuojamas. Saugumas turi būti testuojamas pagal saugumo testavimo planą, kuriame nurodytas testavimo būdas, grafikas ir aplinka.

Įvykdžius testavimą ir nustačius, kad rizikos sumažintos iki priimtino lygio, labai svarbu įvykdyti saugumo įsisąmoninimo programą. Šios programos tikslas – padidinti įsisąmoninimą organizacijoje iki tokio lygio, kad saugumas taptų antrąja prigimtimi, procesas taptų įprastinis ir visų darbuotojų lengvai atliekamas. Programa turi užtikrinti, kad IT personalas ir vartotojai turėtų pakankamai žinių apie IT sistemas, kad jie suprastų, kodėl apsaugos priemonės reikalingos ir kaip jas taisyklingai naudoti.

Saugumo įsisąmoninimo kursai, pranešimai ir kiti renginiai turi apimti šias temas:

- saugumo svarbos organizacijai ir asmenims išaiškinimas;

- IT sistemų saugumo poreikiai ir tikslai, susiję su slaptumu, vientisumu, prieinamumu, atsakingumu, tapatumu ir patikimumu;
- su saugumu susijusių incidentų padariniai organizacijai ir individams;
- tinkamas IT sistemų kompiuterinės ir programinės įrangos naudojimas;
- tikslai, kurių siekia IT saugumo politika, visos saugumo gairės ir direktyvos, IT rizikos valdymo strategija, šių tikslų išaiškinimas, siekiant, kad būtų suvokiamos rizikos ir apsaugos priemonės;
- rizikos, susijusios su IT sistemomis, jų apsaugos būtinumas;
- būtinumas pranešti apie saugumo pažeidimus ar bandymus pažeisti;
- procedūros, pareigos ir darbų aprašymai;
- visa, ko IT personalas ir vartotojai dėl saugumo veiksnių neturi daryti;
- pasekmės, jei bus pažeistas saugumas dėl personalo kaltės;
- apsaugos priemonių įdiegimo ir tikrinimo IT saugumo planai;
- kodėl šios apsaugos priemonės yra būtinos ir kaip jas tinkamai naudoti;
- saugumo tinkamumo tikrinimo procedūros;
- pokyčių ir konfigūravimo valdymas.

Laikui bėgant atsiranda bet kurios paslaugos teikimo ar mechanizmo gedimo tendencija. Priežiūra atliekama, siekiant pastebėti šį gedimą ir pradėti koregavimo veiklą. Tai vienintelis būdas palaikyti būtiną IT sistemų saugumo lygį. IT saugumo valdymas yra nuolatinis procesas, kuris nesibaigia ir įdiegus IT saugumo planą.

Dauguma apsaugos priemonių reikalauja savo būvio laikotarpiu palaikymo ir administravimo, garantuojančių jų tinkamą funkcionavimą. Palaikymas apima šiuos veiksmus:

- įėjimo (log) bylų tikrinimą;
- parametrų keitimą, siekiant atspindėti pokyčius ir papildymus;
- skaitiklių ar pradinių reikšmių kaitaliojimą;
- senų versijų keitimą naujomis.

Saugumo tinkamumo tikrinimas yra įdiegtų apsaugos priemonių apžvalga ir analizė. Per saugumo tinkamumo tikrinimus gali būti patikrinta, ar atitinka reikalavimus:

- įdiegtos naujos IT sistemos ir paslaugos;
- esamos IT sistemos ir paslaugos po to, kai praėjo tam tikras laikotarpis (pvz., metai);
- esamos IT sistemos ir paslaugos po to, kai įvyko IT sistemų saugumo politikos pokyčiai; žiūrima, kokių papildymų reikia saugumo lygiui išlaikyti.

POKYČIŲ (KEITIMŲ) VALDYMAS. IT sistemos ir aplinka, kurioje jos veikia, nuolat keičiasi. Tai vyksta dėl to, kad atsiranda nauji požymiai ir paslaugos, atskleidžiamos naujos grėsmės ir pažeidžiamumai. IT sistemų pokyčius sudaro:

- naujos procedūros;
- naujos savybės;
- programinės įrangos atnaujinimas;
- kompiuterinės įrangos pertvarkymas;
- nauji vartotojai, taip pat ir išoriniai;
- papildomi tinklai ir vidiniai ryšiai.

Keitimas – tai bet koks valdomos aplinkos modifikavimas, įskaitant šios aplinkos komponento (konfigūracijos vieneto) įtraukimą, pašalinimą ar keitimą.

Keitimų valdymo procesas organizacijoje formalizuojamas, siekiant užtikrinti standartizuotų metodų bei procedūrų naudojimą ir efektyvų bei spartų visų keitimų apdorojimą, iki minimumo sumažinti su keitimais susijusių incidentų dėl IT paslaugų kokybės, taigi pagerinti kasdieninį organizacijos darbą.

Keitimai gali būti atliekami dėl įvairių priežasčių:

- siekiant išspręsti incidentus;
- siekiant išspręsti problemų valdymo proceso nustatytas problemas;
- reaguojant į vartotojų reiškiamas pretenzijas;
- sukūrus naujus konfigūracijos vienetus (KV);
- atnaujinant sistemos komponentus;
- atsiliepiant į pakitusius veiklos reikalavimus ar nurodymus;
- įdiegiant naują produktą ar paslaugą;
- keitimas gali būti projektų veiklos rezultatas;
- integruojant sistemos komponentus arba infrastruktūrą.

Keitimų valdymo procesas privalo apimti kiekvieno pasiūlyto IT infrastruktūros keitimo inicijavimą, planavimą ir tvirtinimą, kūrimą ir testavimą, perdavimą naudoti gamybinėje aplinkoje ir peržiūrą. Keitimus sudaro techninės įrangos ir operacinių sistemų programinės įrangos, komunikacijų programinės ir techninės įrangos, taikomųjų programų, dokumentacijos, procesų bei procedūrų ir visų kitų IT infrastruktūros konfigūracijos vienetų (KV) keitimai, jei nustatoma, kad būtinas jų valdymas ir kontrolė.

Keitimų valdymo proceso uždaviniai:

- užtikrinti sankcionuotą ir suderintą organizacijos aplinkos IT infrastruktūros keitimų valdymą;

- valdyti ir tvarkyti vartotojų ir vidinės bendro naudojimo infrastruktūros keitimų valdymą;
- užtikrinti IT infrastruktūros integralumo išlaikymą – bet kurio keitimo poveikis turi būti kvalifikuotai įvertinamas, o pasiūlytas keitimas testuojamas;
- užtikrinti, kad apie numatomą keitimo diegimą būtų informuojami darbuotojai, kuriuos tai liečia;
- pateikti atitinkamą keitimų ir jų įdiegimo veiksmų registravimo mechanizmą.

Keitimų valdymo procesas suteikia galimybę KV keitimus planuoti ir įdiegti, iki minimumo sumažinant IT paslaugos teikimo pertrūkius bei riziką. Keitimų ekspertų grupė keitimus įvertina, tvirtina ir suteikia jiems kategorijas, pvz., keitimai gali būti standartiniai, neesminiai, reikšmingi ir skubūs.

Keitimų valdymo nauda IT teikiamoms paslaugoms:

- **rizikos sumažinimas**: keitimų valdymas ir kontrolė sumažina netikėtų keitimo įdiegimo rezultatų gamybinėje aplinkoje riziką;
- **kaštų sumažinimas**: registruojant keitimus lengviau užtikrinti darbo procesų nenutrūkstamumą ir paspartinti su keitimais susijusių klausimų sprendimą;
- **IT paslaugų teikimo lankstumas**: struktūrizuotos keitimų įdiegimo procedūros suteikia organizacijai galimybę sparčiai ir efektyviai prisitaikyti prie kintančių veiklos poreikių;
- **IT paslaugų kokybės pagerinimas**: kvalifikuotas keitimų poveikio įvertinimas padeda išvengti neplanuotų IT veiklos pertrūkių.

Be keitimų valdymo organizacijoje būtinas ir konfigūravimo valdymas – tai konfigūracijos vieneto būklės (būsenos, ryšių ir t.t.) IT infrastruktūroje dokumentavimas. Jį sudaro visa su šiuo KV susijusi dokumentacija. Konfigūravimo valdymas kuria, prižiūri, seka ir pateikia informaciją, kuri pagerina kitų darbo procesų (ypač keitimų, incidentų, problemų valdymo, programinės įrangos kontrolės bei skirstymo) efektyvumą.

REAGAVIMAS Į INCIDENTUS (INCIDENTŲ VALDYMAS). Stebėjimas yra nuolatinė veikla, kurios metu tikrinama, ar sistema, jos vartotojai ir aplinka išlaiko IT saugumo plane numatytą saugumo lygį. Turi būti stebima turtas ir jo reikšmingumas, grėsmės ir turto pažeidžiamumai, šį turtą saugančios apsaugos priemonės.

Rizikos analizei paremti ir jos rezultatams pagerinti reikia informacijos apie saugumo incidentus. Todėl svarbu, kad kiekviena organizacija turėtų tinkamai sudarytą ir organizuotą IT incidentų analizės schemą (IAS) ir kad gaunama ir apdorojama informacija būtų prieinama rizikos analizei ir valdymui bei kitai su saugumu susijusiai veiklai.

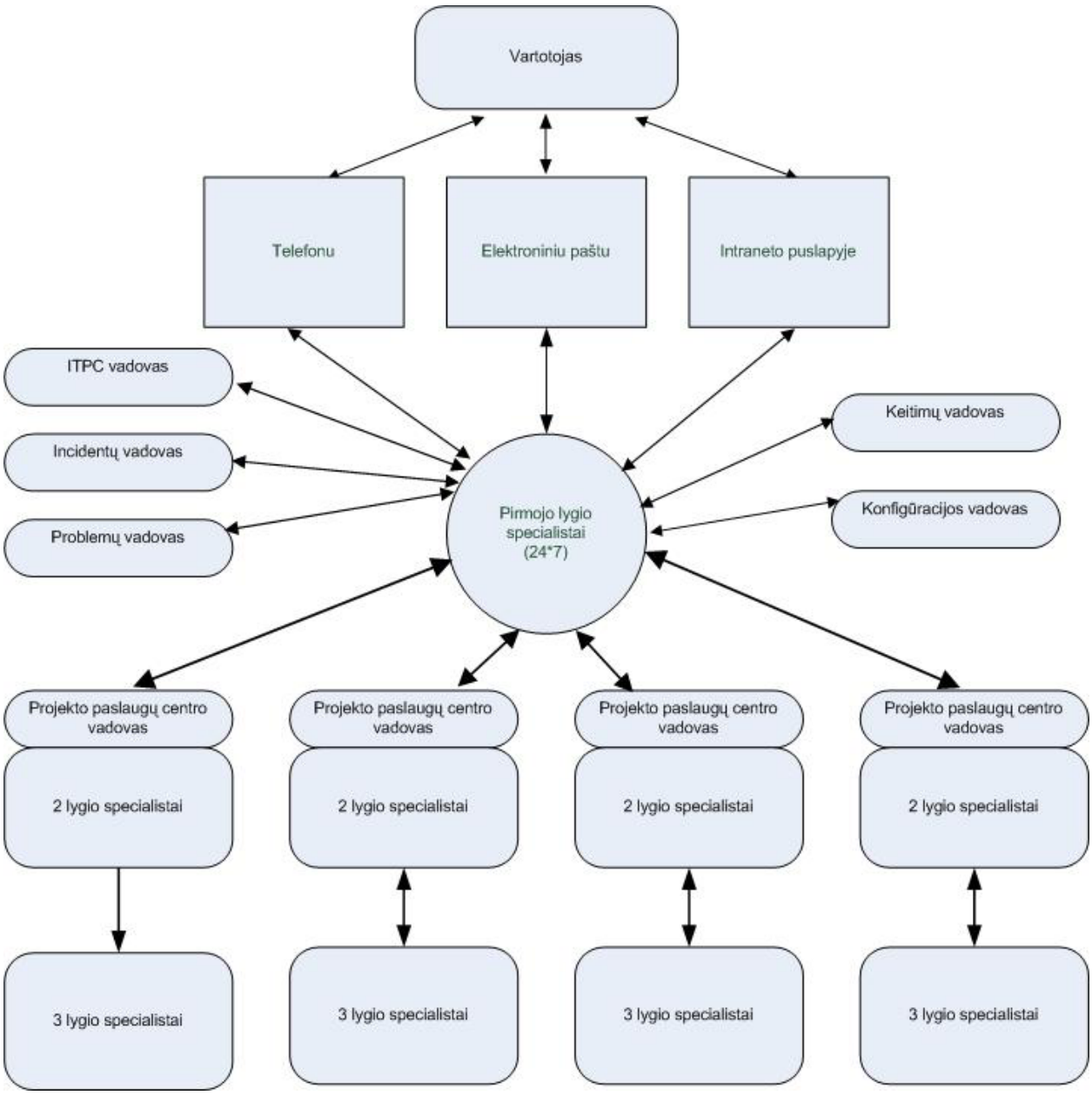
Incidentas – tai veiklos įvykis, nesantis įprastų procedūrų dalis. Pagrindinis incidentų valdymo tikslas yra kuo greičiau atkurti normalų IT paslaugų veikimą ir minimizuoti incidentų poveikį pagrindinei veiklai. Incidentų valdymo proceso komponentai:

- incidentų aptikimas ir registravimas;
- klasifikavimas ir pradinis palaikymas;
- tyrimas ir diagnozavimas;
- sprendimas ir atitaisymas;
- incidento „uždarymas“;
- nuosavybė, stebėjimas, sekimas ir informavimas.

Problemų valdymo proceso paskirtis – vykdyti IT paslaugų kokybės priemones. Problemų valdymas glaudžiai susijęs su incidentų ir aptarnavimo paraiškų valdymo procesu ir iš jo gauna pradinius duomenis. Pagrindiniai problemų valdymo tikslai:

- kiek galima sumažinti incidentų ir problemų, sukeltų IT infrastruktūros klaidų, neigiamą poveikį veiklai;
- išvengti pakartotinių su klaidomis susijusių incidentų;
- gerinti produktyvų IT išteklių naudojimą.

Visiems minėtiems priežiūros procesams – incidentų, problemų, keitimų ir konfigūravimo valdymui – vykdyti ir koordinuoti organizacijoje reikalinga IT paslaugų tarnyba (centras).



8 schema. IT paslaugų centro veiklos modulis

IT paslaugų centras (ITPC) – tai vartotojų problemų registravimas, analizė ir sprendimo paieška bei vykdymas arba vykdymo koordinavimas vienoje vietoje, naudojant tam skirtas vieningas incidentų ir jų sprendimų registravimo, keitimų valdymo, konfigūracijos vienetų ir pan. Duomenų bazes.

Vartotojas kreipiasi į ITPC telefonu, elektroniniu paštu arba užpildo standartizuotą anketą intraneto svetainėje, pranešdamas apie incidentą (kompiuterio, spausdintuvo ar kito kompiuterio priedo, taikomosios programos, duomenų perdavimo tinklo, interneto ar kitų IT paslaugų sutrikimą) arba pateikia klausimą ar paraišką konfigūracijos vieneto keitimui, kai nėra standartinės veiklos ar IT infrastruktūros trikties. Vartotojo kreipimąsi incidentų duomenų bazėje registruoja ITPC pirmjo lygio specialistai, pranešdami apie tai vartotojui elektroniniu paštu. Vartotojas gali stebėti incidento sprendimo eigą specialioje ITPC intraneto svetainėje.

ITPC pirmojo lygio specialistų grupė dirba 24 valandas per parą, 7 dienas per savaitę. Užregistravę vartotojo kreipimąsi, šie specialistai suteikia incidentui prioritetą. Prioritetai nustatomi pagal incidento svarbą ir poveikį IT veiklai: žemas, vidutinis, aukštas ir kritinis. Atitinkamai nustatomi incidento sprendimo terminai, pvz.:

- žemas – 2 darbo dienos;
- vidutinis – 1 darbo diena;
- aukštas – 4 valandos;
- kritinis – spręsti kuo greičiau.

Visų pirma incidentus sprendžia pirmojo lygio specialistai. Nepavykus išspęsti, kreipiamasi į antrojo lygio specialistus, kurie yra paskirti organizacijos vadovo įsakymu ir yra konkretaus IT projekto konsultantai.

Antrojo lygio specialistai privalo spręsti gautus incidentus ir informuoti pirmojo lygio specialistus apie priimtus sprendimus. Jei antrojo lygio specialistams nepavyksta išspręsti incidento, jie kreipiasi į trečiojo lygio specialistus, informuoja incidentų vadovą arba praneša pirmojo lygio specialistams, kad incidento išspręsti nepavyko.

Trečiojo lygio specialistai – tai išorinės organizacijos, sudariusios galiojančias paslaugų teikimo, programinės įrangos ir sistemų aptarnavimo sutartis. Tai gali būti paslaugų tiekėjas, programinės įrangos ar sistemos tiekėjas, kitos organizacijos ar tarpvalstybinių projektų paslaugų centrai.

Neišspręstas arba pasikartojantis incidentas virsta problema. Problema yra vienos klaidos, kurios priežastis nežinoma, požymis. Žinoma klaida yra būklė, nustatoma sėkmingai diagnozavus pirminę problemos priežastį. Problemų vadovas ir problemų analitikai analizuoja incidentus ir nustato problemas. Toliau analizuojamos problemos ir nustatomos žinomos klaidos, kuriamos paraiškos keisti defektyviam konfigūracijos vienetui, esančiam incidentų priežastimi.

Keitimų valdymo procesas tvarko konfigūracijos vienetų, kurie laikomi konfigūravimo valdymo duomenų bazėje, paraiškas keisti. Incidentų, problemų, keitimų ir konfigūravimo procesai tarpusavy labai susiję. Nuo konfigūravimo valdymo duomenų bazėje registruotos ir tvarkomos informacijos tikslumo bei kokybės priklauso kiti organizacijos veiklos, IT strategijos, projektavimo ir valdymo, IT paslaugų kūrimo ir diegimo procesai.

Tuo tikslu organizacijai keliamas reikalavimas – turėti atskiras pareigas ir atsakomybes, aiškiai apibrėžtas kiekvienam iš šių procesų, ir tuo pat metu glaudžiai bendradarbiaujančias, yra išlaikomas sėkmingai organizuojant Informacinių technologijų paslaugų centro darbą.

IŠVADOS

1. Išnagrinėjus Lietuvos Respublikoje galiojančius teisės aktus, kuriais nustatyti duomenų saugos informacinėse sistemose organizavimo ir organizacinių priemonių reikalavimai valstybinėms institucijoms, galima konstatuoti, kad teisinė bazė šiuo klausimu dar nepakankama.

2. Teisės akto, kuris vieningai būtų taikomas visiems be išimties duomenims bei apibrėžtų ir aiškiai susietų visai šiai duomenų visumai turimus taikyti duomenų saugos informacinėse sistemose organizacinių priemonių principus ar standartus, procedūras, arba pateiktų atitinkamas nuorodas, nėra.

3. Viešojo administravimo institucijai iškyla problema, kaip, pasinaudojus informacinių technologijų paslaugas teikiančių įmonių siūlomais projektais, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, ir, nenusižengus galiojantiems teisės aktams, sukurti organizacijoje saugumo valdymo struktūrą ir patvirtinti informacijos saugumo politiką arba nuostatus, kuriais galėtų vadovautis organizacijos vadovybė ir darbuotojai, užtikrindami savo veiklos tolydumą ir nenutrūkstamą.

4. Organizacijos informacinį turtą arba išteklius sudaro ne tik sukaupta informacija, bet ir programinė bei fizinė įranga, su informacijos saugojimu susijusios paslaugos. Šį turtą būtina įvertinti, norint nustatyti potencialią žalą, atsirandančią dėl informacijos ar kito, su ja susijusio, turto atskleidimo, modifikavimo, neprieinamumo ar sunaikinimo. Tačiau nėra tiesioginio ir lengvo būdo nustatyti viso turto finansinę vertę. Todėl būtina nustatyti vertę ar reikšmės dydį organizacijai nefinansiniais terminais, pasirinkus skalę: „nereikšmingas – mažai reikšmingas – vidutiniškai reikšmingas – gana reikšmingas – labai reikšmingas“.

5. Kiekviena viešojo administravimo institucija privalo laikytis Europos Sąjungos ir Lietuvos Respublikos teisės aktų, reglamentuojančių informacijos apsaugą ir kontrolę, ir tinkamai saugoti informaciją. Tam būtinas organizacijoje turimos informacijos klasifikavimas pagal slaptumą ir prieinamumą. Lietuvos Respublikos vidaus reikalų ministro įsakymu patvirtintos Informacijos klasifikavimo pagal duomenų grupes rekomendacijos nėra visiškai priimtinos, norint tinkamai suskirstyti informaciją pagal jos svarbą organizacijos veiklai.

6. Organizacijos saugos valdymo struktūra turėtų būti „plokščia“, nes saugos valdymui reikalingi įvairių sričių specialistai. Iš kitos pusės, kad saugos valdymas būtų sėkmingas, šios struktūros grandžių atsakomybės turi būti griežtai apibrėžtos ir atstovaujamos gana aukštu lygiu. Autorė siūlo sukurti nuolatinį Saugos administravimo komitetą, kuriam vadovautų vienas iš organizacijos administracijos vadovų. Komitetas tiesiogiai vadovautų Saugos administravimo pakomitečiams, įsteigtiems kiekvienoje organizacijos tarnyboje.

7. Kaip ir kiekviena veikla, organizacijos informacijos saugumo valdymas prasideda nuo planavimo, tai yra nuo organizacijos tikslų, strategijos ir politikos saugumo srityje nustatymo. Bendriausias informacijos saugumo valdymo tikslas – garantuoti, kad organizacija galėtų veikti, esant priimtino lygio rizikoms. Joks saugumas negali būti absoliučiai garantuotas. Būtina planuoti žalos padarinių atkūrimo veiklą po nepageidaujamo incidento ir sudaryti sąlygas, kad toks incidentas nepasikartotų.

8. Veiklos planavimo schemose nurodyti veiksmai ir funkcijos turi būti suderinti su organizacijoje įprastu veiklos stiliumi, jos dydžiu ir struktūra, veiklos pobūdžiu. Svarbu pasirinkti rizikos valdymo strategiją, kuri labiausiai tiktų organizacijai, būtų priimtiniausia, atsižvelgiant į galimus skirti finansinius ir žmogiškuosius išteklius, duotus terminus.

Kai kuriais atvejais organizacija gali nutarti nenaudoti jokių apsaugos priemonių arba atidėti jų įdiegimą. Jeigu toks sprendimas yra priimtas, administracija turi visiškai suprasti, kokios rizikos egzistuoja ir kokie žalingi poveikiai yra su jomis susiję, taip pat kiek tikėtini yra nepageidaujami įvykiai. Stokojant šių žinių, organizacija netyčia gali pažeisti įstatymus, kitus teisės aktus, ir jos veiklai gali grėsti potencialūs nuostoliai.

9. Labai patogi priemonė planavimo procese – dokumento „IT saugumo architektūra“ parengimas ir jo aprobavimas administracijos lygyje. Šiame dokumente aptariamos techninės apsaugos priemonės, atsižvelgiama ir į netechninius aspektus. IT saugumo architektūra yra naudojama kaip saugumo elementų struktūros ir loginio grupavimo apibrėžimo priemonė. Joje aprašoma, kokiu būdu IT sistemos saugumo reikalavimai turi būti patenkinti. Remiantis rizikos analizės rezultatais, saugumo reikalavimai paverčiami techninių saugumo paslaugų rinkiniu, taikomu tai sistemai, kuri šiuos reikalavimus turi atitikti.

10. Nustačius IT saugumo tikslus ir numačius bei suderinus su vadovybe jų įgyvendinimo strategiją, formuojama IT saugumo politika, kuri įforminama, kaip saugos dokumentas ir tvirtinama organizacijos vadovybės. Informacijos saugumo politika arba nuostatai – tai taisyklių, standartų, praktinio pritaikymo pavyzdžių rinkinys, reguliuojantis, kaip organizacija valdo, apsaugo ir skirsto jai priklausančią informaciją. Dokumentą rengia arba koordinuoja jo parengimą bei aprobavimą nuolatinis Saugos administravimo komitetas. Politikos išplėtojimui ir efektyviam įgyvendinimui reikalinga visų organizacijos grandžių vadovybės parama ir supratimas.

11. Svarbi informacijos saugumo valdymo grandis – saugumo rizikos analizė. Prieš pradedant bet kokius rizikos analizės veiksmus, organizacija turi turėti šios analizės strategiją, kurios sudedamosios dalys (būdai, metodai ir kt.) turi būti įformintos dokumentais, kurie turi būti nurodyti IT saugumo politikoje. Organizacijoje turi būti susitarta dėl rizikos analizės metodo parinkimo priemonių ir kriterijų. Kadangi paprastai būna per brangu atlikti detalią visų IT

sistemų rizikos analizę, taip pat neefektyvu skirti mažai dėmesio rimtoms grėsmėms, reikalinga pusiausvyra tarp šių variantų. Bendro lygio analizė, derinant ją su pagrindiniu požiūriu ir, kur reikia, su išsamia rizikos analize, daugumai organizacijų yra efektyviausias kelias.

Sėkmingai pasirinkus rizikos analizės strategiją, įvertinus grėsmes, pažeidžiamumus ir rizikos laipsnius, jau įdiegtas apsaugos priemones bei turimus finansinius išteklius, galima nustatyti organizacijai priimtino lygio riziką, tai mažai tikėtinų grėsmių pakankamai apsaugotoms silpnoms organizacijos vietoms tikimybė. Šis rizikos lygis turėtų būti organizacijos informacijos saugumo valdymo pagrindinis tikslas.

12. Laikui bėgant atsiranda bet kurios paslaugos teikimo sutrikimo ar mechanizmo gedimo rizika. Saugumo priežiūra atliekama, siekiant pastebėti šį gedimą ir pradėti koregavimo veiklą. Tai vienintelis būdas palaikyti būtiną IT sistemų saugumo lygį. IT saugumo valdymas yra nuolatinis procesas, kuris nesibaigia ir įdiegus IT saugumo planą. Priežiūra apima tokius IT saugumo valdymo procesus, kaip saugumo tinkamumo tikrinimas, stebėjimas, pokyčių valdymas ir reagavimas į incidentus. Šių priežiūros procesų vykdymą ir koordinavimą tikslingiausia pavesti IT paslaugų tarnybai, kurios struktūros aprašymą autorė pateikia paskutiniame savo darbo skyriuje.

Tuo tikslu organizacijai keliamas reikalavimas – turėti atskiras pareigas ir atsakomybes, aiškiai apibrėžtas kiekvienam iš šių procesų, ir tuo pat metu glaudžiai bendradarbiaujančias, yra išlaikomas sėkmingai organizuojant Informacinių technologijų paslaugų centro darbą.

SIŪLYMAI

1. Kaip teigia Informacinių sistemų audito ir valdymo asociacija (ISACA), kurią autorė jau citavo savo darbo įvade, „bendras informacijos saugumo klausimų suvokimo organizacijoje lygis tiesiogiai priklauso nuo organizacijos vadovybės suvokimo lygio“. Verslo įmonėms informacijos saugumo užtikrinimą valstybė gali reglamentuoti tik teisės aktais, ir dažniausiai asmens duomenų apsaugos srityje. Viešojo administravimo institucijose informacijos saugumo užtikrinimas yra bendravalstybinis reikalas, nes ir šių organizacijų turtas priklauso valstybei. Autorė mano, kad informacijos saugumo principai, jų įgyvendinimas ir priežiūra valstybinėms institucijoms turi būti reglamentuoti norminiais teisės aktais, kurių privalu laikytis. Šiuo metu Vyriausybės nutarimu patvirtintų Bendrųjų duomenų saugos reikalavimų ir Vidaus reikalų ministro įsakymu patvirtintų Tipinių duomenų saugos nuostatų yra per maža.

2. Šiuos norminius teisės aktus rengti ir jų laikymąsi kontroliuoti turėtų valstybės institucija, tiesiogiai pavaldi Vyriausybei, o ne didelės, daug struktūrinių padalinių ir daug veiklos sričių apimančios ministerijos mažas padalinys.

LITERATŪRA

1. Lietuvos Respublikos baudžiamasis kodeksas // Valstybės žinios. 2000, Nr. 89-2741.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.
3. Lietuvos Respublikos visuomenės informavimo įstatymas // Valstybės žinios. 1996, Nr. 71-1706.
4. Lietuvos Respublikos valstybės registrų įstatymas // Valstybės žinios. 1996, Nr. 86-2043.
5. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas // Valstybės žinios. 1999, Nr. 50-1598.
6. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas // Valstybės žinios. 1999, Nr. 105-3019.
7. Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827.
8. Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo // Valstybės žinios. 2001, Nr. 32-1055.
9. Lietuvos Respublikos operatyvinės veiklos įstatymas // Valstybės žinios. 2002, Nr. 65-2633.
10. Lietuvos Respublikos Vyriausybės 1996 m. lapkričio 29 d. nutarimas Nr. 1418 "Dėl valstybės registrų steigimo, projektavimo, reorganizavimo ir naudojimo" // Valstybės žinios. 1996, Nr. 118-2743.
11. Lietuvos Respublikos Vyriausybės 1997 m. liepos 4 d. nutarimas Nr. 726 "Dėl valstybės registrų duomenų naudojimo ir Valstybės registrų sąrašo nuostatų patvirtinimo" // Valstybės žinios. 1997, Nr. 66-1628.
12. Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 "Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose" // Valstybės žinios. 1997, Nr. 83-2075.
13. Lietuvos Respublikos Vyriausybės 2000 m. kovo 27 d. nutarimas Nr. 349 "Dėl Asmens duomenų valdytojų valstybės registro įsteigimo ir šio registro nuostatų patvirtinimo" // Valstybės žinios. 2000, Nr. 27-721.
14. Lietuvos Respublikos Vyriausybės 2000 m. balandžio 27 d. nutarimas Nr. 462 "Dėl Lietuvos Respublikos įslaptintos informacijos apsaugos tvarkos patvirtinimo" // Riboto naudojimo
15. Lietuvos Respublikos Vyriausybės 2001 m. sausio 31 d. nutarimas Nr. 112 "Dėl valstybės kadastrų, klasifikatorių ir registrų duomenų teikimo neatlygintinai 2001-2004 metais" // Valstybės žinios. 2001, Nr. 12-337.
16. Lietuvos Respublikos Vyriausybės 2001 m. vasario 28 d. nutarimas Nr. 228 "Dėl duomenų teikimo duomenų subjektui atlyginimo taisyklių patvirtinimo" // Valstybės žinios. 2001, Nr. 20-651.
17. Lietuvos Respublikos Vyriausybės 2001 m. rugpjūčio 10 d. nutarimas Nr. 984 "Dėl Lietuvos informacinės visuomenės plėtros strateginio plano patvirtinimo" // Valstybės žinios. 2001, Nr. 71-2534.
18. Lietuvos Respublikos Vyriausybės 2001 m. rugsėjo 25 d. nutarimas Nr. 1156 "Dėl Valstybinės duomenų apsaugos inspekcijos struktūrinės reformos, įgaliojimų suteikimo, Valstybinės duomenų apsaugos inspekcijos nuostatų patvirtinimo ir su tuo susijusių Lietuvos Respublikos Vyriausybės nutarimų dalinio pakeitimo" // Valstybės žinios. 2001, Nr. 83-2890.
19. Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 "Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo" // Valstybės žinios. 2001, Nr. 110-4006.
20. Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2105 "Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 "Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose" pakeitimo" // Valstybės žinios. 2003, Nr. 2-45.

21. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės 1997 m. liepos 7 d. įsakymas Nr. 35 “Dėl dokumentų saugyklų” // Valstybės žinios. 1997, Nr. 68-1728.
22. Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės 2000 m. rugpjūčio 30 d. įsakymas Nr. 19 “Dėl Lietuvos Respublikos įslaptintų dokumentų apskaitos, raštvedybos organizavimo, tvarkymo bei kontrolės taisyklių patvirtinimo” // Valstybės žinios. 2000, Nr. 76-2325.
23. Lietuvos Respublikos vidaus reikalų ministro 2003 m. sausio 27 d. įsakymas Nr. 1V-33 “Dėl informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo” // Valstybės žinios. 2003, Nr. 77-3541.
24. Lietuvos Respublikos vidaus reikalų ministro 2003 m. liepos 16 d. įsakymas Nr. 1V-272 “Dėl Tipinių duomenų saugos nuostatų patvirtinimo” // Valstybės žinios. 2003, Nr. 76-3511.
25. Konvencija dėl duomenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) // Valstybės žinios. 2001, Nr. 32-1059.
26. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios. 2004, Nr. 36-1188.
27. Europos Parlamento ir Tarybos direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ (95/46/EB). www.ada.lt, prisijungimo laikas 2004-10-16.
28. Europos Parlamento ir Tarybos direktyva „Dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje“ (97/66/EB). www.ada.lt, prisijungimo laikas 2004-10-16.
29. Europos Parlamento ir Tarybos direktyva „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“ (2002/58/EB). www.ada.lt, prisijungimo laikas 2004-10-16.
30. Augustinaitis A.. Informacijos visuomenės profesionalumo kriterijai // Informacijos mokslai. VU, 2001(16), P.17-30.
31. Česna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. – Vilnius, 2000.
32. Janiūnienė E.. Biblioteka – žinių institucija // Informacijos mokslai. VU, 2001(17).
33. Keras A., Kurapka E., Petrauskas R. Informacinės visuomenės kūrimo, informacinių technologijų taikymo ir informacinių technologijų teisės plėtros tendencijos Europos Sąjungoje. – Vilnius, 2001.
34. Lakis J.. Permainos ir iššūkiai organizacijų vidaus administravimo srityje // Viešoji politika ir administravimas: LTU, KTU, 2003 (6), P.65-67.
35. Mitchell W. J. E-topija.. – Vilnius, 2002.
36. Petrauskas R. Informacinių technologijų taikymas viešajame administravime. – Vilnius, 2001.
37. Dabartinės lietuvių kalbos žodynas. Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2000.
38. Tarptautinių žodžių žodynas. –Vilnius: Alma littera, 2003.
39. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų saugumo sąvokos ir modeliai. – Lietuvos standartas (tapatus ISO/IEC TR 13335-1:1996).
40. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 2 dalis. Informacijos technologijų saugumo valdymas ir planavimas. – Lietuvos standartas (tapatus ISO/IEC TR 13335-2:1997).
41. Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 3 dalis. Informacijos technologijų saugumo valdymo metodai. – Lietuvos standartas (tapatus ISO/IEC TR 13335-3:1998).
42. Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai. – Lietuvos standartas (tapatus ISO/IEC 17799:2000).
43. World Public Sector Report 2003: E-government at the Crossroads. United Nations, New York, 2003, P.110-122.

44. John Kramer. The CISA Prep Guide: Mastering the Certified Information Systems Auditor, 4 chapter, Protection of Information Assets. 2003, Wiley Publishing, Inc.Indianapolis, Indiana, P.184-185.
45. ISACA Lietuva. Informacinių sistemų audito ir valdymo asociacija // http://www.isaca.lt/lt/naujienos/?news_id=News192, prisijungimo laikas 2004-10-16.

SANTRAUKA

2001 m. Lietuvos Respublikos Vyriausybė, suderinusi su Europos Sąjungos veiklos planais *eEurope 2005* ir *eEurope*+, patvirtino Lietuvos informacinės visuomenės plėtros strateginį planą, kuriame numatė užtikrinti informacinių technologijų saugumą valstybės institucijose ir įstaigose. Tais pačiais metais buvo patvirtinta Informacijos technologijų saugos valstybinė strategija, įpareigojanti teisiškai reglamentuoti bendruosius duomenų saugos reikalavimus.

2002 m. gruodžio 31 d. patvirtinti Bendrieji duomenų saugos reikalavimai informacijos saugumo politiką traktuoja kaip atskirų dokumentų visumą (nuostatai ir detalios instrukcijos), tuo tarpu komercinės IT paslaugas teikiančios įmonės siūlo organizacijoms vieną bendrą IT saugos politikos dokumentą, pažodžiui atspindintį ISO/IEC standartą 17799, bet netinkamą tvirtinti organizacijos vadovo įsakymu. Iškyla problema, kaip pasinaudoti komercinių įmonių parengtais projektais, pripažintais standartais, ir, nenusižengus galiojantiems teisės aktams, sukurti organizacijoje saugumo valdymo struktūrą, patvirtinti informacijos saugumo politiką arba nuostatus, kuriais galėtų vadovautis organizacijos vadovybė ir darbuotojai.

Magistro baigiamojo darbo tikslas – išnagrinėti Lietuvos ir Europos Sąjungos teisės aktų keliamus reikalavimus informacijos saugumo užtikrinimui viešojo administravimo institucijoje, pateikti savo siūlymus, kokia turėtų būti organizacijos informacijos saugumo valdymo struktūra, strategija ir politika, jų įgyvendinimo administracinės, organizacinės ir technologinės priemonės.

SUMMARY

In 2001, the Lithuanian Government, considering EU's eEurope 2005 and eEurope+ Action Plans, approved Lithuania's strategic plan of information society development, which set a goal to ensure the IT security at public institutions and offices. The same year saw the State's strategy of technological security approved, which enforced legal regulation of general data security requirements.

On December 31st, 2002, the General data security requirements treat information security policy as a sum of different documents (rules and detailed instructions), while commercial IT providers offer organizations only one general document of IT security policy, which reflects ISO/IEC standard 17799 word-to-word, but is not approvable by the order of organization's head. Therefore the problem is how to use projects prepared by commercial companies, meet the accepted standards and, without contradicting the existing legal acts, create the organization's security management structure, plus approve the information security policy or rules, usable by organization's heads and staff.

This written work is aimed to analyze Lithuanian and EU legal requirements for information security at public administration institutions and present the student‘s own suggestions on the desirable ideal of organization‘s information security management structure, strategy and policies; administrative, organizational and technological tools of bringing these policies‘ to reality.

2 priedas

SĄVOKOS IR APIBRĖŽIMAI

Grėsmė – tikėtinas įvykis, procesas, veiksmas ar savybė, įsikūniję viename ar daugiau grėsmės veiksnių, kurie, jiems suveikus, gali pažeisti informacinių technologijų, duomenų, informacijos saugumą organizacijoje.

Grėsmės veiksnys – bet koks asmuo ar dalykas, kuris veikia ar gali veikti, sukelti, nešti, perduoti ar palaikyti grėsmę.

Pažeidžiamumas – silpnoji organizacijos vieta ar kitas keliamų reikalavimų, standartų neatitikimas, kuria gali pasinaudoti grėsmė.

Rizika – tikimybė, kad esant tam tikrai grėsmei ir sistemos pažeidžiamumui, bus neįvykdyti teisės aktų, reglamentuojančių saugą, reikalavimai arba sutrikdyta organizacijos veikla ir patirti nuostoliai.

Rizikos analizė – procesas, kurio metu nustatomi saugos rizikos veiksniai, nustatomas rizikos dydis bei apsaugos priemonių reikalaujančios sritys. Tai organizacijos informacijos išteklių, egzistuojančių jos kontrolės priemonių ir mechanizmų bei kitų organizacinių ir IT pažeidžiamumų analizė.

Rizikos įvertinimas – jos priklausomybės nuo turto reikšmingumo, grėsmių, galinčių padaryti žalingą poveikį veiklai, tikėtinumo, pasinaudojimo pažeidžiamumais paprastumo ir visų esamų ar planuotų apsaugos priemonių, galinčių sumažinti riziką, dydžio nustatymas.

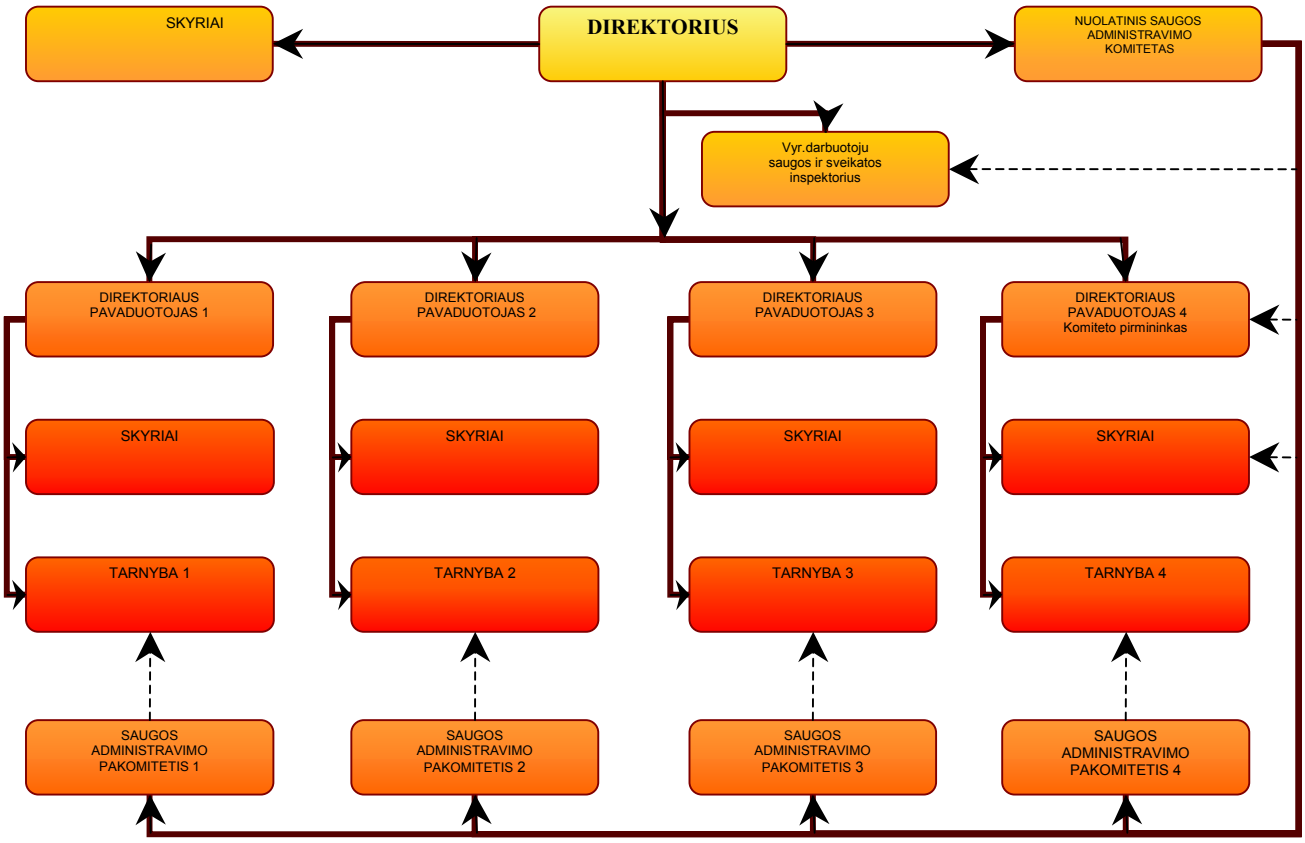
Apsaugos priemonės – kontrolės priemonės ar mechanizmai, atliekantys veiksmus, siekiant sumažinti esamą organizacijos pažeidžiamumą iki tam tikros nustatytos grėsmės realumo tikimybės.

Organizacijai priimtino lygio rizika – mažai tikėtinų grėsmių pakankamai apsaugotoms silpnoms organizacijos vietoms tikimybė.

Strategija – veiksmai ir sprendimai bei organizacijos sąveika su aplinka ilgu laikotarpiu.

Politika – nuostatų ir strategijų visuma tikslui pasiekti.

Klasifikavimas – sisteminis informacijos išdėstymas grupėmis ar kategorijomis pagal apibrėžtą kriterijų.


SKYRIAI
DIREKTORIUS
NUOLATINIS SAUGOS ADMINISTRAVIMO KOMITETAS
Vyr.darbuotoju saugos ir sveikatos inspektorius
DIREKTORIAUS PAVADUOTOJAS 1
DIREKTORIAUS PAVADUOTOJAS 2
DIREKTORIAUS PAVADUOTOJAS 3
DIREKTORIAUS PAVADUOTOJAS 4 Komiteto pirmininkas
SKYRIAI
SKYRIAI
SKYRIAI
SKYRIAI
TARNYBA 1
TARNYBA 2
TARNYBA 3
TARNYBA 4
SAUGOS ADMINISTRAVIMO PAKOMITETIS 1
SAUGOS ADMINISTRAVIMO PAKOMITETIS 2
SAUGOS ADMINISTRAVIMO PAKOMITETIS 3
SAUGOS ADMINISTRAVIMO PAKOMITETIS 4