Vilniaus Universitetas
Tarptautinis žinių ekonomikos ir žinių vadybos centras

Gediminas Subačius,
Informacijos sistemų vadybos studijų programos studentas

Informacijos saugos politikos formavimas šiuolaikinėje organizacijoje

MAGISTRO DARBAS

Mokslinis vadovas Lekt. S. Jastiuginas

Vilnius, 2006

Gedimino Subačiaus magistro darbas

(magistranto (-ės) vardas, pavarde)

tema

Informacijos saugos politikos formavimas šiuolaikinėje organizacijoje

parengtas gynimui.

_____ _____

(data) (vadovo parašas)

Darbas įregistruotas _____ centre

_____

(data) (administratores parašas)

Magistro darbą ginti leidžiu

_____ (centro direktoriaus parašas) _____

(data)

Recenzentu skiriu

_____

_____ _____

(data) (Direktoriaus parašas)

Darba recenzavimui gavau

_____ _____

(data) (recenzento parašas)

Su 02 Subačius, Gediminas

Informacijos saugos politikos formavimas šiuolaikinėje įmonėje: magistro darbas / Gediminas Subačius, informacijos sistemų vadybos studijų programos studentas; mokslinis vadovas lekt. S. Jastiuginas; Vilniaus universitetas. Tarptautinis žinių ekonomikos ir žinių vadybos centras. – Vilnius, 2006. – 88, lap.: – Mašinr. – Santr. Angl. – Bibliogr.: 70 – 73 p. (42 pavad.).

UDK 65.011.681.3.01

Informacijos saugos politika, strategija, saugumo procesų dokumentacija, rizikų analizė, IT Outsorsingas, organizacijos veiklos tęstinumas, saugumo standartai ir metodikos, teisinis reguliavimas, saugumo rinkos statistika.

Magistro *darbo objektas* – informacijos apsaugos politikos formavimas, šiuolaikinės verslo aplinkos kontekste. *Darbo tikslas* – išnagrinėti informacijos apsaugos procesus, pagrindinius elementus ir pateikti rekomendacijas, kurios būtų naudingos kuriant funkcionalią ir efektyvią saugumo politiką
Išsiaiškinti informacijos saugos sampratą, išskirti pagrindiniai darbo uždaviniai elementus, apibrėžti informacijos saugumo politikos sampratą, išnagrinėti pagrindinius jos formavimo etapus, apžvelgti ir pristatyti tarptautinių standartų asociacijų rinkoje siūlomus sprendimus, supažindinti su saugumo strategijos ir dokumentacijos pagrindiniais etapais, apibrėžti pagrindinius organizacijos brandos modelius, naudojamus rizikų analizėje, išanalizuoti, kokia situacija saugos politikos srityje yra Lietuvos organizacijose, taip pat apžvelgti, kokie sprendimai yra siūlomi Lietuvos rinkoje.

Geras organizacijos vadovybės informacijos svarbos suvokimas, sugebėjimas išskirti pagrindinius informacinius resursus ir numatymas, kokią įtaką verslo sėkmingumui turės saugumo politikos įdiegimas, gali lemti sėkmingą saugumo įgyvendinimą. Analizuojant saugumo politikos pagrindinius etapus, procesus ir remiantis įvairiomis saugumo metodikomis, galima identifikuoti pagrindinius pavojus, lengviau pašalinti esančias problemas. Taip pat svarbu įvertinti įmonės veiklos apimtis, specifiką ir pagal tai pasirinkti atitinkamas technologijas ir metodikas.Būtina taip pat ne tik rinktis metodikas, bet ir nepamiršti įvertinti „Outsorsingo“ teikiamų privalumų ir pavojų, teisingai valdyti investicijas, sukurti veiklos tęstinumo mechanizmą, vertinti rizikas ir dar daug kitų su saugumu susijusių procesų. Todėl tik sėkmingai valdant ir planuojant paminėtus ir kitus veiksnius, galima tikėti sėkmės.

Šis magistro darbas – susisteminta informacija apie pagrindinius saugumo politikos etapus ir procesus, populiariausius standartus, pasitaikančias problemas ir patarimus kaip jų išvengti. Todėl šis darbas galėtų būti panaudojamas, kaip apibendrinta ir susisteminta teorinė priemonė apie pagrindinius saugumo procesus ir etapus. Ji gali būti naudinga visiems besidomintiems informacijos saugumu.

Turinys

ĮVADAS

Globalinėje informacinėje visuomenėje žinios ir informacija turi išskirtinę vertę. Informacijos pagrindu kuriamos žinios tampa esminiu modernios visuomenės požymiu. Naujos informacinės technologijos sukūrė puikias sąlygas greitesniam informacijos perdavimui, didėjantis informacijos poreikis paskatino spartų informacinės visuomenės vystymąsi. Tačiau negalima pamiršti, kad sparti skaitmeninių technologijų ir nuo jų neatsiejamos informacinės visuomenės plėtra valstybei ir jos piliečiams kuria tiek naujas galimybes, tiek naujus iššūkius. Galima drąsiai teigti, kad gyvename informacijos amžiuje, kai nuo informacijos tikslumo, jos pateikimo greičio priklauso daugelio žmonių gyvenimas. Informacija ir jos apdorojimo sparta tapo neatsiejama verslo įmonių, valstybinių įstaigų bei kitų organizacijų dalimi. Tam tikros informacijos turėjimas gali suteikti konkurencinį pranašumą, o jos praradimas – atnešti nuostolių.

Šiandieninėje aplinkoje vis sparčiau plinta ir tobulėja informacinių technologijų bazėje sukurti darbo įrankiai. Darbui su moderniomis IT priemonėmis pasirengusi vis didesnė visuomenės dalis.

Tačiau informacijai tapus vienu iš svarbiausių resursų, iškilo klausimas, kaip šį resursą apsaugoti. Informaciją vis labiau kompiuterizuojant, iškyla pavojus, jog ji gali patekti į viešumą arba gali būti pavogta Tai gali būti pavojinga paprastam žmogui, nekalbant apie nuostolius, kuriuos gali patirti organizacija.

Informacija gali būti saugoma daug kur: knygose, žmonių galvose, užrašuose, brėžiniuose, kompiuterių sistemose. Nepriklausomai nuo to, kur informacija yra saugoma visada išlieka pavojus, jog ji gali būti bet kada sugadinta, prarasta ar pakeista.

Organizacijos, vystančios savo veiklą informacijos amžiuje ir norėdamos sėkmingai konkuruoti vis tobulėjančios rinkos sąlygomis, yra priverstos nuolat tobulinti savo informacijos apsaugos metodus, naudotis geromis praktikomis, ir diegti naujas apsaugos priemones. Tarptautinių standartų asociacijų (ISACA- COBIT, International - Educational - ISO 13335, British Standard. Predecessor to ISO 17799) ir kitų organizacijų sukurtose metodikose pateikiama daug praktinių patarimų, pavyzdžių, kurie gali būti naudingi formuojant įmonės saugumo politiką. Tai yra sudėtingas procesas, apimantis strategijos formavimą, pagrindinių procesų dokumentavimą, esamos organizacijos rizikų išaiškinimą, darbuotojų mokymus ir kitus svarbius veiksnius. Norint sėkmingai tęsti įmonės veiklą, visiems jos procesams turi būti skiriamas vienodai svarbus dėmesys. Todėl informacijos politikos formavimo proceso svarba negali būti nuvertinama.

Informacinės visuomenės vystymosi pradžioje, nedaug žmonių suvokė, kas ta informacija ir kodėl ją reikėtų saugoti, todėl tuomet tai buvo tik IT profesionalų tyrinėjama sritis, kuriai nebuvo skiriama daug dėmesio. Tačiau informacijai tampant vis svarbesniu verslo elementu, organizacijoms patiriant vis

didesnius nuotolius dėl duomenų praradimo, ar kitokio pakenkimo, šia sritimi buvo pradėta domėtis daug labiau. Organizacijų vadovai pradėjo suprasti, kad nepakanka įdiegti informacijos saugos politiką, ji turi būti glaudžiai susijusi su įmonės strategija, vizija. Šiai sričiai tampant vis aktualesnei, jau minėtų tarptautinių standartų organizacijų parengti „gerų praktikų“ rinkiniai ir standartai tapo populiarūs. Jie tapo puikia priemone palengvinančia apsaugos procesų diegimą. Atsirado kompanijų, kurios pradėjo siūlyti specifines „IT Outsorsing“ paslaugas, kurios organizacijoms leido joms neparankias sritis perduoti specialistams.

Siūlomi sprendimai, bėgant laikui darėsi vis tobulesni, geriau orientuoti į organizacijų verslo procesus ir poreikius. Tam tobulėjimui įtakos turėjo technologinis vystymasis, tobulėjantys nusikaltėlių naudojami metodai, besikeičiantis teisinis reguliavimas ir kiti veiksniai. Saugumo srities specialistai, stengdamiesi padėti organizacijoms, sukūrė jau minėtus standartų ir geriausių praktikų rinkinius, kurie leidžia daug lengviau analizuoti procesus ir pasirinkti tinkamus sprendimus atsižvelgiant į kiekvienos organizacijos specifiką. Todėl žodžiai „saugumo politika" ir „formavimas“ šiame darbe bus vartojami kontekste, susijusiame su organizacijos informacijos saugumo sąvoka, esminiais informacijos saugumo principais, pagrindiniais informacijos saugumo politikos formavimo etapais ir organizacijos vadovybės požiūriu į saugumo politiką ir jos formavimą. Šis darbas nepretenduoja tapti išsamiu vadovu, kaip sukurti ir palaikyti organizacijos saugumo politiką, tačiau jame bus stengiamasi išanalizuoti ir pateikti pagrindinius saugumo politikos formavimo etapus, naudojamas metodikas, žmogiškojo faktoriaus klaidas, kurios gali sukelti pavojų organizacijos turimai informacijai, duomenims. Darbe pateikiama medžiaga gali būti naudinga ir padėti sužinoti, kokie sprendimai yra siūlomi šiandieninėje rinkoje, kokie svarbiausi žingsniai turi būti žengti, norint įgyvendinti informacijos saugumo politiką, kodėl ši politika kartais būna nefunkcionali, kaip suvaldyti netikėtumus ir kt.

Temos aktualumas. Organizacijoms tenka vystyti savo veiklą vis intensyvesnėje rinkoje, tam didelės įtakos turi sparčiai besivystančios technologijos, kurios suteikia daug naujų galimybių tiek organizacijoms, tiek privatiems žmonėms. Organizacijos susiduria su būtinybe vis daugiau investuoti į savo svarbiausių resursų apsaugą. Nusikaltėliai, vykdantys nusikaltimus, taip pat tobulėja, todėl organizacijos turi skirti vis didesnį dėmesį apsaugai. Įmonės sugebėjimas apsaugoti net tik savo, klientų bei partnerių informaciją, bet ir sugebėjimas užtikrinti savo veiklos nepertraukiamumą, gali jai padėti sutaupyti daug laiko ir resursų.

Temos problematika. Daugelis organizacijų susiduria su problema, kurią sukelia dažnai neefektyvus įsigytų technologijų panaudojimas, nemokėjimas įvertinti esminių įmonės resursų, nepakankamas darbuotojų mokymas, rizikų valdymas, netikslingos investicijos, netinkamas IT procesų tęstinumo valdymas taip pat įdiegtos saugumo politikos nepasiteisinimas, kartais ir žlugimas.

Darbo *tyrimo objektas* – informacijos apsaugos politikos formavimas šiuolaikinės verslo aplinkos kontekste. *Darbo tikslas* – išnagrinėti informacijos apsaugos procesus, pagrindinius elementus ir pateikti rekomendacijas, kurios būtų naudingos kuriant funkcionalią ir efektyvią saugumo politiką. Siekiant įgyvendinti šį tikslą buvo užsibrėžti *uždaviniai*:

- ✓ išsiaiškinti informacijos saugos sampratą, apibrėžti pagrindinius informacijos saugos elementus;
- ✓ apibrėžti informacijos saugumo politikos sampratą, išnagrinėti pagrindinius jos formavimo etapus;
- ✓ apžvelgti ir pristatyti tarptautinių standartų asociacijų rinkoje siūlomus sprendimus, supažindinti su saugumo strategijos ir dokumentacijos pagrindiniais etapais, apibrėžti pagrindinius rizikų analizės etapus ir naudojamus metodus
- ✓ ištirti į ką reikėtų atsižvelgti skiriant investicijas, organizacijos informacijos saugumui, apibrėžti veiklos tęstinumo sąvoka, išvardinti jos privalumus
- ✓ apžvelgti kokie teisiniai aktai Lietuvoje ir Europos sąjungoje yra reguliuoja veiklą susijusią su informacijos apsauga.
- ✓ išanalizuoti, kokia situacija saugos politikos srityje yra Lietuvos organizacijose, taip pat apžvelgti, kokie sprendimai yra siūlomi Lietuvos rinkoje;

Siekiant įgyvendinti darbe užsibrėžtus tikslus, darbas buvo suskirstytas į tris pagrindines dalis.

Pirmoje darbo dalyje apžvelgiamos informacijos saugos sąvokos. Taip pat skiriami ir analizuojami pagrindiniai informacijos saugumo principai. Jie yra labai svarbūs norint suvokti informacijos apsaugos svarbą, nes jei kuris nors iš tų principų yra pažeidžiamas, tolesnė informacijos sauga tampa netikslinga.

Antroje darbo dalyje dėmesys skiriamas pagrindinių saugumo politikos elementų analizei. Pateikiami pagrindinių sąvokų apibrėžimai. Analizuojami saugos politikos formavimo etapai: saugumo strategijos formavimas, pagrindinių procesų dokumentavimas, rizikų įvertinimas, investicijų valdymas, kokios metodikos ir standartai yra naudojami diegiant saugumo politiką, taip pat analizuojamos priežastys, dėl kurių saugumo politika tampa nelanksti, neveiksni ir neatlieka visų numatytų funkcijų. Darbe pateikiama naujausia su saugumo susijusi statistika(investicijos į saugumą, „IT paslaugų outsorsingas“ ir kt.). Pateikiami patarimai kaip užtikrinti įmonės veiklos tęstinumą, kaip valdyti nenumatytas situacijas.

Paskutinėje darbo dalyje apžvelgiami Lietuvos ir ES teisiniai bei rekomendacinio pobūdžio aktai, kurie turi įtakos procesams susijusiems su informacijos apsauga. Įmonės sugebėjimas apsaugoti net tik savo, klientų bei partnerių informaciją, bet ir sugebėjimas užtikrinti savo veiklos nepertraukiamumą, gali jai padėti sutaupyti daug laiko ir resursų. Pateikiama su darbo tema susijusių, Lietuvoje atliktų tyrimų statistika, paminimi Lietuvoje siūlomi sprendimai, įvardijamos įmonės, pasinaudojusios tais sprendimais.

Darbo pabaigoje pateikiamos rekomendacijos, kurios gali būti naudingos įmonėms formuojančios saugumo politiką. Darbo prieduose pateikiama, tyrimų, kuriais buvo remtasi darbe tikslesnė, statistika, ir vieno iš saugumo standartų aprašas . Prieduose pateikta informacija gali būti panaudota, kaip statistinė informacija, naudinga asmenims, besidomintiems informacijos apsauga.

Darbo pradžioje užsibrėžtų uždavinių įgyvendinimui buvo naudotasi sisteminės analizės metodais, su informacijos sauga susijusiais tarptautiniais tyrimais, apžvelgtos tarptautinių asociacijų metodikos ir standartai (COBIT, ITIL, CRAMM, NIST 800 ir kt.). Siekiama pateikti sistemingą informaciją apie organizacijos saugos politiką, jos pagrindinius elementus, geriausias metodikas, rizikų ir investicijų vertinimo metodus, pagrindines problemas. Visa tai gali turėti įtakos užtikrinant sėkmingą organizacijos politikos formavimą. Todėl šis darbas galėtų papildyti informacijos saugos tyrimų sritį. Kuriai visame pasaulyje skiriamas labai didelis dėmesys, tuo tarpu Lietuvoje ši sritis vis nepakankamai ištirta. Rašant šį magistro darbą, buvo stengtasi kuo plačiau pasinaudoti visais galimais informacijos šaltiniais. Remtasi informacija, paskelbta įvairiuose straipsniuose, konferencijų pranešimais, saugumo metodikomis, geriausių praktikų rekomendacijomis. Darbe nagrinėjama sritis Lietuvos organizacijų dar nėra pakankamai vertinama, bet pamažu atsiranda tendencijų, jog organizacijos ima vis labiau suvokti informacijos saugos svarbą pavyzdžiui, galima paminėti Lietuvoje vykstančias tarptautines saugumo tematikos konferencijas, kuriamus specializuotus portalus (eSaugumas), pažangos informacijos ir tinklų saugumo srityje memorandumą ir kt.

Bibliografinių nuorodų sąraše pateikiamos knygos, elektroniniai žurnalai, internetiniuose puslapiuose pateikta medžiaga, kurioje nagrinėjami darbo tematikos aspektai. Šaltiniai yra lietuvių ir anglų kalbomis.

1. INFORMACIJOS SAUGUMO SĄVOKA

Informacija visais laikas buvo vertinama. Tačiau gyvenant informacijos amžiuje, jos vertė padidėjo dar labiau. Todėl ne veltui sakoma, jog tas, kas valdo informaciją, valdo pasaulį. Informacijos vientisumas gali būti pažeidžiamas ne tik vagystės ar tyčinio sunaikinimo būdu. Būtina įvertinti ir atsitiktinumo faktorių, jis dažniausiai apima nenumatytas sistemos klaidas, kurios įvyksta perduodant ar apdorojant duomenis. Taip pat tai gali būti ir žmogiškoji klaida, kuomet duomenys yra suvedami klaidingai. Tokia informacija taip pat gali sutrikdyti organizacijos veiklos nepertraukiamumą ir atnešti nuostolių. Svarbu išsiaiškinti, kaip turimą informaciją galima apsaugoti, kas apskritai yra informacija ir kaip suvokiamos jos ir jos saugumo sąvokos.

Informacija – tai žinios, perduodamos vienų asmenų kitiems žodžiu arba žiniasklaidos priemonėmis: per spaudą, radiją, televiziją, kiną, kompiuterių tinklus.[1]

Informacinė sauga – tai veiksmų ir specifinių priemonių visuma, kuri yra skirta apsaugoti informaciją nuo neautorizuotos prieigos, sunaikinimo, modifikavimo, atskleidimo ir neteisėto panaudojimo. [15]

Informacinė sauga apima duomenų sukūrimo, jų įvesties, apdorojimo ir išvesties procesų apsaugą. Informacinės saugos tikslas - apsaugoti sistemos vertybes, apsaugoti ir užtikrinti informacijos tikslumą ir vientisumą bei sumažinti nuostolius, kurie gali būti patirti, jei informacija būtų modifikuota arba sunaikinta. Norint pasiekti, kad informacija būtų saugi, būtina fiksuoti visus įvykius, kurių metu sukuriama ir modifikuojama informacija, prie jos suteikiama prieiga ar atliekami jos platinimo veiksmai.[9]

Jei įmonėje yra sėkmingai gerinami visi informacinės saugos elementai, tuomet galima tikėtis, kad organizacijoje šie veiksmai bus vykdomi efektyviau:

- bus geriau užtikrinamas (būtina paminėti, kad jokios priemonės negali garantuoti 100 apsaugos) kritinės informacijos konfidencialumas;
- informacijos ir su ja susijusių procesų (kūrimo, įvesties, apdorojimo ir išvesties) vientisumas;
- bus galima prieiga prie informacijos, kai jos reikia;
- geriau vykdoma su informacija susijusių procesų apskaita.[9]

Paskutiniame praeito amžiaus dešimtmetyje informacijos reikšmė verslui, ekonomikai ir visuomenės gyvenimui labai padidėjo. .

Informacijos saugumo problema pamažu tampa vienu iš labai rimtų stabdžių tolimesniam informacinių technologijų vystymuisi ir ypač taikymui. Ne veltui *Microsoft* kompanijos prezidentas Bilas Gates, 2003 metų didžiausioje pasaulyje informacinių technologijų konferencijoje *Comdex* Las Vegase nebepristatinėjo didingų *Microsoft* kompanijos ateities kompiuterių vystymosi ir taikymo vizijų. Visas

jo pranešimas buvo skirtas žemiškiems ir, atrodytų, neįdomiems dalykams: programinei įrangai, galimybei palengvinti ir pagreitinti saugumo skylių lopymą, naujai ugniasienei ar kovos su „spamu“ iniciatyvai.

Tradiciniai kovos su informacijos nutekėjimu, vagystėmis būdai remiasi dviem pagrindiniais metodais: pagal įvairius požymius yra tikrinamas autentiškumas, siekiant užtikrinti, kad informacija būtų prieinama tik legaliems jos vartotojams, ir bandoma kaip galima anksčiau aptikti įsilaužimus. Įprastiniame gyvenime tai būtų spynos ir signalizacijos sistemos. Kompiuteriniuose tinkluose sukurta ir naudojama daug įvairių autentiškumą užtikrinančių, slaptažodžiais, magnetinėmis arba lustinėmis kortelėmis su slaptais kodais, vartotojo biometrine informacija paremtų sistemų.

2. PAGRINDINIAI INFORMACIJOS SAUGUMO PRINCIPAI

Toliau darbe gilinsimės į informacijos saugumo principus. Dauguma šios srities tyrinėtojų ir ekspertų teigia, kad norint užtikrinti informacijos saugumą, reikia išsaugoti jos ***Konfidencialumą, Vientisumą ir Prieinamumą.*** Šie terminai į lietuvių kalbą yra verčiami skirtingai, todėl darbe bus pateikiamos jų reikšmės anglų kalba:

- *Confidentiality*
- *Integrity*
- *Availability.*[38]

Toliau bus detaliau apžvelgiamas kiekvienas iš šių terminų atskirai, bus bandoma išsiaiškinti, kokį poveikį kiekvienas jų turi bendram informacijos saugumui.

2.1 Konfidencialumas (Confidentiality)

Konfidencialumas – tai procesas skirtas užtikrinti, kad su informacija galėtų susipažinti tik tie asmenys, kurie turi teisę su ja susipažinti, ir ji nebus tyčia ar netyčia atskleista kitiems asmenims.[38] Konfidencialumo pažeidimas - tai tyčinis ar netyčinis informacijos atskleidimas pašaliniams asmenims.

Konfidencialumo pažeidimai ir jų keliami pavojai

Paprasčiausi tokio pažeidimo pavyzdžiai - organizacijos konfidencialios informacijos atskleidimas pašaliniams. Konfididencialumo pažeidimą gali sukelti daug veiksnių: įsilaužimas į kompanijos duomenų bazę, papirkus organizacijos darbuotojus, ar dokumentus palikus nesaugomoje vietoje. Konfidencialumo praradimas ne visada baigiasi nuostoliais. Kartais dėl to gali būti sutrikdyta įmonės veikla. Galima paminėti Lietuvos Interneto rinkos kūrimosi laikotarpį, kuomet daug įmonių buvo sujungę savo kompiuterius į tinklus ir apie apsaugą nebuvo galvojama. Prie įmonės duomenų galėjo prieiti bet kuris su informacinėmis technologijomis susipažinęs asmuo.

2.2 Vientisumas (Integrity)

Vientisumas – antrasis saugumo principas, kurio pagrindinis tikslas užtikrinti, kad informacija, kuri yra informacinėse sistemose, nebus pakeista nesankcionuotu būdu, sugadinta arba visiškai prarasta. [38]

Lietuviškuose šaltiniuose šis terminas kartais verčiamas kaip „integralumas“. Su informacijos vientisumu susiję pažeidimai – tai dažniausiai nesankcionuoti prisijungimai prie IS ir joje atlikti pakeitimai, dalinis arba visiškas informacijos praradimas. Prie vientisumo pažeidimų taip pat priskiriami jau minėti nesklandumai, tarp sistemų perduodant duomenis arba kai įsivelia klaida darbuotojams juos įvedinėjant. Šie pažeidimai gali būti tyčiniai arba netyčiniai.

Vientisumo pažeidimai ir jų keliami pavojai

Šis saugumo principas yra sudėtingesnis negu konfidencialumas, nes yra susijęs ne tik su kompiuteriuose saugoma informacija, bet ir su pačiomis informacinėmis sistemomis. Dažniau pasitaikantys vientisumo pažeidimų pavyzdžiai:

- nesankcionuotas prisijungimas prie kompiuterių tinklo, tinklo komponentų parametrų pakeitimas. Piktavaliams asmenims dažnai pavyksta įsilaužti į apsaugotus organizacijos tinklus, prieš tai pakeitus tam tikrus tinklo įrenginių parametrus.
- nesankcionuotas papildomų teisių suteikimas naudotojams. Kartais gudresni naudotojai specialiomis programomis ar kitais būdais gali suteikti sau daugiau teisių, nei numatyta organizacijos saugumo politikoje, taip jie susikuria sau galimybes susipažinti su konfidencialia ar kitiems asmenims priklausančia informacija.
- nesankcionuotas duomenų bazės ar kitų dokumentų įrašų pakeitimas, informacijos sugadinimas. Tokia problema gali nutikti planuojant tyčia, siekiant pakenkti arba netyčia - dėl nežinojimo ar žmogaus klaidos. Taip pat informacija gali tapti nebeprieinama dėl kompiuterių gedimų ir įvairių virusų. [38]

Informacijos vientisumo pažeidimo padariniai gali būti kur kas blogesni, nei anksčiau aprašyti informacinių sistemų konfidencialumo pažeidimai. Pavyzdžiui, galima paminėti situaciją, kuomet organizacija siunčia mokesčių deklaraciją Valstybinei mokesčių inspekcijai. Informacijos perdavimo metu įvyksta klaida ir inspekcija gauna kitus duomenis. Dėl šios klaidos įmonė gali prarasti laiko ir turėti kitų problemų,

Informacijos vientisumo pažeidimo pavyzdžių ir pažeidimo motyvų galima išvardinti daug ir įvairių, nes informacinių sistemų yra labai įvairių. Pateiksime porą pavyzdžių:

- interneto svetainės turinio pakeitimas (angl. *deface*). Tai vienas populiariausių saugumo pažeidimų pastaraisiais metais. Jauni kompiuterių specialistai keičia svetainių turinį daugiausia

iš sportinio intereso, bando sumenkinti konkurentų prestižą. Taip pat „nulaužiamos“ svetainės ir jose skelbiamos įvairios politinės deklaracijos. Nors tokie įsilaužimai dažniausiai turi tik moralinių padarinių, tačiau sulaukia plačiausio atgarsio pasaulyje.

- banko sistemų apgaudinėjimas. Bankai tai neigia ir neigs - nė vienas bankas nenorės pasirodyti nepatikimas ir neleis klientams suabejoti ten saugomų pinigų saugumu. Tačiau ši problema egzistuoja, galima paminėti Lietuvoje neseniai įvykdytą pasikėsinimą iš *Hanza banko* klientų išvilioti slaptažodžius, naudojamus jungiantis prie e-banko. Kol kas nuostoliai buvo nedideli ir bankai neturėjo problemų. Dar galima paminėti tai, kad prieš penkerius metus buvo populiaru pirkti internetu svetimo žmogaus sąskaita. Užsakant pakakdavo nurodyti kredito kortelės numerį, ir prekės atkeliaudavo nurodytu adresu. Dabar bankai apsaugojo klientus nuo panašių pavojų.
- kiti nesankcionuoti įvairių duomenų bazių ir registrų keitimai.

2.3 Prieinamumas (Availability)

Prieinamumas - trečiasis saugumo principas, skelbiantis, kad reikiami informacinių sistemų resursai bet kuriuo metu yra prieinami įgaliotiems asmenims.[38]

Šis terminas dar gali būti verčiamas kaip „pasiekiamumas“, „veiksmingumas“ arba „darbingumas“, tačiau nė vienas iš lietuviškų terminų visiškai neatspindi angliško *availability*.

Prieinamumo pažeidimas – tai pilnas arba dalinis informacinės sistemos darbingumo pažeidimas, dėl kurio informacija ir sistemos resursai tampa nepasiekiami visiems arba daliai jos naudotojų. Siauresne prasme prieinamumas gali būti suprantamas kaip informacinės sistemos darbingumas. [18]

Prieinamumo pažeidimai ir jų keliami pavojai

Prieinamumo pažeidimai dažniausiai susiję su sabotažo aktais. Prie šio tipo saugumo pažeidimų priskiriama:

- kompiuterinės įrangos vagystės;
- ryšio kabelių nutraukimas;
- stichinės ir kitos nelaimės, trukdančios sklandžiam informacinių sistemų darbui (drėgmė, dulkės, žaibas, pastato griuvimas, kitos nelaimės);
- kompiuterinės ir programinės įrangos gedimai, darbo sutrikimai dėl kompiuterinių virusų;
- tyčiniai trukdymai sistemos darbui (sistemos konfigūracijų pakeitimai, puolimas per internetą);
- kiti veiksmai, trikdantys prieigą prie informacinės sistemos resursų. [18]

Gali atrodyti keista, jog sistemų darbingumas, prieinamumas laikomas saugumo problema. Tačiau šie trys prieš tai paminėti principai yra glaudžiai susiję. Jei bent vienas iš jų yra pažeidžiamas, organizacijai iškyla realus pavojus patirti nuostolių. Todėl ir formuojama organizacijos saugumo problema, kuri padėtų išvengti tokių problemų. Kaip pavyzdį galima paminėti problemas, kai prekybos

centre negalima atsiskaityti kreditinėmis kortelėmis. Tai gali nutikti dėl įvairių priežasčių. Tai būtų galima padaryti pranešant, kad kortelėmis negalima atsiskaityti. Taip galima išvengti klientų nepasitenkinimo, ir išvengti nuostolių, bet galima tikėtis, kad klientas, kuris buvo informuotas, sugrįš pirkti į šią parduotuvę.

Saugumo pažeidimų priežastys

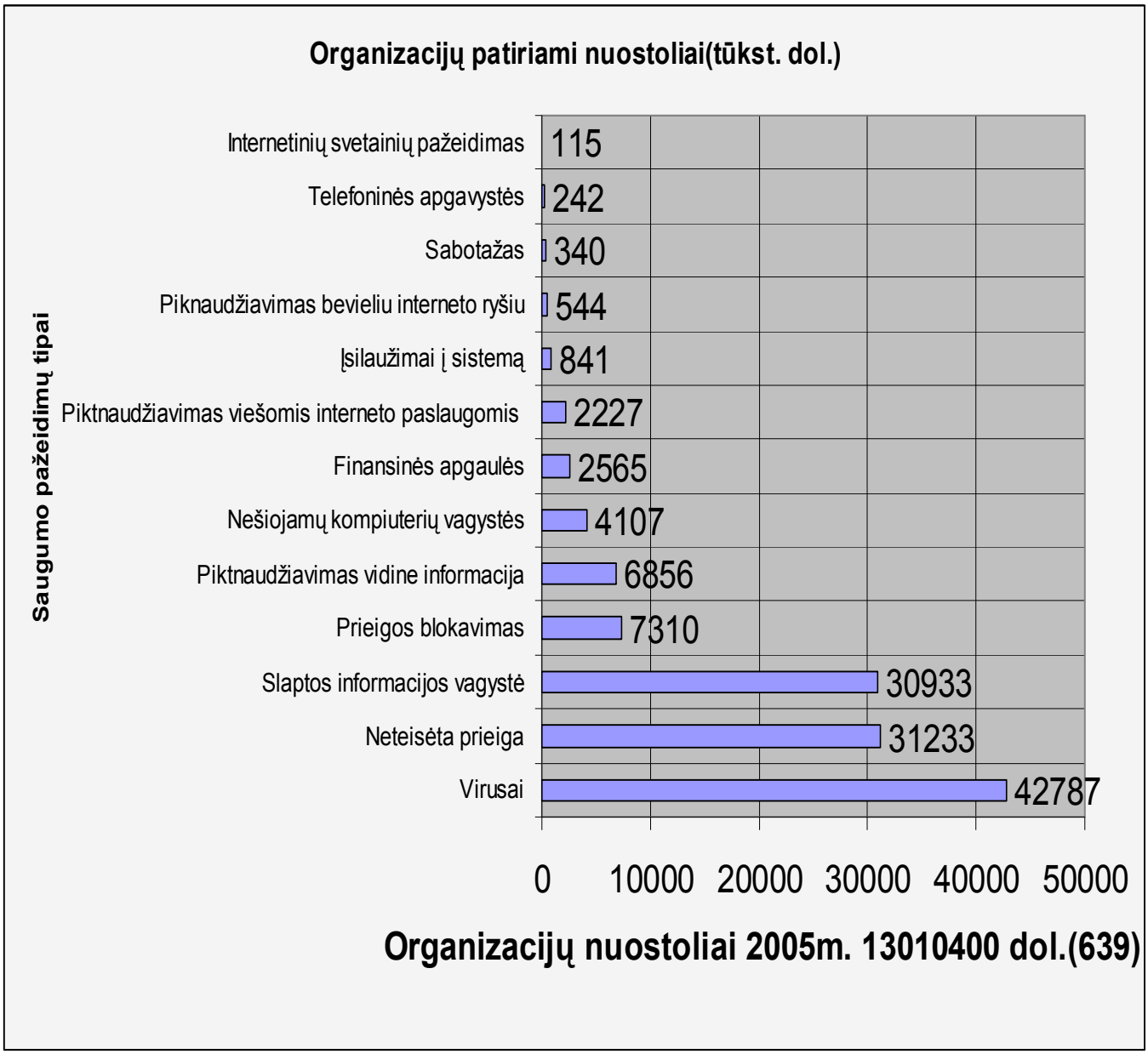
Saugumo pažeidimų priežasčių gali būti daug ir jos visos yra labai įvairios. Toliau pateiksime keletą pavyzdžių:

- siekiant asmeninės naudos (kompiuterinės įrangos ir informacijos vagystės);
- siekiant atkeršyti ar pakenkti;
- iš „sportinio intereso";
- politinė veikla;
- netyčinė pavojinga veikla (nežinojimas);
- kompiuterinės technikos ir programinės įrangos gedimai, kompiuteriniai virusai;
- stichinės ir kitos nelaimės;
- kiti saugumo pažeidimai.[18]

Saugumo pažeidimų rezultatai taip pat gali būti labai įvairūs:

- tiesioginiai finansiniai nuostoliai;
- sumažėja darbo veiksmingumas (atsiranda papildomo darbo);
- reputacijos praradimas. [38]

Toliau bus pateikta JAV organizacijų statistika, kuri atspindi su kokiais saugumo pažeidimų tipais susiduria organizacijos ir kokius nuostolius dėl to patiria. Lietuvoje, deja, nėra atliekami šios srities tyrimai, net ir organizacijos nėra linkusios pateikti tokios informacijos. Didžiausią nerimą kelia žymiai padidėjęs neteisėtos prieigos ir slaptos informacijos vagysčių atvejai. Dėl neteisėtos prieigos 2004 buvo patirta 51547 dolerių nuotolių, o 2005 daugiau kaip 300 000. Slaptos informacijos vagystės 2004 sudarė apie 170000 dolerių, 2005, jau 355000. Specialistai teigia jog šį padidėjimą, lėmė tai kad organizacijos didžiausią dėmesį skyrė kovai su virusais, ir paprasčiausiai neįvertino šių sričių svarbumo.[36]



1 Diagrama. Organizacijų patiriami nuostoliai. **[36]**

3. ORGANIZACIJOS SAUGUMO POLITIKA

Ankstesniame skyriuje buvo apžvelgti pagrindiniai informacijos saugos principai. Paminėti principai neduos jokios naudos, jei organizacijos vadovybė nesidomės saugumo problemomis, nebus diegiama saugumo politika. Todėl siekiant, kad organizacijos informacija nenukentėtų, reikia, kad visas procesas būtų suplanuotas, suderintas, visi organizacijos darbuotojai remtųsi patvirtintais ir visiems žinomais saugumo standartais. Toliau bus apibrėžta saugumo politikos sąvoka ir analizuojamos jos sudėtinės dalys.

Saugumo politika – oficialus vadovybės patvirtintas veiksmų ir taisyklių rinkinys, kurių privalo laikytis visi organizacijos darbuotojai bei kiti asmenys, besinaudojantys organizacijos paslaugomis, informacija ir technologijomis. [9]

Terminas „saugumo politika" atitinka anglišką sąvoką *Security Policy*. Organizacija, investavusi šimtus tūkstančių litų į įvairias modernias technines ir programines saugumo priemones, yra mažiau saugi už organizaciją, kuri turi įsidiegusi ne tokias modernias priemones, bet turi savo saugumo politiką. Skirtumas tarp tų dviejų organizacijų yra tas, kad antroji tiksliai žino, ką saugo ir kokiu keliu jai reikia eiti. Saugumo priemonių pirkimas ir diegimas neturint aiškios saugumo politikos yra neveiksmingas. Tyrėjai išskiria tris pagrindinius organizacijose stebimus saugumo politikų tipus:

- Neegzistuojanti;
- Abejinga;
- Traktatas apie slaptažodžių naudojimą.[38]

Saugumo politikos formuotojai

Saugumo politiką nustato aukščiausia organizacijos vadovybė. Rekomenduojama, kad sudarant saugumo politiką dalyvautų visi arba bent dalis vadovaujančių organizacijos darbuotojų. Saugumo politikos formavimo procese labai didelis vaidmuo tenka IT skyriaus vadovui. Kitų padalinių vadovai didžiausias problemas ir prioritetus mato savo veiklos sektoriuje: vyr. finansininkui svarbiausi yra buhalteriniai duomenys, pardavimo vadovui – ryšių su klientais ir pardavimo sistema, gamybos vadovui – resursų valdymas, IT skyriaus vadovui – nenutrūkstama kompiuterinių sistemų veikla. Todėl lemiamą sprendimą ir politikos kryptį turi nustatyti organizacijos vadovas, nes tik jis geriausiai žino ilgalaikius ir strateginius organizacijos tikslus. [9]

Saugumo politikos aprašymas

Visi saugumo politikos reikalavimai informacinių sistemų ir jose saugomos informacijos saugumui yra aprašomi oficialiame, aukščiausios organizacijos vadovybės patvirtintame – Saugumo politikos dokumente.

Šiame dokumente aprašoma norima pasiekti informacinių sistemų saugumo būklė, konkrečios saugumo sistemos, sprendimai, technologijos, numatytų sistemos darbų atlikimo datos, bendrieji saugumo principai, išvardijama saugoma informacija ir resursai, nustatomi saugumo prioritetai.

Saugumo politikos dokumento reikalavimai turi būti privalomi visiems darbuotojams ir kitiems asmenims, besinaudojantiems organizacijos informacinėmis sistemomis. Todėl šis dokumentas turi turėti statusą, savo galiomis prilygstantį vadovo įsakymui.

Saugumo politikos dokumento nauda

Šis dokumentas, kaip jau minėjome, yra labai svarbus. Neturint galiojančio saugumo politikos dokumento, nesukonkretinus ir neužfiksavus saugumo reikalavimų, duomenų saugos priemonių įsigijimas ir diegimas gali būti netikslingas ir neefektyvus, neatitinkantis strateginių organizacijos tikslų. Jei organizacija turės galiojantį saugumo dokumentą, kuris padės sutaupyti organizacijos laiko ir lėšų, jis jai labai pravers sprendžiant saugumo klausimus ateityje. Šio dokumento privalumus galima iliustruoti šiais pavyzdžiais.

- iškilus tam tikriems su saugumu susijusiems klausimams kartais pakaks paskaityti Saugumo politikos dokumentą, o ne kiekvienu atveju trukdyti aukščiausią vadovą, laukti, kol jis galės skirti laiko susidariusiai situacijai išspręsti.
- turint aiškius ir aukščiausio vadovo parašu patvirtintus saugumo reikalavimus, galima pradėti įsigyti reikalingas saugumo priemones, planuoti biudžetus. [9]

Šis dokumentas, priklausomai nuo organizacijos tipo, dydžio, veiklos ir kitų veiksnių, gali būti kelių arba kelių šimtų puslapių dydžio.

Saugumo politikos dokumentas gali apimti visą organizacijos turimą informaciją (rašytinę, spausdintinę, žodinę ir t. t.). Ir atvirkščiai – informacinių sistemų saugumo reikalavimai gali būti įtraukti į visuotinį organizacijos saugumo politikos dokumentą. Kuriant šį dokumentą rekomenduojama pasisamdyti tos srities profesionalus: gautas rezultatas bus kokybiškesnis, pasikeis vadovaujančių darbuotojų požiūris į saugumą, bus gauti objektyvesni įvertinimai, pateikti profesionalūs pasiūlymai, kaip spręsti vienas ar kitas problemas (pavyzdžiui, kaip klasifikuoti informaciją, kaip paskirstyti naudotojus).

Labai klaidinga nuomonė yra ta, kad kai dokumentas yra sukurtas, nieko daugiau jau nebereikia daryti. Tačiau reikia nepamiršti, kad keičiantis organizacijos veiklai, informacinėms sistemoms, aplinkai, keičiasi ir saugumo reikalavimai, todėl šį dokumentą reikia nuolat (bent kas porą metų) peržiūrėti ir

pakoreguoti, kad jis atitiktų organizacijos tikslus. Reikia nepamiršti, kad organizacijos saugumo politikos palaikymas yra besitęsiantis nuolatinės priežiūros reikalaujantis procesas.

3.1 Organizacijos saugumo strategijos formavimas

Organizacijos saugumo politikos formavimas, tai procesas reikalaujanti daug laiko ir pastangų. Todėl norint, kad jis būtų įgyvendintas sėkmingai, visi susiję veiksmai turi būti atliekami nuosekliai. Toliau bus pateikiamas saugumo strategijos apibrėžimas

Informacijos saugos strategija – tai veiksmų rinkinys, apjungiantis organizacijos veiklos tikslus, informaciją šiems tikslams pasiekti ir organizacijos kompiuterines sistemas. [26]

Organizacijos vadovybei suvokus informacijos saugumo principus, įvertinus kokius nuostolius galima patirti jei jie bus pažeisti, galima pradėti formuoti saugumo strategiją.

Ypač didelę svarbą informacijos saugos strategija įgijo išaugus technologijų vystymosi tempams. Remdamasi organizacijos poreikiais, strategija nurodo tikslus, nedetalizuodama jų pasiekimui taikytinų technologijų.

Veiksmingam strategijos įgyvendinimui svarbus yra ir organizacijos lankstumas – lemiamą reikšmę jis turi neišvengiamai iškilus situacijoms, kurių neįmanoma numatyti.

Specialistai(Isect Ltd., Dr. Gary Hinson), dirbantys su informacijos saugumo valdymu, išskiria ir pabrėžia, koks svarbus yra ryšys tarp informacijos saugumo kontrolės pagerinimo ir rizikų sumažinimo, bei teikia rekomendacijas, kaip šiuos procesus reikėtų sureguliuoti.[33] Tačiau dažnai organizacijose pasitaiko tokių situacijų, kuomet vadovybė investicijas į saugumą laiko eilinėmis nereikalingomis išlaidomis. Dėl to susidaro, tokia situacija, kad informacijos saugumo įgyvendinimas, tarsi nukeliamas į antrą planą. Pirmenybė skiriama kitoms veikloms ir kitiems procesams. Todėl (Isect Ltd.) organizacijos specialistai išskyrė 6 pagrindinius saugumo strategijos žingsnius, kurių laikantis galima pasirinkti geresnius sprendimus ir organizacijai priimtinesnes priemones. Saugumo strategijos žingsniuose aprašyti veiksmai ir rekomendacijos jau yra praktiškai realizuoti užsienio įmonėse. Todėl užsienio kompanijų patirtis, valdant organizacijos informacijos saugumą, galėtų būti naudinga mažiau patirties turinčioms organizacijoms. Taip galima sutaupyti laiko ir resursų bei sukurti geresnę organizacijos saugumo struktūrą, tiksliau apibrėžti funkcijas bei išvengti dalies potencialių problemų. Žinoma, šie strategijos žingsniai negali šimtu procentų garantuoti, kad ja remiantis sėkmingai pavyks įgyvendinti gerą saugumo politiką visose organizacijose. Tačiau suformuoti strategijos žingsniai gali būti naudingi ir sukelti minčių kaip geriau valdyti saugumo formavimo procesą. Taigi šie žingsniai yra svarbus etapas, prieš pradedant kurti organizacijos informacijos politiką.

Strateginis požiūris, kuris veikia

Nepriklausomai nuo to, ar informacijos saugumas tik pradedamas kurti, ar tobuliname esanti sistema, rekomenduojama suplanuoti tiek ilgalaikius, tiek trumpalaikius veiksmus, numatyti jų įvykdymo planą, nenumatytų situacijų sprendimą ir kt. Veiksmai atliekami trumpuoju–taktiniu laikotarpiu, gali pagerinti siaurų sričių veiklos įgyvendinimą, taip pat suteikti informacijos apie didesnes ir sudėtingesnes problemas. Tokio tipo informacija turi būti perduodama atitinkamiems asmenims, nes jei ji bus sena, gali iškilti pavojus informacijos saugumui.

Toliau pateikiamų strategijos žingnių, tyrinėtojai (Dr. Gary Hinson) nevertinio griežtais laiko intervalais

Organizacijų aplinka nuolat keičiasi, todėl sunku įvertinti, kiek laiko reikės strategijai įgyvendinti. Jei ji bus bandoma įdiegti didelėse organizacijose, tam gali prireikti kelerių metų, jei – mažose, tai galima įvykdyti greičiau.

Pirmas žingsnis: Pagrindinių kontrolės taškų įgyvendinimas

Specialistai šiame etape, akcentuoja investicijų svarbą. Organizacija turi turėti finansinių pajėgumų keisti nusistovėjusią tvarką ir įgyvendinti naują projektą. Taip pat svarbu ištirti esamą situaciją, ar saugumu buvo rūpinamasi anksčiau. Jei informacijos saugumui nebuvo skiriamas dėmesys, organizacijoje gali būti daug įvairių problemų. Jas būtų galima pašalinti tokias būdais:

- pradėti šalinti, pačias seniausias problemas, tai daryti bendromis visos organizacijos pastangomis;
- Organizacijos vadovams pateiki duomenis, statistiką, kuri padėtų įrodyti, kad naujais metodais problemas gali išspręsti greičiau. Turint tokią statistiką, bus lengviau gauti reikalingas investicijas.[33]

Bazines saugumo priemones galima įsigyti, tam neskiriant per ne lyg didelių investicijų. Taip pat kai yra kuriama strategija, rekomenduojama atsižvelgti į tai ar organizacijos saugumo tikslai, atitinka bendrą įmonės strategija ir jos tikslus. Vienas iš populiaresnių naudojamų standartų yra **ISO 17799 (BS7799)**. Jame yra pateikiama daug praktinės informacijos, kuri naudinga formuojant saugumo strategiją. Galima paminėti tokius šio standarto pateikiamos informacijos elementus:

- organizacijos informacijos saugumo funkcija turi būti suderinta su vyresniąja vadovybe, už jos palaikymą turi būti atsakingi kompetentingi darbuotojai.
- Ar organizacijoje yra gera fizinė apsauga: geri durų užraktai, storos sienos ir kt.?
- Ar daromos atsarginės duomenų kopijos, ar jos saugomos, ar tikrinama kaip veikia atsarginių kopijų darymo mechanizmas?

- Ar į organizacijos sutartis, kontraktus įtraukti kitų šalių įsipareigojimai saugumo klausimais?
- Ar organizacijoje yra naudojama slaptažodžių politika?
- Ar naudojama antivirusinė įranga, ar ji reguliariai atnaujinama ?
- Saugumo aspektai turi atsispindėti organizacijos operacijose ir procedūrose.
- Ar organizacijoje vykdoma programa, kurios tikslas didinti darbuotojų žinias apie informacijos saugumą, ar visi darbuotojai turi galimybę ja pasinaudoti?
- Ar informacijos saugumas įdiegtas į sistemos vystymo ir testavimo procesą ?

Išanalizavus pradinę situaciją, organizacijoms rekomenduojama pačias svarbiausias problemas spręsti iš karto, nelaukiant pilnos rizikos analizės.

Organizacijai bus lengviau vertinti saugumo svarbą jei ji atsižvelgs į toliau pateikiamus etapus:

- Organizacija rekomenduojama turėti sąmatą, kurioje atsispindėtų suplanuotos investicijos, taip pat sugebėti įvertinti netikėtai atsiradusių investicijų veiksmingumą ir kokią pridėtinę vertę jos suteiks organizacijai
- Vertinant saugumo svarbą, būtina apžvelgti kuo daugiau elementų kuriuos ta sauga apims, taip bus sudaromas tikslesnis vaizdas, ir bus lengviau įvertinamas investicijų į saugą dydis.
- Organizacijos sukaupti duomenys apie saugumo spragas gali būti naudojami kaip argumentai, jog esamą situaciją reikėtų gerinti. Taip pat reikėtų numatyti ir įvertinti išlaidas, kurios atsiras tobulinant valdymą ir išvengiant pasikartojančių problemų. [32, p.23]

Organizacijose kuriose yra formuojama saugumo strategija, rekomenduoja supažindinti visus darbuotojus su naujai atsirasiančiomis atsakomybėmis (*t.y.* informacijos saugumas, fizinis saugumas, rizikos vertinimas ir kt.). Vadovybė turėtų kontroliuoti vykdomus veiksmus, ir šalinti iškylančius netikslumus.

Antras žingsnis: saugumo rizikų analizė

Rizikos analizė yra sudėtingas procesas nuo kurio labai priklauso organizacijos sėkmė. Todėl jis bus detaliau analizuojamas atskirame darbo skyriuje.

Trečias žingsnis: verslo paruošimas pasikeitusiai kontrolei

Šiame strategijos žingsnyje būtina aptarti tuos pakeitimus, kuriuos tikimasi atlikti. Svarbu įvertinti ar tie nauji pakeitimai bus efektyvūs. Atnaujinimo darbus rekomenduojama pradėti nuo organizacijos procedūrų tobulinimo. Nes vien jau pačių procesų patobulinimas duos teigiamų rezultatų. Dr. Gary Hinson nuomone, procedūrinė kontrolė, turėtų apimti rutinines saugumo užduotis slaptažodžių keitimą, antivirusinės įrangos atnaujinimą ir kt. Organizacijai išanalizavus savo procesus ir nusprendus, jog jų patobulinimui yra būtina įsigyti procesus galinčių modernizuoti priemonių. Būtina nepamiršti parengti personalą, darbui su naujomis priemonėmis, tai savo ruožtu padės padidinti šių priemonių veiksmingumą.

- organizacijos vadovybė turėtų rengti mokymus darbuotojams, kuriuose būtų identifikuojami pagrindiniai įmonės resursai, ir kaip juos reikėtų saugoti. Taip pat perteikti darbuotojams, kad jie taip pat yra informaciniai įmonės ištekliai, ir kad jie taip pat turėtų saugoti savo turimas žinias.
- įmonėje turi būti įsidiegusi veiklos tęstinumo rizikos valdymo sistema, kuri padėtų sumažinti nuostolius, jei organizaciją ištiktų nenumatytos problemos. Apie veiklos tęstinumo valdymą bus kalbama atskirame skyrelyje

Ketvirtas žingsnis: organizacijos informacijos saugos programa

Kai organizacija įvykdo prieš tai analizuotus tris strategijos žingsnius, galima pradėti įmonės saugumo tobulinimo programą. Ji dar kitaip vadinama metiniu informacijos saugumo planu. Šiame plane yra suderinti visi pagrindiniai ir smulkesni su saugumu susiję elementai.

Rekomenduojama įsitikinti, ar organizacija turi pakankamai išteklių įgyvendinti savo suplanuotai programai. Būtina stebėti kaip diegiami pasirinkti sprendimai, ar viskas atliekama laiku, ar jie atitinka įmonės veiklos specifiką, ir jei procese pastebimi nesklandumai, būtina juos pašalinti. Įmonėje, turi būti numatytas lėšų fondas, kuris būtų panaudojamas, jei diegimo metu būtų susiduriama su nenumatytomis išlaidomis.[33]

Penktas žingsnis: saugumo programos vykdymo kontrolė ir rezultatų pateikimas

Vykdomai programai turi būti skiriamas toks pat dėmesys, kaip ir prekybai, logistikai ir kitiems organizacijoje vykstantiems darbams. Sėkmingas programos įgyvendinimas galimas tuomet kai yra parengti tinkami projektiniai planai, vykdoma biudžeto kontrolė, vertinami pasiekti rezultatai ir kt.

Rekomenduojama surinkti kompetentingą organizacijos saugumo komandą, kuri savo veikloje naudotų geriausias saugumo praktikas ir produktus, kurie duotų ilgalaikės naudos organizacijai. Šiame etape turi būti suformuota ir vystoma informacijos saugumo infrastruktūra, kurią rekomenduojama vystyti kartu su organizacijos strategija. Taip pat apibrėžiama esama, ir kokia bus pagerinta informacijos saugumo kontrolė.

Šeštas žingsnis: pasiektos pažangos vertinimas

Paskutinis strategijos žingsnis iš esmės yra rekomendacinis, jame patariama nuolat peržiūrėti ir naujai įvertinti informacijos apsaugos aspektus, atsižvelgti į besikeičiančią verslo aplinką, atsirandančius naujus pavojus.

Jei nusprendžiama remtis kitos įmonės paslaugomis, turi būti numatyti ir paslaugos sutartyje išskirti šalių įsipareigojimai ir atsakomybės. Taip pat jei matoma, kad projektas yra netikslus, būtina jį patobulinti.

Taip pat būtina atkreipti dėmesį ar su duomenimis dirba tik atitinkamus prieigos leidimus turintis personalas. Nes pasitaiko situacijų kurių metu žmonės, kurie turėtų būti atsakingi tik už procesų ir sistemų priežiūra, gali prieiti prie jiems nepriklausančių duomenų. Apibendrinant galima teigti, kad organizacija atsižvelgianti į išvardintus strategijos žingsnius gali tikėtis, kad jos saugumo programa bus sėkminga ir taps viena iš gerai funkcionuojančių saugumo politikos dalių. [33]

3.2 Saugumo procesų dokumentacija

Kai įmonėje yra apibrėžta saugumo politikos sąvoka, žinomi jos privalumai, pasiremiant svarbiausiais žingsniais sukurta saugumo strategija, galima pradėti įmonės saugumo procesų dokumentaciją.

Organizacijos saugumo dokumentacija - tai jos politikos, architektūros, standartų, nurodymų, procesų ir kt. visuma, kuria remdamasi organizacija gali geriau apsaugoti savo svarbiausius duomenis, lengviau įsidiegti apsaugos standartus, nenukrypstant ir nepakenkiant organizacijos tikslams. [27, p.107]

Toliau bus pateikiami išskiriami svarbiausi elementai kuriuos organizacijos turėtų dokumentuoti:

- Saugumo politika;
- Informacijos išteklių vertinimas;
- Sistemos ir jų aplinka;
- Atsakomybės sritys;
- Saugumo sistemos ir procedūros;
- Įrašai, ataskaitos ir jų archyvavimas;

- Saugumo auditas ir verslo tęstinumo planavimas;
- Standartų laikymasis.

1. Politika

Saugumo politikos sąvoka ir pasitaikantys jos tipai buvo apžvelgti darbo pradžioje. Čia bus pateikiamos tik tos rekomendacijos, kurios turėtų būti dokumentavimo fazėje. Organizacijos saugumo pareigūnai turi būtinai konsultuotis ir bendrauti tiek su įmonės vadovais, tiek su darbuotojais. Šių veiksmų dėka galima geriau ištirti ir tiksliau dokumentuoti esamus ir planuojamus organizacijos veiksmus. Vykdoma dokumentacija, padės lengviau įvertinti ir numatyti kokie sprendimai ir procesų pakeitimai gali turėti įtakos organizacijos saugumui.

Turi būti dokumentuojama ar jų vykdoma veikla, veiksmai, kuriamos saugumo politikos atitinka teisinius ir tarp organizacijų, partnerių sudarytų sutarčių reikalavimus

Visi paminėti veiksniai gali turėti vienokios ar kitokios įtakos informacijos saugai. Organizacijų vadovams rekomenduojama, įtraukti į dokumentaciją savo, tiek ir samdomų darbuotojų prieigą prie informacijos, jų galimybes ta informacija disponuoti. Tai padės išvengti nereikalingų išlaidų ir įmonės veiklos sutrikdymo.[32, p.108]

2. Informacijos išteklių įvertinimas

Kaip jau buvo užsiminta darbe, turi būti įvertinti informacijos resursai paskirtos atitinkamos teisės dirbti su vienokia ir kitokia informacija. Svarbiausi informaciniai ištekliai turėtų būti identifikuoti ir išskirti vadovybės. Jei prieigos prie informacijos bus paskirstytos netinkamai, galimas informacijos konfidencialumo praradimas, bus pažeistas jos vientisumas, taip pat kurį laiką jie gali būti nepasiekiami, o tai gali sukelti veiklos sutrikimų.

Organizacijos rekomenduojama, jei yra galimybių, pavaizduoti informacinės sistemos, duomenų ir informacijos saugojimo, apdorojimo ir perdavimo procesus. Dokumentuojant problemas, susijusias su informacijos saugumu, reikėtų nepamiršti ir bent minimaliai dokumentuoti verslo procesus.[29]

3. Sistemos ir jų aplinka

Šioje dokumentacijos dalyje, turi būti pateikiami vertinimai ir charakteristikos su IS susijusiais visais organizacijos procesais ir įrenginiais. Problemos dažniausiai atsiranda, kai reikia nuolat atnaujinti dokumentaciją, tai ypač sunku padaryti didelėse tinklinėse organizacijose. Todėl didelių organizacijų IT departamentams rekomenduojama reikiamą dokumentaciją teikti elektroniniu būdu. Jei iškiltų papildomų duomenų poreikis, tuomet saugumo darbuotojai kreiptųsi reikiamos informacijos į savo departamentą.

Jei saugumo sistemos dokumentacija vykdoma pagal visus reikalavimus, tuomet darbuotojai yra laiku supažindinami su aktualia informacija. O tai savo ruožtu padeda palaikyti priimtiną saugumo lygį.

4. Atsakomybės

Kaip jau minėta darbo pradžioje, organizacijos informaciją turi vertinti jos vadovybė . Ji turi suvokti, jog jos praradimas arba netinkamas panaudojimas, gali turėti labai neigiamų padarinių. Todėl ir organizacijos saugumo politika, ir saugumo sistemos nebus efektyvios, jei įmonėje saugumui nebus skiriamas pakankamas dėmesys. Geros praktikos rekomendacijos, teigiama, kad atsakomybių dokumentą turėtų parengti asmenys atsakingi už saugumą, ir parengtą dokumentą teikti patvirtinti vadovybei.

Tokiu būdu lengviau galima valdyti prieigą prie informacijos, specialistai gali konsultuoti organizacijos darbuotojus ir atsakyti į jiems aktualius klausimus. Dokumentacijoje turi būti numatyti darbuotojų mokymai, jų dalyvavimas ir už tai atsakingas asmuo. Turi būti atkreiptas dėmesys į sutartis, kurios yra sudaromos su trečiosiomis šalimis dėl įvairių paslaugų. Jei organizacijoje įvyktų incidentas, pažeidžiantis nustatytas saugumo normas, remiantis saugumo dokumentacija turėtų būti galima nustatyti tokius faktus:

- identifikuoti darbuotojus, kurie nesilaikė nustatytų organizacijos saugumo normų.
- taip pat kokios saugumo normos buvo pažeistos ir kokios už tai yra numatytos nuobaudos.

5. Saugumo sistemos ir procedūros

Šioje saugumo dokumentacijos dalyje, turi būti aiškiai išdėstytos ir aprašytos sistemos sudedamosios dalys: ugniasienės, VPN, autentifikavimo kortelės, antivirusinė programinė įranga, slaptažodžiai ir kt. Didžioji šios informacijos dalis yra susijusi su kitų procesų dokumentacija, todėl reikia stengtis, kad visa tai būtų suderinta. Asmenys, atsakingi už informacijos saugumą, turi turėti tokią prieigą kuri atitiktų jų pareigas. Jie jų pareigos yra prižiūrėti informacijos sistemą, tai tą jie ir turi daryti, o ne stengtis išsiaiškinti kokie duomenys yra perduodami. Šioje vietoje galima paminėti IT administratorių problemą.

Šiandien rinkoje labiausiai paplitusios „Microsoft Windows" tinklo operacinės sistemos. Šiose sistemose (kaip, beje, ir beveik visose kitose) IT administratorius yra visagalis: jis gali „nepastebėtas" prieiti prie bet kokios informacijos, perskaityti visus laiškus, susipažinti su slapčiausiais organizacijos duomenimis, padaryti nelegalias jų kopijas ar net išsiųsti Internetu. Ir niekas to nepastebės. IT administratorius gali net išsiųsti laišką kito asmens vardu.

Ištrynus pėdsakus („logus") net aukštos kvalifikacijos audituojantis IT specialistas negalės nieko pasakyti apie atliktus blogus veiksmus. Deja, šiuo metu jokio veiksmingo priešnuodžio šiam pavojui nėra. Todėl IT administratorių patikimumo ir pasitikėjimo jais klausimas turi būti sprendžiamas nuo pat jų priėmimo į darbą.

Pagrindinis kriterijus priimant administratorių dažniausiai yra jo kvalifikacija ir patirtis. Darbo patirtis dešimtyje bendrovių neretai priimama kaip didelis privalumas, neužduodant sau klausimo, kodėl jis taip dažnai keičia darbą. Kartais administratoriaus patikimumas gali būti svarbesnis nei jo aukšta kvalifikacija.

Tarp aukščiausios organizacijos vadovybės ir IT administratorių turi būti pasitikėjimas, antraip informacijos galbūt geriau visai nesaugoti kompiuteriuose.[9]

Vykdant šios srities dokumentaciją saugumo vadybininkai dažniausiai susiduria su šiais klausimais:

- Kaip saugumo sistemos ir procedūros yra susiję su kitomis sistemomis ir organizacijos aplinkos dokumentacija?
- Kokia šių saugumo procedūrų ir sistemų įtaka organizacijai, kokios organizacijos vertybės, kaip ir kas jas saugo nuo pavojų?
- Kokie gali būti pavojai, kurie yra nepaminėti saugumo sistemos procedūrose?
- Ar organizacijoje yra naudojamasi geriausių praktikų pavyzdžiais?
- Ar sudarytas veiksmų planas, kaip reaguoti į netikėtus pažeidimus ir atakas? [29]

Į šiuos klausimus galima atsakyti, tik atlikus nuoseklų saugumo politikos auditą. Jo dėka galima geriau identifikuoti ir dokumentuoti sistemos fizinius ir loginius elementus, pagrindinius pažeidžiamumus, kaip

vertinama informacija ir kt. Taip pat būtina dokumentuoti saugumo auditą, nes tai gali būti naudinga ateityje, sprendžiant panašias problemas.

6. Įrašai, ataskaitos ir jų archyvavimas

Organizacijos vadovybė turėtų dokumentuoti teisinius reikalavimus. Šios srities dokumentacijoje turėtų

būti numatyta, kaip bus tvarkomi organizacijos finansiniai pervedimai, atsiskaitymai, duomenys apie sutartis su kitomis organizacijomis, įstatyminiai nuostatai. Kiekvienoje organizacijoje vyksta daug veiksmų ir procesų, todėl reikia nepamiršti, kad visos įmonės dokumentacijos turi būti susiję.

Organizacijoje esanti dokumentacija gali būti naudinga iškilus teisinėms ir kitokioms problemoms. Visi duomenys turi būti nuolat atnaujinami ir pasiekiami bet kuriuo metu, iškilus krizinei situacijai.

7. Saugumo auditas ir verslo tęstinumo planavimas

Jei yra tobulinama ar kuriama nauja organizacijos politika, rekomenduojama atlikti organizacijos auditą. Todėl, jei įmonėje prieš auditą buvo rengiama organizacijos procesų dokumentacija, auditas vyks greičiau ir bus gautos tikslesnės ataskaitos. Jos naudingos gerinant organizacijos saugumo politiką, ataskaitų dėka galima geriau identifikuoti pagrindines problemas ir gauti rekomendacijas,

kaip jas pašalinti. Darbuotojams rekomenduojama dokumentuoti net tik ataskaitas, bet ir sekti vykdomus veiksmus organizacijoje, taip pat atkreipti dėmesį į naujausias tendencijas ir rekomendacijas, stebėti pasikeitimų vykdymo grafiką, perteikti vadovybei, kaip įgyvendinami procesai, kurie iš jų jau įgyvendinti, kurie dar ne ir kokios problemos tai trukdo padaryti.

8. Nustatytų reikalavimų laikymasis

Paskutiniame dokumentacijos etape pateikiami duomenys, pagal kuriuos organizacijos vadovybė gali matyti, kaip vyksta organizacijos saugumo politikos formavimas. Ar yra įgyvendinami visi strategijoje numatyti tikslai, su kokiomis problemomis susiduriama, kokios praktikos naudojamos, ar darbuotojai laikosi nustatytų reikalavimų, ar buvo iškilę nenumatytų problemų ir kt. Galima sakyti, jog tai apibendrinanti dalis, kurią rekomenduojama nuolat tobulinti viso projekto metu. [29]

3.3 Organizacijos rizikų analizė

Organizacijos vadovybė kurdama savo saugumo politiką, turi labai gerai įvertinti su kokiomis rizikomis organizacijai teks susidurti, kurios iš jų pavojingiausios, kokią įtaką jos gali padaryti, taip pat kaip reikėtų reaguoti į jas ir kt. Taigi prieš pradedant bet kokį darbą naudinga apibūdinti siekiamą tikslą. Lygiai taip pat prieš diegiant saugumą įmonėje, investuojant nemažas sumas į įvairius saugumo sprendimus, labai naudinga numatyti, ką norime apsaugoti. Priešingu atveju tai bus „darbas dėl darbo", t. y. be aiškaus tikslo. Kaip jau buvo analizuota pirmasis žingsnis yra gana paprastas - tereikia išvardyti informaciją ir tarnybas (dar kitaip vadinamas resursais), kuriuos reikia apsaugoti.

Kadangi darbe analizuojama tema yra glaudžiai susijusi su IT, būtina paminėti kas yra IT rizika. IT prasme rizika - tai galimų nuostolių, kurie gali įvykti dėl sumažėjusios paslaugų kokybės, neįvykdytų užduočių ar tiesiog neveikiančių informacinių paslaugų, tikimybė. Rizika, glaudžiai susijusi su IS naudojimo sprendimais, gali būti suprantama kaip vertės praradimo galimybė pasikeitus informacinės sistemos funkcijoms, suprastėjus kokybei ar kai nėra kontrolės.

Toliau pateikiami pagrindiniai su rizikos analize susiję terminai:

Rizikos analizė - tai rizikos lygio identifikavimas, apskaičiuotas įvertinant turto vertę ir jam gresiančių pavojų bei pažeidžiamumo lygį. [9]

Rizikos identifikavimas – tai pirmasis žingsnis rizikos valdymo procese, sudarytas iš sąlygų ir rezultatų. Rizikos identifikavimas turi apimti riziką, susijusią su žmonių veiksmais, procesais, technologija ir aplinka. Rizikos identifikavimo rezultatas turėtų būti rizikų sąrašas. [9]

Rizikos valdymas - tai kontrpriemonių, parinktų pagal įvertintas rizikas, gresiančias turtui, identifikavimas, atranka ir pritaikymas, leidžiantis sumažinti tas rizikas iki priimtino lygio.[38]

Rizikos valdymo procesas

Pirmasis žingsnis rizikos valdymo procese turėtų būti – rizikos nustatymas kurį sudaro sąlygos ir rezultatai. Rizikos nustatymas turi apimti riziką, susijusią su žmonių veiksmais, procesais, technologija ir aplinka, o rezultatas turėtų būti rizikos sąrašas.

Vertinant, kokie gali būti organizacijos nuostoliai, reikia atsižvelgti į kelias sritis:

- Išlaidos. Informacinės sistemos infrastruktūra gali veikti nepriekaištingai, bet ji bus per brangi ir neatsipirks
- Našumas
- Pajėgumas
- Saugumas

Informacinė sistema gali neapsaugoti organizacijos informacijos arba būti nepakankamai lanksti bei neužtikrinti priėjimo prie jos. Sekantis organizacijos žingsnis, tai pradėti galvoti apie IT rizikos valdymą ir rizikos valdymo kultūra organizacijoje. Ją turi palaikyti organizacijos vadovybė, ir tai turi tapti visų darbuotojų darbo dienos dalimi. Šios kultūros tikslas - kad organizacijos rizikos valdymas taptų kasdiene visų darbuotojų veikla, kuri užkirstų kelią nuostoliams ir organizacijai leistų instinktyviai priimti veiksmingus sprendimus. Sunkumai diegiant IT rizikos valdymą organizacijoje dažniausiai yra susiję su tuo, kad:

- rizikos valdymas yra per daug kompleksiškas ir nesuprantamas.
- nėra darbuotojų motyvacijos.
- informacinės sistemos naudotojai ir susiję asmenys (angl.*Stakeholders*) nemato naudos.
- aukščiausia organizacijos vadovybė nepalaiko šios iniciatyvos.[9]

Pagrindinis rizikos valdymo tikslas - ne kaip galima geriau taisyti klaidas, bet jų išvengti. Išankstinis rizikos valdymas organizacijoje gali būti vykdomas sukuriant rizikos valdymo komitetą, kaupiant informaciją apie sistemos klaidas ir jų sprendimo būdus. Tai reikalauja daug pastangų, o rezultatai dažniausiai būna neapčiuopiami ir sunkiai pamatuojami (nieko blogo neįvyksta).

Rizikos analizės procesas

Sėkminga rizikos analizė priklauso nuo daugelio įvairių veiksnių. Tai aiškiai apibrėžta apimtis, galiojantys dokumentai, nešališkumas, rizikos analizės proceso brandumas, informacijos ir duomenų apsaugos užtikrinimo metodai ir organizavimas, rizikos analizėje dalyvaujančių darbuotojų kompetencija, patirtis ir jų vaidmuo organizacijoje. Rizikos analizė yra privalomas procesas kiekvienai organizacijai, siekiančiai valdomo saugumo. Būtina atsižvelgti į šias rizikos rizikos analizės proceso savybes:

- saugumo politika, uždaviniai ir veiksmai turi atspindėti organizacijos uždavinius;
- diegiamos saugos priemonės turi atitikti organizacijos kultūrą;
- būtina akivaizdi vadovybės parama ir dėmesys;
- būtinas geras saugumo reikalavimų, rizikos analizės ir rizikos valdymo supratimas;
- būtinas efektyvus saugumo reikšmės išaiškinimas visiems vadovams ir darbuotojams;
- duomenys apie informacijos apsaugos politiką ir standartus turi būti išplatinta visiems darbuotojams ir rangovams;
- būtina užtikrinti reikalingą švietimą ir mokymus;[2, p.15-21]

Norint, kad rizikos analizė būtų sėkminga, reikia pastebėti, jog vadovybė turėtų įvertinti savo organizacijos brandumą. Tai yra vienas iš svarbiausių elementų, kurie gali turėti didelės įtakos saugumo analizei. Toliau darbe bus pristatomi organizacijos brandos modeliai (juos analizuojant remtasi COBIT IT valdymo metodologija).

Organizacijos brandumas - tai įgūdžių visuma, įgalinanti efektyvų procesų įgyvendinimą.
Šio modelio pagalba galima nustatyti, ar organizacija yra pajėgi įgyvendinti procesus, planuoti tų procesų tobulinimo būdus ir taikyti procesų įgyvendinimo priemones, atitinkančias jos brandumo lygį. Brandumo
modelis yra patogus tuo, kad juo brandumo lygį gali nustatyti pati organizacija. Sugebėjimų brandumo modelis buvo sukurtas ir paskelbtas 1995 m. Carnegie Mellon universiteto Programinės įrangos kūrimo institute Pitsburge, JAV.
Modelio pagrindinis uždavinys buvo užtikrinti sisteminį požiūrį į programinės įrangos kūrimo procesų tobulinimą. Tačiau sukurtas modelis buvo patogus ir paprastas naudoti, todėl jį pradėjo naudoti kiti specialistai (pvz., CobIT IT valdymo metodologija), nes jis leido atsakyti į klausimą, kodėl vienoje organizacijoje veiksminga procedūra, kitoje pasirodo visiškai neefektyvi ar net kenksminga. Tai galima paaiškinti tuo, kad kiekviena organizacija funkcionuoja skirtingoje aplinkoje, todėl kiekvienai iš jų tinka skirtingos priemonės ir jas reikia taikyti skirtingai. Todėl organizacija turi būti pakankamai subrendusi, kad galėtų taikyti sudėtingus sprendimus ir procesus, nes jei tai darys nepakankamai subrendusi, tuomet iškyla rizika, kad tas įdiegimo procesas bus nesėkmingas. Todėl tyrėjai išskyrė tokias pagrindines požymių grupes, kuriomis remiantis galima nuspręsti, ar organizacija yra subrendusi ar ne:

Nesantis

Visiškas bet kokių atpažįstamų procesų nebuvimas. Organizacija net nėra suvokusi, kad egzistuoja problema, kurią reikia spręsti. Politika (arba procesai) nėra dokumentuoti, ir anksčiau organizacija nebuvo suvokusi veiklos rizikos. Todėl tokia problema organizacijos viduje net nebuvo svarstoma. Tokioje organizacijoje taip pat nevyksta procesų ir veiklos sprendimų rizikos analizė. Organizacija neįvertino su saugos pažeidžiamumu ir plėtros projektų neaiškumu susijusios rizikos poveikio veiklai. Organizacijoje rizikos valdymas nebuvo identifikuotas kaip IT sprendimų įsigijimo ir IT paslaugų tiekimo sudėtinė dalis.[2]

Pradinis

Organizacijoje yra tam tikrų požymių, jog organizacija pripažino, kad problema egzistuoja ir ją reikia spręsti. Šioje stadijoje dažniausiai dar nėra standartizuotų procesų, yra tik „*ad hoc“* (specialūs) sprendimai, taikomi atskiriems asmenims arba atskiriems atvejams. Bendras požiūris į rizikos valdymą yra dezorganizuotas. Matoma, kad kai kurie organizacijos nariai jau suvokė ir pripažino rizikos valdymo vertingumą. Tačiau rizikos valdymas atliekamas „*ad hoc“* principu.[2]

Nėra nei formaliai dokumentuotos politikos, nei procesų, o jei kuriuos nors iš jų ir bandoma įvesti, tai yra įgyvendinami nenuosekliai. Apskritai rizikos valdymo projektai atrodo chaotiški ir nekoordinuojami, o rezultatai nėra nei įvertinami, nei audituojami.

Organizacija suvokia savo teisinius ir sutartinius įsipareigojimus, bet tvarko IT riziką „*ad hoc“* principu, neturėdama apibrėžtos politikos ir procesų. Neformali projekto rizikos analizė atliekama kiekvienam projektui atskirai ir taip, kaip jame nustatyta. Rizikos analizė nėra išskiriama projekto plane ir nėra

pavedama konkretiems projekte dalyvaujantiems vadovams. IT vadovybė nenurodo atsakomybės už rizikos valdymą pareiginiuose nuostatuose ir nedetalizuoja jos kitais būdais. Specifinė su IT susijusi

rizika, tokia kaip saugumas, prieinamumas ir vientisumas, kartais yra analizuojama kiekvieno konkretaus projekto atveju. Su IT susijusi rizika, veikianti kasdienes darbines operacijas, kartais aptariama vadovybės

susirinkimuose, bet rizikos prevencijos priemonės yra nenuoseklios.

Kartotinis

Procesai jau yra išplėtoti iki tokio lygio, kad skirtingi žmonės, atliekantys identiškas užduotis, laikosi panašių procedūrų. Formalūs mokymai ir informavimas apie standartines procedūras nėra organizuojami,

o atsakomybė paliekama kiekvienam asmeniui atskirai. Kartais pernelyg pasitikima atskirų darbuotojų žiniomis, todėl vykdant tam tikrus procesus galimos klaidos. Rizikos valdymas suvokiamas visos organizacijos mastu

Rizikos valdymo procesas yra kartotinis, bet nebrandus. Procesas nėra visiškai dokumentuotas, tačiau veikla vykdoma reguliariai, ir organizacija siekia sukurti visapusį rizikos valdymo procesą, į kurį būtų įtraukta ir jos aukščiausioji vadovybė. Formalūs rizikos valdymo mokymai arba informavimas apie rizikos valdymo procesus nėra vykdomi, atsakomybė už jų įgyvendinimą yra paliekama atskiriems darbuotojams. Organizacijoje didėja supratimas, kad IT rizika yra svarbi ir kad į ją reikia atsižvelgti. Egzistuoja tam tikra rizikos analizė, tačiau procesas tebėra nebrandus – jis vis dar vystymosi stadijoje. Rizikos analizė paprastai atliekama aukščiausiame lygyje ir taikoma tik svarbiausiems projektams.

Vykdomų operacijų analizė paprastai priklauso tik nuo to, ar IT vadovai pasistengia įtraukti šį klausimą į darbotvarkę, o jie tai daro dažniausiai tik iškilus problemai. Bendrai IT vadovybė nėra nustačiusi procedūrų arba pareiginių instrukcijų, formalizuojančių rizikos valdymą.[2]

Apibrėžtas

Procedūros jau yra standartizuojamos ir dokumentuojamos, su jomis darbuotojai yra supažindinti mokymų metu.Tačiau šių procedūrų laikymasis paliktas darbuotojų nuožiūrai, ir atsirandantys nukrypimai nuo normų fiksuojami gana retai. Pačios procedūros nėra išplėtotos, jos tiesiog formalizuoja egzistuojančią praktiką. Organizacija yra priėmusi formalų sprendimą imtis rizikos valdymo visomis jėgomis ir įgyvendinti savo informacijos apsaugos programą. Pamatiniai procesai yra sukurti, jie turi aiškiai nustatytus tikslus, o taip pat apima procedūras, leidžiančias juos pasiekti ir įvertinti procesų sėkmingumą. Yra rengiami tam tikri rudimentiniai rizikos valdymo mokymai rengiami visam personalui.

Pagaliau organizacija aktyviai įgyvendina savo dokumentuotus rizikos valdymo procesus. Rizikos valdymo politika, taikoma visos organizacijos mastu, nustato, kada ir kaip reikia atlikti rizikos analizę. Rizikos analizė vykdoma, laikantis nustatytų procedūrų, kurios yra dokumentuotos ir su kuriomis darbuotojai buvo supažindinti mokymų metu. Sprendimą dėl procedūrinių reikalavimų laikymosi ir dalyvavimo mokymuose priima kiekvienas darbuotojas savo nuožiūra.

Metodologija yra darni ir veiksminga, užtikrinanti, kad pagrindiniai veiklos rizikos tipai bus identifikuoti. Procedūrinių reikalavimų laikymasis paliktas kiekvieno atskiro IT vadovo nuožiūrai, nėra procedūros, užtikrinančios, kad rizikos analizė bus atliekama kiekvieno projekto atveju, ir kad jau vykdomos operacijos bus reguliariai įvertinamos rizikos požymiai.[2. p. 19]

Valdomas

Yra galimybė prižiūrėti ir kontroliuoti procedūrų laikymąsi, o taip pat imtis veiksmų, paaiškėjus, kad procesas nėra pakankamai efektyvus. Procesai nuolat tobulinami, atsižvelgiant į pasiteisinusią praktiką.

Automatizacija ir techniniai instrumentai naudojami ribotai arba fragmentiškai.

Visuose organizacijos lygmenyse egzistuoja išsamus rizikos valdymo supratimas. Rizikos valdymo procedūros yra sukurtos, procesas yra aiškiai apibrėžtas, plačiai skatinamas sąmoningumas, rengiami griežti mokymai, o taip pat egzistuoja kai kurios pradinės priemonės, leidžiančios įvertinti sėkmingumą. Rizikos valdymo programai yra skirti pakankami ištekliai, daugelis organizacijos padalinių yra patyrę jos naudingumą, o Saugumo rizikos valdymo grupė yra pajėgi nuolat tobulinti procesus ir instrumentus.

Rizikos analizė yra standartinė procedūra, ir jos nesilaikymo atvejus gali pastebėti IT vadovybė. IT rizikos valdymas yra suvoktas aukščiausios vadovybės ir yra jiems priklausanti funkcija. Procesas yra išplėtotas, rizika analizuojama tiek atskiro projekto lygyje, tiek reguliariai visos IT sistemos veikimo požiūriu.

Vadovybė informuojama apie IT aplinkos pakeitimus, galinčius iš esmės paveikti rizikos scenarijus, tokius kaip padidintas pavojus iš tinklo pusės, arba techninius sprendimus, darančius įtaką IT strategijos vidinei logikai. Vadovybė yra pajėgi prižiūrėti rizikos situaciją ir priimti pagrįstus sprendimus dėl rizikos lygio priimtinumo.[30 p. 245]

Aukščiausioji vadovybė ir IT vadovybė yra nustačiusi organizacijos toleruojamą rizikos lygį ir turi standartines priemones rizikos ir rezultatų santykiui įvertinti. Vadovybė skiria biudžeto lėšų operacinės rizikos analizės projektams, leidžiantiems reguliariai pervertinti riziką. Šioje stadijoje yra sukurta įmonės rizikos valdymo duomenų bazė.

Optimizuotas

Procesai yra ištobulinti iki geriausios praktikos lygio, remiantis nuolatinio tobulinimo rezultatais ir brandumo modeliavimu kartu su kitomis organizacijomis.

IT yra nuosekliai naudojamos darbui automatizuoti, jos teikia kokybės ir efektyvumo gerinimo instrumentus ir leidžia įmonei greitai prie jų prisitaikyti.

Organizacija saugumo rizikos valdymui skiria pakankamai lėšų, o darbuotojai siekia užtikrinti, kad problemos ir jų sprendimai būtų numatomi prieš kelis mėnesius ir metus. Rizikos valdymo procesas yra gerai perprastas ir stipriai automatizuotas, pasitelkus atitinkamus instrumentus (sukurtus pačios organizacijos arba įsigytus iš nepriklausomų programinės įrangos tiekėjų). Nustatoma kiekvieno saugumo incidento pirminė priežastis ir imamasi tinkamų veiksmų, leidžiančių išvengti jo pasikartojimo. Darbuotojams rengiami įvairaus kvalifikacinio lygio mokymai. Rizikos analizė yra

išplėtota iki tokio lygio, kad visos organizacijos mastu yra įgyvendinamas struktūruotas, reguliariai prižiūrimas ir gerai valdomas procesas. Pasitelkiant specialistus, kolektyvinis rizikos svarstymas ir pirminių priežasčių analizė atliekami visoje organizacijoje. Rizikos valdymo duomenų fiksavimas, analizavimas ir pranešimas yra stipriai automatizuotas. Specialistai yra parengę instrukcijas, o IT organizacija dalyvauja patirties keitimosi grupių darbe. Rizikos valdymas yra realiai integruotas į visą organizacijos veiklą ir IT operacijas, jį pripažįsta ir jame plačiai dalyvauja IT paslaugų vartotojai.[2]

Todėl apibendrinant galima teigti, kad brandumo lygį lemia trys pagrindiniai veiksniai – žmonių kompetencija, organizacija ir naudojamos technologijos. Taip pat nereikėtų pamiršti, kad rizikos valdymo procesai ir rizikos analizės procesai gali pasirodyti identiški.

Tačiau būtina suprasti jų skirtumus ir sąsajas. Rizikos valdymo proceso tikslas yra sumažinti riziką iki priimtino lygio, tuo tarpu rizikos analizė atliekama tam, kad jos rezultatai būtu panaudoti kaip pagrindas

rizikos mažinimo procesams įgyvendinti ir jų veiksmingumui įvertinti. Šie procesai giliau nagrinėjami nebus, nes norint išanalizuoti visus rizikos niuansus būtų galima parašyti atskirą darbą.

Rizikos planavimas procesas

Todėl dažnai organizacijos apsiriboja tik paslaugų tęstinumo planavimu, turi darbuotojus ar jų grupes, atsakingas už nepaprastąsias padėtis, ar remiasi tiesiog siaurais mokymais, susijusiais su tuo, kaip išvengti vienos ar kitos rizikos.

IT rizikos valdymas apima nemažai veiksmų, susijusių su įmonių ar organizacijų rizika, kuri gali pasireikšti eksploatuojant ar diegiant informacines sistemas. Rizikos valdymo tikslas - sumažinti galimą neigiamą įtaką organizacijai, įskaitant ir alternatyvių verslo galimybių praradimą. IT rizikos valdymas taip pat apima ir išankstinius (angl. *proactive*) veiksmus, kurių tikslas - ne tik sumažinti organizacijos nuostolius įvykus vienam ar kitam nenumatytam atvejui, bet ir apskritai neleisti, kad ši rizika pasireikštų.

Išankstiniai, integruoti ir nuolatiniai veiksmai užtikrina geresnius rezultatus.

Rizikos valdymo procesą galima aprašyti šiais pagrindiniais etapais:

1. Nustatymas
2. Rizikos analizė
3. Planavimas
4. Stebėjimas ir ataskaitos
5. Kontrolė
6. Patirties analizė[9]

Kalbant apie rizikas, dar reikėtų paminėti šiuos rizikos mechanizmo elementus: rizikos stebėjimas, rizikos kontrolė, patirties analizė. Procesus ir veiksnius susijusius su rizikomis būtų galima nagrinėti detaliau, tačiau dėl darbo apimties jie analizuojami nebus. Darbe buvo išskirti tie procesai kurie mano nuomone yra svarbiausi ir darantys didžiausią įtaką saugos politikai.

3.3.1 Organizacijos veiklos tęstinumo valdymas

Ši sritis yra labai svarbi organizacijoms netik formuojant savo saugumo politika, bet ir vykdant bet kokią kitą veiklą. Todėl toliau trumpai bus apžvelgiamos pagrindinės šios veiklos sąvokos ir jos teikiami privalumai.

IT paslaugų/veiklos tęstinumo valdymas ***(IT Service Continuity Mangement) -*** procesas, apimantis informacinės sistemos teikiamų paslaugų atkūrimo planus. Šis procesas labai glaudžiai susijęs su analizuotu organizacijos rizikos valdymu. [9]

Į besiplečiančių ir bręstančių ir savo saugumo politikas kuriančių organizacijų sėkmės veiksnių sąrašą jau galime įtraukti ir veiklos tęstinumo rizikos valdymo sistemas. Susiduriama su problema, kad daugelis įmonių turi vienokias ar kitokia veiklos tęstinumo rizikos valdymo sistemas, apsaugos komponentus, įdiegtas apsaugos priemones, bet dažniausiai jos nepakankamai yra suderintos tarpusavyje, dėl ko įmonė anksčiau ar vėliau patiria įvairių problemų. Veiklos tęstinumo rizikos valdymas tiesiogiai veikia organizacijos turtą. Organizacijų veiklos rezultatai labai priklauso nuo turto naudojimo ir valdymo metodų bei įrankių. Pažeidus informacijos ar duomenų, vientisumą, prieinamumą, tapatumą ir patikimumą, bus padryta žala organizacijos veiklai ir jos rezultatams. Tad svarbu apsaugoti turtą ir garantuoti, kad organizacija veiktų esant priimtinam rizikos lygiui. Dėmesys turto apsaugai ypač svarbus dabartiniu metu, nes daugelyje organizacijų yra didelė darbuotojų kaita, daug reikšmingos informacijos yra elektroninėse laikmenose, kurios ir viduje, ir išoriškai yra susietos informacijos technologijų sistemų tinklais.

Veiklos tęstinumo rizikos valdymas - tai procesas, kuriuo siekiama užtikrinti, kad vykstant pokyčiams veiklos tęstinumo riziką identifikuosime, kontroliuosime, sumažinsime ar net pašalinsime.

Veiklos tęstinumo rizikos valdymą sudaro šie elementai:

Veiklos tęstinumo rizikos valdymo sistema

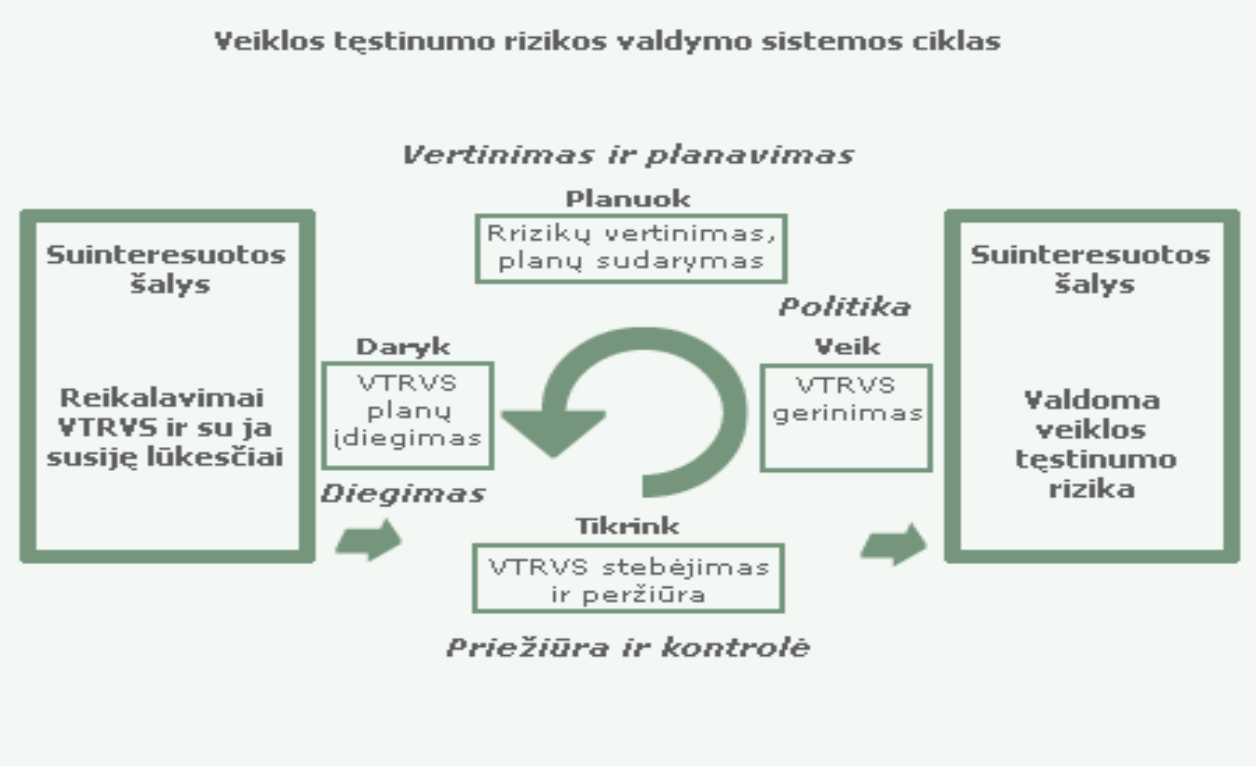
- turtas ir jo reikšmė organizacijai (turtas ir galima žala jo netekus);
- grėsmė (potenciali nepageidaujamų įvykių, galinčių padaryti žalą organizacijai, galimybė);
- pažeidžiamumas (silpnos turto ar turto grupės pusės, kuriomis gali pasinaudoti grėsmė);
- rizika (potenciali galimybė, kad konkreti grėsmė pasinaudos turto ar turto grupės pažeidžiamumu ir sunaikins ar sugadins turtą);

- apsaugos priemonės (praktinės priemonės, procedūros ar mechanizmai, mažinantys riziką).[10]

Veiklos tęstinumo rizikos valdymo sistemos įgyvendinimas apima šias sritis:

- organizacijos saugumo tikslų, strategijos ir politikos nustatymas;
- organizacijos saugumo reikalavimų nustatymas turtui;
- grėsmių turto saugumui organizacijos viduje nustatymas ir analizė;
- rizikos nustatymas ir analizė;
- atitinkamų apsaugos priemonių specializavimas;
- priemonių, efektyviai apsaugančių turtą organizacijos viduje, įdiegimo ir naudojimo priežiūra;
- saugumo įsisąmoninimo programos plėtra ir diegimas;
- incidentų atskleidimas ir reakcija į juos.

Veiklos tęstinumo rizikos valdymo procesai gerai atsispindi toliau pateikiamoje schemoje.



1 schema. Veiklos tęstinumo rizikos valdymo sistemos ciklas [10]

Veiklos tęstinumo rizikos valdymo sistemos įgyvendinimas gali padėti:

- užtikrinti suinteresuotų šalių lūkesčius įgyvendinant strateginius tikslus;
- identifikuoti turtą ir jo reikšmę organizacijoje;
- nustatyti veiklos tęstinumui gresiančias rizikas, organizacijos trūkumus ir jų reikšmingumo laipsnį (įvertinant grėsmes, pažeidžiamumus);

- užsibrėžti norimą ir nustatyti turimą apsaugos priemonių lygį;
- racionaliai panaudoti apsaugos priemonėms skirtus išteklius;
- padidinti darbuotojų saugumą ir pasitenkinimą;
- operatyviai reaguoti į incidentus garantuojant veiklos tęstinumą;

3.4 Organizacijų investicijos IT saugumui

Informacinių sistemų saugumas - bene pati aktualiausia pastarųjų metų tema. Jai skiriamas vis didesnis dėmesys, kuriasi šios srities problemas tyrinėjančios profesionalų organizacijos, forumai, kuriuose saugumo temos yra nagrinėjamos nuo visuotinių teisinių ir organizacinių problemų iki siauriausių ir giliausių techninių aspektų, rašomi straipsniai ir net moksliniai darbai.

Saugumo sprendimai dažniausiai nemažai kainuoja. Tačiau kalbant apie verslą visos investicijos privalo būti nukreiptos į tai, kad padidintų paskutinę eilutę metinėje finansinėje ataskaitoje arba įmonei atneštų kitokią finansinę naudą. Tad kaip įvertinti investicijų į informacinių sistemų saugumą dydį ir teikiamą naudą?

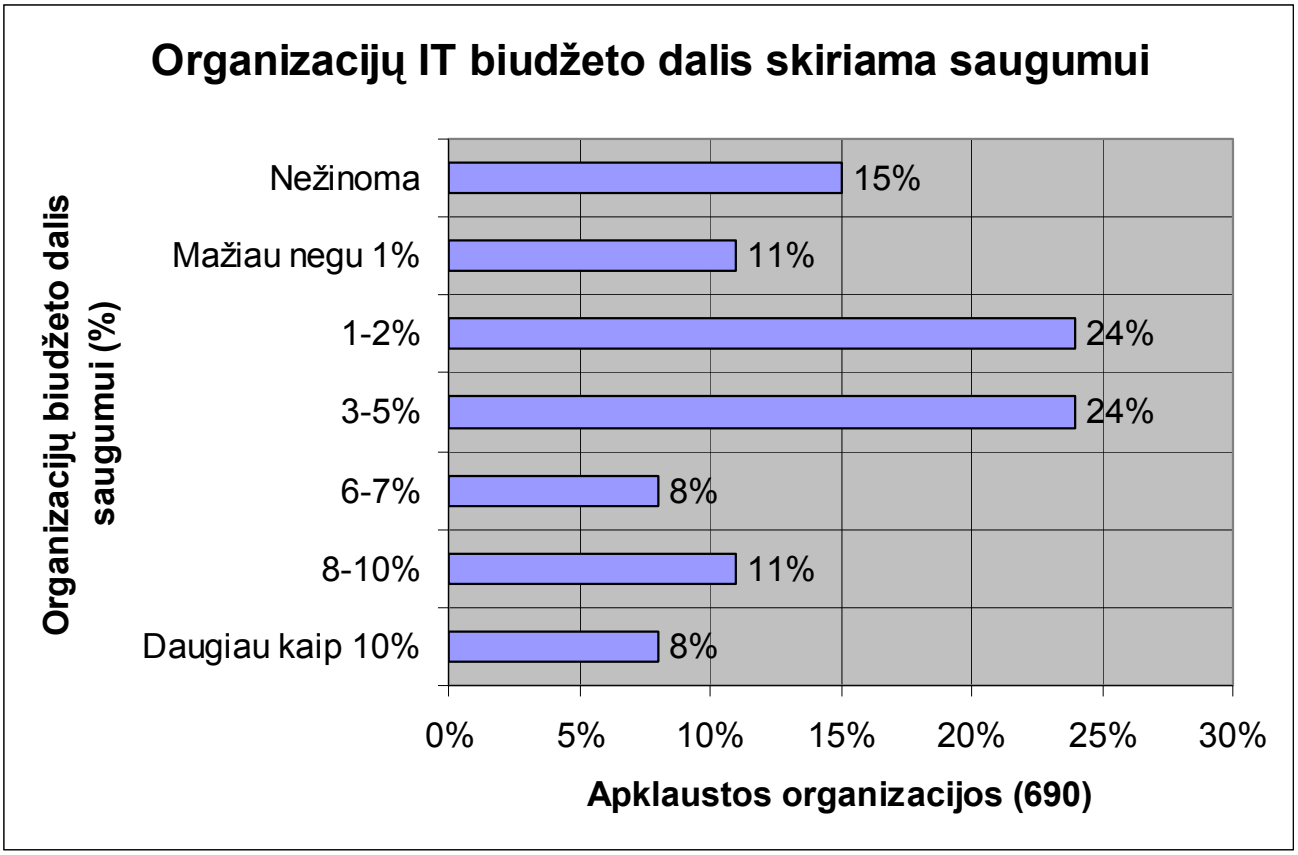
Saugumui skirtuose renginiuose galima išgirsti teiginį, kuris jau tapo aksioma: „Diegiamų saugumo priemonių išlaidos negali viršyti saugomos informacijos vertės". [9]

Apskaičiuoti saugumo diegimo išlaidas nesunku - tereikia žinoti, ko nori, ir išsiųsti klausimą keletui firmų. Kiek sunkiau nustatyti saugomą vertę, ypač jei ta informacija nuolat kinta Deja, į šį klausimą atsakyti sunkiausia. Informacinių sistemų apsauga yra ne būklė, o nuolatinis procesas, reikalaujantis nuolatinės priežiūros ir investicijų. Ir kol neišrasta stebuklinga formulė ir pagal ją neparašyta kompiuterinė programa, tenka pačioms (su IT ir kitų specialistų pagalba) bandyti nustatyti „protingas" išlaidas norimo lygio saugumui užtikrinimui.

Tik nedaugelis įmonių vadovų gali tiksliai pasakyti, kokios saugumo priemonės turėtų įsidiegti jų kompanija. Tačiau jie žino, kiek gali mokėti už vieną ar kitą priemonę, lygindami tai su galimais padariniais įmonei pažeidimo atveju.

Šioje vietoje labai svarbu vadovams rasti bendrą kalbą su IT specialistais: nesileidžiant į technines detales pakanka paprastai nurodyti informacijos konfidencialumo lygmenis, tarnybų darbingumo reikalavimus, paaiškinti vieno ar kito kompiuterizuoto proceso reikšmę organizacijos veiklai. Galutinis variantas - IT specialistai ir organizacijos vadovai turi sutarti dėl priimtinų sumų, kurios reikalingos norint pasiekti reikalaujamą saugumo lygį.

Nepriklausomai nuo informacijos vertės ir jos prieinamumo, visada gali atsirasti norinčiųjų ją pavogti arba sugadinti. Tačiau jei nėra saugumo priemonių organizacijoje, tai nesankcionuoto priėjimo prie informacijos galima netgi nepastebėti. Toliau pateikiama JAV organizacijų 2005 m. išlaidų, skirtų IT saugumui užtikrinti, statistika.



2 Diagrama. Organizacijų skiriamas biudžetas IT saugumui [35]

3.4.1 IT saugumo nauda

Informacinės sistemos yra puiki priemonė, padedanti apsaugoti verslą nuo finansinių netekčių kompiuterinių nusikaltimų ar kitokių nelaimių atvejais. Deja, pinigai, kurie yra investuojami į saugumą, tiesioginio pelno neduoda, šių investicijų pagrindinis rezultatas yra šis, kad užtikrinamas stabilus verslo funkcionavimas ir išvengiama nereikalingų praradimų. Gali kilti klausimas, jei jau turime organizacijos informacijos sistemą, tai kaip iš jos galima paimti duomenis. Šį klausimą galima pailiustruoti tokiu pavyzdžiu, kurį mėgsta cituoti dauguma informacinės saugos specialistų:

„Vienintelė tikrai saugi informacinė sistema būtų tokia, kuri yra įdiegta atskirame kompiuteryje. Šis turi būti išjungtas, visi laidai atjungti (net maitinimo laidas ištrauktas iš lizdo), pats įrenginys saugomas seife su devyniais užraktais ir sudėtinga signalizacijos sistema, o seifas įrengtas bunkeryje, kurį saugo divizija rinktinių, iki dantų ginkluotų kareivių. Bet ir tada nebūtų visiško saugumo". [9]

Todėl matome, jog tokio dalyko kaip šimtaprocentinis saugumas, negali būti. Tačiau naudojantis įvairiomis saugumo priemonėmis pavojų galima sumažinti iki priimtino lygio.

Informacinėse sistemose saugumo priemonių diegimas ne visuomet yra tik grynosios išlaidos. Pastaruoju metu atsirado naujas požiūris į informacinių sistemų saugumą: tam tikrais atvejais įdiegtos

saugumo sistemos verslą leidžia pakelti į naują lygmenį, atveria naujų veiklos perspektyvų: pavyzdžiui, užtikrinus reikiamą saugumą užsienyje ir Lietuvoje pastaraisiais metais labai paplito internetinė bankininkystė, jos saugumui užtikrinti yra naudojama daug įvairių priemonių, tačiau apie jas šiame darbe nebus kalbama. Apibendrinant galima pasakyti, kad informacijos saugos priemonių diegimas:

- gali padėti išvengti nuostolių;
- leidžia diegti naujas technologijas, su kurių pagalba įmonė gali veiksmingiau organizuoti savo veiklą.

Matome, kad dalis organizacijų informacijos saugumui skiria daugiau finansų, kitos mažiau. Tačiau organizacijos turėtų įvertinti savo investicijų tikslingumą, ir atsipirkimą. Todėl kalbant apie IT saugumo naudą negalima praleisti finansinės pusės. Tai svarbus investicijų į organizacijos saugumą aspektas. Organizacija, investuodama į saugumo priemones, tikisi, kad jos duomenys bus geriau apsaugoti, taip pat, kad tos organizacijos investicijos padės pasiekti geresnius rezultatus. Šiandien yra naudojami šie pagrindiniai investicijų į IT vertinimo būdai:

- tradiciniais finansiniais,
- kokybiniais,
- tikimybės. [31 p. 110]

Šie dalykai nebus tyrinėjami, tiktai reikėtų paminėti, kad kuriant informacijos saugumo sistemą reikia stengtis, kad ji neprarastų savo lankstumo, nenaudoti specifinių techninių, programinių priemonių, dėl kurių palaikymo vėliau gali kilti problemų, ir kad pasikeitus technologijoms, ar pasaulinėms tendencijoms, sistemą būtų galima patobulinti ir pritaikyti prie naujų reikalavimų. Taip pat nekurti didelės ir sudėtingos sistemos, kuri vėliau nepasiteisins. Ir gerai įvertinti ar išlaidos tai informacijai yra tikslingos, t.y. ar informacija verta išleistų pinigų. Tai dar kartą parodo saugumo politikos svarbą ir vadovybės rimtą požiūrį į organizacijos duomenų apsaugą, kurios dėka identifikuojami pagrindiniai informaciniai resursai ir taip lengviau apsaugomi pagrindiniai dalykai.

3. 5 IT paslaugų Outsorsingas

Pasak IT rinkos ekspertų, besikeičiantis požiūris į IT paslaugų nuomą rodo augančią informacijos technologijų infrastruktūros, o ypatingai gebėjimų ją valdyti, svarbą siekiant užtikrinti bendrovės efektyvią veiklą. Todėl vis populiaresnė darosi specializuotų IT paslaugų teikimo forma. Ji vadinama „Outsorsingu“.

IT outsourcing - tai informacinių technologijų verslo procesų perkėlimas į išorines organizacijas. Tai IT srities paslaugų teikimas už sutartą mokestį, suteikiant galimybę pačiam klientui pasirinkti

pageidaujamą IT paslaugų paketą. Paslauga apima duomenų saugyklas, gedimų šalinimą, IT turto, tinklo, sistemų valdymą, konsultacijas ir t. t.[24]

Organizacijos saugumo politikos, techninių priemonių pasirinkimas kiekvienai organizacijai gali sukelti nemažai problemų. Nes ne visos turi tokios patirties, ir joms saugumo proceso kūrimas ir užtikrinimas gali pareikalauti daug išlaidų ir laiko, todėl mažesnėms organizacijoms reikėtų pasidomėti, vis labiau populiarėjančiomis „ Outsoursingo“ paslaugomis. Galima paminėti privalumus kuriuos teikia „Outsorsingas“

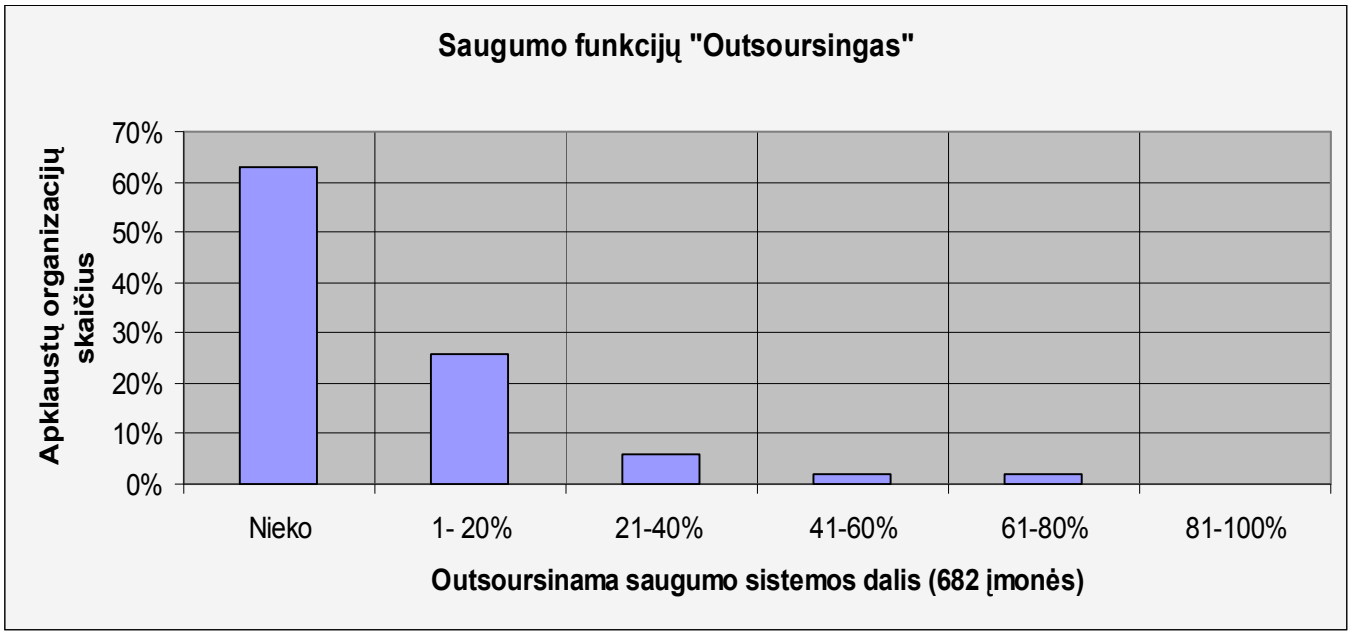
- Išlaidų mažinimas
- Atliekamų darbų kokybė
- Veiklos kontrolė
- Koncentracija ties pagrindine įmonės veikla
- Atsakomybė ir lankstumas
- Pranašumas prieš konkurentus

Tačiau jis turi ir minusų, iš kurių išskiriami trys pagrindiniai :

- Loginis IS saugumas (57%)
- Priklausomybė nuo paslaugų teikėjo (45%)
- Teisiniai padariniai (38%)

Organizacijų vadovybei svarbu įvertinti teisinius faktorius, ir tai koki nuostoliai gali būti patiriami jei paslauga teikianti įmonė pažeis saugumo reikalavimus. Visa tai turi būti aptarta ir išdėstyta pasirašomose sutartyse. Taip pat prieš „outsorsinant“ būtina identifikuoti pagrindinius organizacijos išteklius ir identifikuoti “uotsorsingo“ įtaką verslui. Toliau pateikiama bendra saugumo funkcijų „outsorsingo“ statistika. Toliau pateikiama JAV „IT Outsorsingo“ rinkos 2005 m. statistika.

3 Diagrama. Organizacijų outsorsinama saugumo funkcijų dalis.[35]



Statistika rodo, kad dar pakankamai didelė dalis įmonių nepasitiki kitų paslaugomis ir nori visus procesus valdyti pačios. Lietuvoje ši sritis dar yra ganėtinai nauja, tačiau pastebimas vis didesnis susidomėjimas šiuo rinkos segmentu. Lietuvoje nebuvo atlikta daug tyrimų, kiek įmonių naudojasi šiomis paslaugomis. Todėl darbe bus pateikti didžiausios Lietuvoje viešosios nuomonės ir rinkos tyrimų bendrovės "TNS Gallup" atlikto tyrimo rezultatai. Jie atskleidė, kad vis daugiau įmonių, turinčių kompiuterius, konsultacijoms informacijos technologijų (IT) srityje renkasi joje besispecializuojančią išorės kompaniją. Atlikto tyrimo duomenimis, 2005 metais, palyginti su 2004-aisiais, bendrovių, kurios dėl savo IT ūkio konsultuodavosi su jį prižiūrinčia IT kompanija, skaičius padidėjo - iki 36 procentų. Tyrime buvo apklausti 600 įmonių atstovai.[21]
Prognozuojama, kad IT paslaugų nuomos rinkos augimas turėtų nesulėtinti tempų ir šiais metais.
Kaip pagrindines šio augimo priežastis galima paminėti tai, jog kompanijos vis dažniau konsultuojasi su IT kompanijomis bei apsisprendžia joms perduoti savo IT ūkio aptarnavimą ir valdymą, yra augantis bendrovių pasitikėjimas išorės partneriais. Taip pat didėjant bendrovių verslo plėtros tempams ir siekiant juos išlaikyti, auga ir bendrovių poreikiai jų informacinėms sistemoms, todėl dažnai šiems poreikiams patenkinti vidinio bendrovės IT padalinio nebeužtenka.
Bendradarbiaudamos su išorės partneriais, bendrovės spėjo įžvelgti ir daugelį kitų privalumų. Anot IT konsultantų, nuomodamos paslaugas iš išorės verslo organizacijos ne tik pasitelkia IT srityje besispecializuojančių partnerių kompetenciją, bet jos taip pat turi galimybę gauti ir panaudoti naujausias tos verslo srities žinias bei perimti gerąsias verslo vadybos praktikas – daug greičiau, nei šias žinias pritaikytų, pasikliaudamos tik savo jėgomis.

3.6 Informacijos apsaugos standartai ir metodikos

Šiame skyriuje Bus apžvelgiami tarptautinių standartų organizacijų, vyriausybių(Didžioji Britanija), IT specialistų sukurtos ir siūlomos metodikos, ir standartai. Šios metodikos yra sudėtingos ir didelės, todėl bus pateikti tik patys bendriausi jų ypatumai ir savybės.

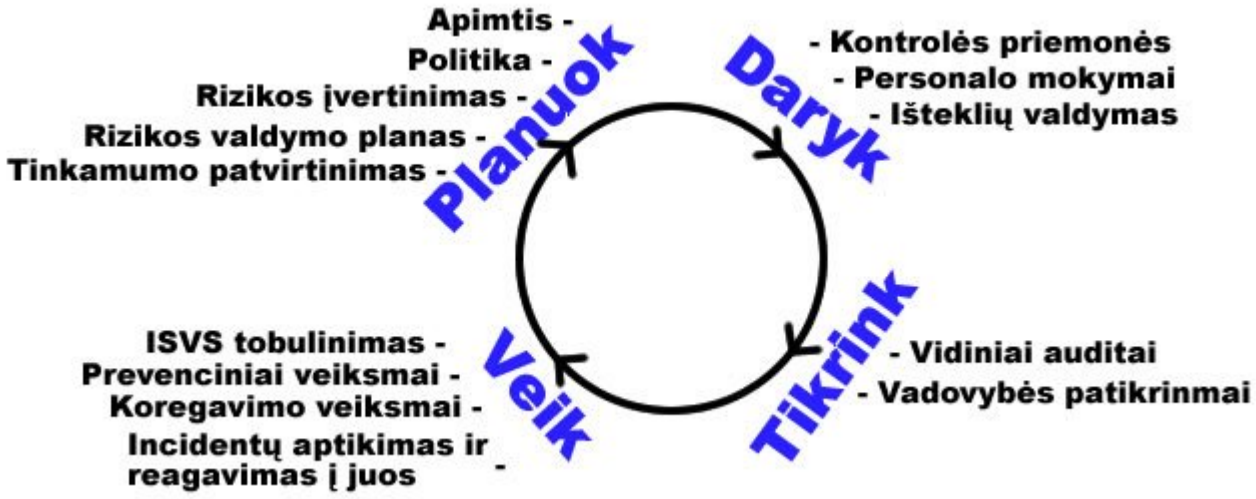
Tarptautinė standartizacijos organizacija (ISO) Didžiosios Britanijos informacijos apsaugos standarto BS7799-1 pagrindu yra parengusi informacijos apsaugos priemonių rinkinį, kurio visas pavadinimas: **ISO/IEC 17799:2005 Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas**. Šis standartas yra patvirtintas Lietuvos standartizacijos departamento ir priimtas kaip Lietuvos standartas **LST ISO/IEC 17799:2005**.
Standartas iš esmės būna dviejų dalių: **ISO/IEC 27001:2005** yra standartiniai nurodymai Informacijos Saugumo Valdymo Sistemoms (ISVS). ISVS yra priemonė, kurios pagalba aukštesnioji administracija

tikrina ir valdo savo saugumą, minimizuodama likutinę verslo riziką ir užtikrindama, kad saugumas ir toliau vykdys korporacijos, kliento ir teisinius reikalavimus. Ji sudaro organizacijos vidinės kontrolės sistemos dalį.

ISO/IEC 17799:2005 yra standartiniai veiklos principai ir gali būti laikomi išsamiu gerų saugumo dalykų, kuriuos verta daryti, žinynu. Reikia paminėti, **kad ISO/IEC 27001:2005** yra naujas standartas, kuris išleistas (2005 metų spalio 14 d.). Jis pakeitė B**S 7799-2:2002.**

ISO/IEC 27001:2005 duoda nurodymus, kaip taikyti **ISO/IEC 17799** ir kaip sukurti, valdyti, išlaikyti ir gerinti ISVS. 1999 m. leidime buvo k pateikiama informacija, tik kaip pritaikyti ISO/IEC 17799 ir kurti ISMS.[16]

Pagrindinius ISVS komponentus galima pavaizduoti toliau pateikiama schema. Darbai nuolat sukasi ratu PLANUOK-DARYK-TIKRINK-VEIK cikle. [18]



2 schema. Pagrindiniai saugumo ciklo veiksniai [18]

Toliau bus trumpai apžvelgti visi pagrindiniai ciklo veiksmai ir juos sudarantys etapai.

PLANUOK

Pirmiausiai reikia nustatyti ISVS apimtį. Ji gali apimti visą organizaciją. Tai taip pat gali būti orientuota į kokią nors konkrečią veiklą ar sritį, tai priklauso nuo organizacijos poreikių.

ISVS Politika

Kaip jau buvo minėta, organizacija turi atsakyti į tokius klausimus:

Kodėl jai svarbi informacijos apsauga? Ar yra konkrečių grėsmių ar kitų rūpesčių, keliančių nerimą organizacijos vadovybei? Ką organizacija nori pasiekti, pavyzdžiui, dėl informacijos konfidencialumo, integralumo ir naudingumo? Kai išsiaiškinama, būtina dokumentuoti atsakymus prieš pateiktus klausimus politikos dokumente. Būtina nepamiršti, kad tas politikos dokumentas apima visą ISVS, ne tik saugumo valdymo priemones. Todėl jis yra daug platesnis nei „informacijos saugumo politika“,

kuri nurodoma organizacijų veiklos principuose. Organizacijos turėtų žinoti, kad tai turėtų būti santykinai trumpas dokumentas (1-3 puslapiai), pasirašytas vadovaujančio darbuotojo. Saugumas, kaip ir visos kitos vidinės kontrolės priemonės atkeliauja iš organizacijos viršaus.

Rizikos įvertinimas

Rizikų vertinimas jau buvo analizuotas ankstesniame darbo skyriuje. Kalbant apie saugumo standartus, organizacijoms reikėtų nepamiršti, kad jei planuojama poveikio kilimo tikimybę lyginti su poveikio reikšmingumu, reikia žinoti, kad yra tokios rizikos, dėl kurios nereikia labai jaudintis, nes:

- net jei ji turėtų didelį poveikį, ji yra ypatingai neįtikėtina,
- arba, jei ji kiltų nuolat, ji turėtų nereikšmingą poveikį.

Kai yra pabaigtas rizikos vertinimas pagal **BS7799-2:1999** standartą, organizacijos vadovybės prašoma nuspręsti, kaip tą riziką valdyti. Naujesnėje ISO versijoje, taip pat ir 2002 metų leidime, kurie yra brandesni standartai, jau yra pateikiama patarimų kaip elgtis su rizika. Organizacijai reikia nuspręsti, ar ji tiesiog priims riziką ir pasikliaus savo sugebėjimais greitai nustatyti bei reaguoti į saugumo incidentus. (Beje, tokia procedūra bus reikalinga organizacijai, kad būtų galima laikytis standarto.) Ar vadovybė vengs rizikos, perkeldama ją trečiajai pusei (pvz., per outsorsingą), ar bus taikomi atitinkami valdymo svertai.

Ne visi išvardinti BS7799-2 elementai tinka visoms organizacijoms, todėl reikėtų atsižvelgti į konkrečias situacijas.

Tinkamumo Patvirtinimas (TP)

Organizacijai reikės nustatyti, kokias saugumo kontrolės priemones pasirinkti, ir pagrįsti, kodėl jas pasirinko, ar jos yra tinkamos, ir kurios BS7799 valdymo priemonės yra nesvarbios. Taip pat reikia susieti valdymo priemones su rizikos įvertinimu.

DARYK

Šioje ciklo dalyje reikalaujama, kad būtų įdiegti reikalingi priežiūros metodai. Tam atlikti bus reikalingos procedūros, galinčios užtikrinti greitą incidentų aptikimą ir reagavimą į juos. Reikia siekti, kad visi darbuotojai suprastų saugumą ir būtų tinkamai apmokyti bei kompetentingi įgyvendinti savo atitinkamas

saugumo užduotis. Norint, kad tai būtų pasiekta, reikia įsitikinti, kad organizacija turės resursų tiems veiksmams atlikti. [18]

TIKRINK

Tikrinimo fazėje stengiamasi užtikrinti, kad kontrolės metodai būtų vietoje ir pasiektų savo tikslus. Yra daug įvairių galimų tikrinimo veiksmų, tačiau tik vidiniai ISVS ir vadovybės patikrinimai priskiriami privalomiems reikalavimams. Kiti žemiau pateikiami veiksmai yra laisvai pasirenkami:

- Įsibrovimo nustatymas
- Incidentų valdymas
- Einamieji patikrinimai
- Savikontrolės procedūros
- Mokymasis iš kitų (pvz., CERT)
- Vidinis ISVS auditas
- Valdymo patikrinimas[18]

VEIK

Veiksmai yra TIKRINK veiklos rezultatas. Yra trys jų rūšys:

- Koregavimo veiksmai;
- Prevenciniai veiksmai;
- Tobulinimas. [18]

Dar būtų galima paminėti, kad **ISO/IEC 17799:2005** nustato 132 saugumo valdymo svertus, sudarytus pagal 11 pagrindinių kategorijų, kad leistų organizacijoms nusistatyti konkrečius saugiklius, kurie tiktų konkrečiam verslui ar konkrečiai atsakomybės sričiai. Į šiuos saugumo valdymo svertus įeina papildomi detalūs valdymo svertai, bendrai labai daug (apie 5000 su viršum geriausios praktikos valdymo) priemonių ir elementų.

Taigi, kaip matome, šis standartas nuolatos tobulinamas, koreguojamas ir papildomas, prie jo sukūrimo ir tobulinimo prisidėjo daug valstybinių ir komercinių organizacijų Didžiojoje Britanijoje ir kitose šalyse. Todėl šio darbo rezultatas yra pats išsamiausias, nuolat atnaujinamas informacijos apsaugos priemonių rinkinys. Atskirai įmonei nėra būtina naudoti visų jame išvardytų informacijos apsaugos priemonių. Tačiau siekiant užtikrinti reikiamą informacijos apsaugos lygį, reikėtų peržiūrėti visas standarte išvardytas apsaugos priemonės ir, jeigu kažkuri iš priemonių nėra naudojama, turi būti žinoma, kodėl ji nenaudojama. Standartas pabrėžia rizikos valdymo svarbą ir aiškiai pasako, kad organizacijai nebūtina įdiegti kiekvienos atskiros rekomendacijos – tik tas, kurios yra jai aktualios.

ISO/IEC 15408 (LST ISO/IEC 15408:2002) standartas pavadinimu „Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“, priimtas 1999 m., susideda iš trijų dalių:

- LST ISO/IEC 15408-1:1999(E) „Įvadas ir bendras modelis“,
- LST ISO/IEC 15408-2:1999(E) „Saugumo funkciniai reikalavimai“,

- LST ISO/IEC 15408-3:1999(E) „Saugumo užtikrinimo reikalavimai“.

Standartas skirtas įvairios paskirties IT sistemų bei IT produktų saugumo įvertinimui ir nustato bendruosius kriterijus (angl. Common Criteria), nepriklausančius nuo konkrečių IT objektų, kurių dėka, priklausomai nuo grėsmių ir saugumo reikalavimų, pagal bendruosius reikalavimus sudaromi apsaugos profiliai (angl. Protection Profile). Standarte taip pat suformuluoti septyni įvertinimo patikimumo lygiai (angl. Evaluation Assurance Level), kurie nustato patikimumo matavimo skalę, individualius patikimumo komponentus, iš kurių sudaryti patikimumo lygiai, ir apsaugos profilių įvertinimo kriterijus. Šis standartas gali būti naudojamas tiek IT produktų gamintojų, tiek vartotojų, tiek auditorių, kontroliuojančių IT saugumą..[16]

ISO/IEC 27001 (BS7799-2) Informacijos technologija. Saugumo metodai. Informacijos apsaugos valdymo sistema.

Gali būti sėkmingai naudojamas kartu su ISO 17799 standartu. Metodika paremta procesiniu požiūriu į rizikų valdymą.

ISO/IEC 13335 Informacijos technologija. Informacijos technologijų saugumo valdymo gairės.

Tai daugiau techninis informacinių technologijų (IT) apsaugos standartas, sudarytas iš penkių dalių:

1. IT saugumo sąvokos ir modeliai;
2. IT saugumo valdymas ir planavimas;
3. IT saugumo valdymo metodai;
4. Apsaugos priemonių parinkimas ;
5. Tinklo saugumo valdymo patarimai[16].

Tarptautinius ISO standartus ar jų lietuviškas versijas galima įsigyti Lietuvos standartizacijos departamente.

ITIL – Information Technology Infrastructure Library

Pagrindinis ITIL standarto ir metodikos tikslas – IT paslaugų valdymo įgyvendinimas. Tai geriausių pavydžių, naudojamų siekiant šio tikslo, rinkinys. ITIL gali padėti įmonei pasiekti informacijos apsaugos

politikoje numatytų tikslų ir gali būti naudojamas kartu su **ISO 27001/27002** standartais.

Šiuolaikinė ITIL - tai populiariausia pasaulyje IT įmonių bei įmonių IT padalinių valdymo metodologija, kombinuojanti paprastumą su gana išsamiais verslo įsipareigojimais bei IT veiklos

optimizacija.[14] Remiantis tyrimais, visa IT veikla gali būti suskirstyta į tris dalis, kurių svarba dažniausiai pasiskirsto taip:

* Technologijos (technika, programos ir pan.) – 20%
* Darbuotojai (kvalifikacija, atsakingumas ir pan.) – 40%
* Procesai (procedūros, instrukcijos, įvykių registravimas ir t.t.) – 40%

Pastebima, kad dauguma IT kompanijų bei įmonių IT padalinių didžiausią dėmesį kreipia į technologijas (įrangos, programų ir t.t. atnaujinimą), kiek mažesnį dėmesį - į darbuotojus (jų atranką, kvalifikacijos kėlimą), todėl dažniausiai procesai lieka menkai formalizuotais ir nesutvarkytais. Taigi, daugumai bent kiek stambesnių IT įmonių bei IT padalinių (10–15 žmonių ar daugiau) lieka labai didelės galimybės pagerinti veiklą, tiesiog sutvarkant IT procesus, kitaip tariant – įdiegiant ITIL.

ITIL yra paremta keliomis teorinio apibendrinimo idėjomis: visų pirma siekiant tiksliai aprašyti galimus procesus, ITIL sukuria specifinę terminiją, skirtą procesų aprašymui: daug ITIL naudojamų sąvokų ne visiškai tiksliai atitinka įprastas atitinkamų žodžių prasmes, pvz., Incidentas ITIL terminologijoje reiškia bet kokį paslaugos sutrikimą, nepriklausomai nuo jo kilmės, o Problema – ne vartotojo patiriamą
paslaugos sutrikimą, o tik Incidento priežastį. Tokia terminija garantuoja tikslų ir vienareikšmį įmonėje vykstančių procesų aprašymą, tačiau truputį apsunkina pačios ITIL teorijos greitą įsisavinimą. Pritaikant ITIL teoriją įvairioms kalboms, pirmiausiai būna išverčiamas ITIL terminų žodynas. Šiuo metu Lietuviško ITIL terminų žodyno nėra. [8]

ITIL gana abstraktus standartas, jis nekonkretizuoja procesų, ar kokios priemonės turėtų būti naudojamos. Nepaisant to, ITIL stengiasi supažindinti su labiausiai vykusiais IT valdymo metodologijų pavyzdžiais.
ITIL modulių skaičius, einant laikui, keičiasi. Tradiciniai ITIL moduliai yra 6:

- service support (paslaugų parama)
- service delivery (paslaugų perteikimas)
- planning to Implement Service Management (Planavimas įgyvendinti paslaugų valdymą)
- ICT Infrastructure Management (ICT infrastruktūros valdymas)
- applications Management (Panaudojimo valdymas)
- The Business Perspective (Verslo perspektyvos)

Taip pat yra ir du naujesni moduliai:

- security Management (Saugumo valdymas)
- software Asset Management (Programinės įrangos resursų valdymas)

Šiuo metu yra kuriamas naujas, patobulintas ITIL leidimas, kuriame specialistų skiriami tokie 5 moduliai:

- service Strategies (Paslaugų strategija)
- service Design (Paslaugų projektavimas)
- service Introduction (Paslaugų pristatymas)
- service Operation (Paslaugų veikimas/funkcionavimas)
- sontinuous Service Improvement (Besitęsiantis paslaugų/eksploatacijos tobulinimas)[13]

Dabartiniame ITIL svarbiausi yra du moduliai, kuriuos įdiegus įmonėje, galima tarti, kad ši yra "ITIL-zuota":

Service support – su paslaugų aptarnavimu susiję procesai

- *service desk - klientų aptarnavimas*
- *incident management - incidentų (paslaugos sutrikimų) taisymas*
- *problem management - ilgalaikių problemų (incidentų priežasčių) taisymas*
- *configuration management - dokumentacijos palaikymas*
- *change management - bendras procesų valdymas ir dokumentacijos teisingumo palaikymas*
- *rRelease management - naujų paslaugų įvedimo ar esamų paslaugų pakeitimo valdymas*[13]

Service delivery - su paslaugų sukūrimu ir pateikimu susiję procesai

- *availability management - paslaugos pateikiamumo įvertinimas*
- *capacity management - resursų valdymas*
- *fnancial management - finansų valdymas*
- *srvice level management - įsipareigojimų vykdymo priežiūra*
- *IT Service continuity management - katastrofinių situacijų valdymas*
- *IT Security management - duomenų saugumo ir konfidencialumo valdymas*

Nors daugelis dalykų ITIL teorijoje atitinka CobIT sampratą, ITIL yra daugiau orientuota į kokybės gerinimą, o ne į taupų lėšų panaudojimą, todėl labiau tinka valstybinėms įstaigoms, įmonėms, kurioms IT veikla yra kritiškai svarbi bei IT firmoms, besiorientuojančioms į viršutinį rinkos sektorių. Kita

vertus, skirtingai nei CobIT, ITIL nekelia ypatingų reikalavimų, susijusių su auditais ir pan., todėl diegiama žymiai lengviau. [14]

COBIT – Control Objectives for Information and related Technology

Tai audito kompanijų parengta metodika, kuri turi padėti vartotojams, įmonėms ir auditoriams planuoti, įgyvendinti ir audituoti IT valdymo priemones. Kaip ir ITIL, COBIT gali padėti įmonei sustiprinti informacijos apsaugą. Sėkmingai veikiančios organizacijos suvokia, kad IT padeda joms kurti pridėtinę vertę. Todėl vystantis informacinėms technologijomis, organizacijos sėkmės faktorius vis labiau priklauso nuo sėkmingo jų pritaikymo. Bendradarbiaujant IT specialistams buvo sukurta **COBIT** metodika. [4;11].

COBIT metodika yra tiek valdymo, tiek pagalbinė priemonė, kuri daugiausia yra skirta organizacijos darbuotojams dirbantiems su informacijos apsauga. Jos dėka galima lengviau užpildyti tarpus organizacijoje tarp kontrolės reikalavimų, techninių problemų ir egzistuojančių pavojų verslui. **COBIT** yra naudingas organizacijoms, kurios kuria ar vysto jau esančią saugumo politiką, taip pat padeda geriau pritaikyti „gerus“ praktinius IT kontrolės organizacijose pavyzdžius. Organizacijos, naudojančios šią metodiką, padeda padidinti vertę, gaunamą iš IT. Specialistai **COBIT** standartą rekomenduoja organizacijoms, kuriose IT kaitos iniciatyvos yra planuojamos ir valdomos, taip pat yra numatyta organizacijos informacinės sistemos strategija. Jo dėka galima daug paprasčiau ir praktiškiau užtikrinti IT srities tobulinimą ir valdymą. [36]

SE-CMM – Systems Security Engineering Capability Maturity Model

SSE-CMM yra organizacijos brandos lygio matavimo modeliai. Šie modeliai yra sukurti matuoti ir tobulinti organizacijos saugumo projektavimo sugebėjimus. SSE-CMM metodikos tikslas yra sukurti tokį pasitikėjimo laipsnį, kuris atitiktų organizacijos klientų poreikius. Organizacijoje metodika jungia tokius elementus:

- organizacijai lengviau vertinti ir gerinti procesus, kurių metu organizacija transformuoja klientų įsivaizduojamas saugumo vizijas į realias paslaugas ir produktus, kuriuos jie norėtų įsigyti.
- organizacija savo klientams galės pasiūlyti sertifikuotas ir patikimas paslaugas klientams.
- įmonei bus lengviau vykdyti savo veiklą rinkoje, nes klientai rinksis jos paslaugas ir produktus žinodami, kad jie atitinka jų poreikius.[41]

Organizacijos naudojančios SSE-CMM turėtų sugebėti gerai identifikuoti, įgyvendinti ir perduoti klientų poreikius susijusius su informacijos sauga. Taip suteikti klientams galimybes išbandyti jų siūlomos produktus.

NIST 800 serija

Tai JAV Nacionalinio standartizacijos ir technologijos instituto parengtas informacijos apsaugos metodikų ir priemonių rinkinys. Visa medžiaga pateikiama nemokamai. Šioje metodikoje didžiausias dėmesys yra skiriamas šiems elementams. [40]

Kriptografiniai standartai ir jų naudojimas

Organizacijoms teikiami patarimai ir rekomendacijos, kaip kriptografinių metodų dėka apsaugoti informacijos integralumą, konfidencialumą ir informacijos resursų autentiškumą. Taip pat skiriamas dėmesys: techninei sričiai, PKI, sudėtingoms autentifikavimo sistemoms, kriptografinei kontrolei ir interfeisams, TOKEN raktams, ir kt. Standartai padeda plačiau naudoti kriptografines paslaugas privačioje

ir valstybinėje sferoje.

Saugumo standartai

Šiose metodikos daugiausia skirtos vyriausybei ir didelėms pramoninėms organizacijoms. Jomis remiantis patogiau kurti saugesnes sistemas, geriau valdyti, vystyti ir kurti saugumo vertinimo įrankius. Taip pat galima kurti metodologijas, testavimo metodikas ir kt.

Saugumo tyrimai / saugumo technologijos

Ši metodikos dalis padeda organizacijai geriau suvokti ir pagerinti saugumo situaciją įmonės viduje. Taip pat skleisti supratimą, kad technologijos padeda geriau identifikuoti ir sušvelninti įvairius pažeidžiamumus. Pateikiama pavyzdžių, kaip vykdyti įsilaužimų kontrolę, kokias ugniasienes pasirinkti,
kaip valdyti priėjimo prie informacijos kontrolę ir kt.

Saugumo valdymas ir konsultacijos

Šioje srityje daugiausia dėmesio saugumo valdymo nurodymai nukreipti į tokias sritis: rizikos valdymas, saugumo programos valdymas, apmokymai ir supratimas, nenumatytų situacijų valdymas, personalo saugumas, administracinės priemonės, saugumo įgijimas ir palengvinimas.

ISF – The Information Security Forum Standard of Good Practice

ISF – tai Informacijos saugumo forumo, kurį sudaro daugiau nei 200 didžiausių pasaulio kompanijų parengtas informacijos apsaugos priemonių rinkinys. Jo pripažinimas ir populiarumas yra mažesnis negu **ISO 17799** standarto, tačiau šis rinkinys yra platinamas nemokamai.

Minėras rinkinys yra skirtas padėti organizacijoms, nepriklausomiems rinkos sektoriams vertinti pavojus, susijusius su informacinėmis sistemomis. Tai yra efektyvus įrankis, padedantis gerinti saugumo kontrolės efektyvumą ir patogesnį pritaikymą organizacijai. [39]

ISF standarte yra sukaupta 16 metų didelėmis investicijomis paremta medžiaga, kurioje pateikiama daug praktinių duomenų ir informacijos saugumo forumo specialistų patarimų. Jame informacijos saugumo suvokimas, pateikiamas iš verslo perspektyvų. Tai naudinga vadovams, nes teikia praktinių patarimų, kurie yra sufokusuoti į informacijos saugumą ir geras praktikas. Saugumo forumas remia gerų praktikų skleidimą visoms pasaulio organizacijoms. Taip pat padeda organizacijoms, kurios nėra ISF narės. Jis padeda testuoti informacijos saugumą viso pasaulio mastu ir yra atnaujinamas kas du metai.

CRAMM (CCTA Risk Analysis and Management Methodology) – tai D. Britanijos Vyriausybės užsakymu sukurta ir visame pasaulyje taikoma informacijos apsaugos rizikų analizės ir valdymo metodika. CRAMM metodika yra nuolat tobulinama jau beveik 20 metų ir yra nepakeičiama priemonė saugumo vadovams ir analitikams.

CRAMM – tai laipsniškas ir metodiškas būdas analizuoti ir valdyti tiek techninius (pavyzdžiui, IT techninę ir programinę įrangą), tiek netechninius (pavyzdžiui, fizinius ir žmogiškuosius) informacijos apsaugos aspektus.

Norint juos įvertinti, CRAMM metodikoje naudojami trys etapai:

1. Vertybių identifikacija ir įvertinimas;

CRAMM leidžia identifikuoti fizines (pavyzdžiui, techninė įranga), programines (pavyzdžiui, taikomoji programinė įranga), duomenų (pavyzdžiui, informacija, esanti informacinėse sistemose) vertybes bei vietas, kuriose yra informacinės sistemos.

Fizinės vertybės yra vertinamos pagal jų pakeitimo kaštus. Duomenų ir programinės vertybės yra vertinamos pagal tai, kokį poveikį sukels organizacijos veiklai, jeigu informacija bus neprieinama, sunaikinta, nesankcionuotai atskleista ar pakeista. [5]

2. Grėsmių ir pažeidžiamumų įvertinimas;

Žinant saugumo incidentų poveikį ir problemas, kurias jie gali sukelti, kitas žingsnis yra nustatyti, kiek tikėtina, kad problemos iškils. CRAMM apima pilną tyčinių ir atsitiktinių grėsmių, galinčių paveikti informacines sistemas, spektrą, įskaitant:

- Įsilaužimus;
- Virusus;
- Techninės ir programinės įrangos veikimo sutrikimus;
- Tyčinę žalą arba terorizmą;
- Žmonių klaidas ir t.t. [5]

3. Kontrolės priemonių parinkimas ir rekomendacijos.

CRAMM metodikoje yra sukaupta labai didelė kontrolės priemonių biblioteka, kurią sudaro virš 3000 kontrolės priemonių, suskirstytų į 70 loginių grupių. CRAMM programiniai įrankiai lygina praeitame žingsnyje gautus rizikos lygius su kontrolės priemonių apsaugos lygiais (kurie užtikrina tam tikrą apsaugos lygį), siekiant nustatyti, ar rizika yra pakankamai didelė, kad būtų pateisintas tam tikros kontrolės priemonės diegimas.

CRAMM taip pat turi gana daug pagalbos priemonių, kaip antai, grįžtis (angl. Backtracking), „Kas, jeigu“ (angl. What if?), prioretizavimo, ataskaitų kūrimo ir kitas priemones, skirtas palengvinti kontrolės priemonių įgyvendinimui bei efektyviam identifikuotų rizikų valdymui.

Lietuvoje informacijos apsaugos rizikos analizės ir valdymo metodiką CRAMM turi įsigiję šie klientai:

- AB „Lietuvos energija“
- AB „Lietuvos geležinkeliai“
- Lietuvos Respublikos finansų ministerija
- Lietuvos Respublikos vidaus reikalų ministerija. [5]

3.7 Kodėl saugumo politikos tampa neveiksniomis?

Kaip jau buvo minėta darbe, nėra šimtaprocentinės apsaugos, ją tik galima sumažinti iki priimtino lygio. Organizacijos naudoja įvairaus sudėtingumo saugumo politikas, tačiau kartais saugomo politika nebeatitinka reikiamų normų ir tampa neveiksni. Toliau bus analizuojamos situacijos, pateikiama pavyzdžių kodėl taip nutinka.

Pirmiausiai bus apžvelgiami veiksniai, kuriuos (**Globat networked IT services**) kompanijos specialistai įvardija „Natūraliais silpnumais“ (angl. Natural weaknesses). Pradėjus formuoti saugumo politiką, šie veiksniai gali atrodyti nereikšmingi, tačiau vėliau saugumo politikai tampant sudėtingesnei, jai valdyti reikia vis daugiau lėšų ir pastangų, ir tam tikru momentu dėl per didelio savo sudėtingumo, ar natūralių veiksnių tampa neveiksnia. [42]

Saugumas – barjeras organizacijos pažangai

Apsaugos priemonės, ir kiti su sauga susiję veiksniai visada apsunkina verslo procesų vykdymą. Organizacijos naudojami saugumo sprendimai, tam tikru laipsniu sumažina informacijos apsikeitimo tarp darbuotojų greitį. Todėl darbuotojai tas priemones dažniausiai vertina kaip kliūtis ir mano, kad jos neteikia jokios praktinės naudos. Nes įmonės personalas nori, kad procesai vyktų greitai ir jie gautų jiems reikalingą informaciją. Viena iš politikos neveiksnumo priežasčių yra tai, kad vadovai norėdami pasiekti geresnių rezultatų, renkasi sudėtingus technologinius sprendimus neatsižvelgdami į darbuotojų nuomones. Dėl to kartais darbuotojai būna nepasiruošę pasikeitimams. Todėl būtina įvertinti saugumo poveikį klientams ir verslo procesams, ir suvokti kad ir nesudėtingos priemonės sumažins veiklos produktyvumą. [42]

Saugumas - tai elgesys kurio išmokstama

Kiekvienas žmogus pasižymi savisaugos jausmu, o tai yra instinktyvus elgesys. O saugumo vertinimas, priskiriamas aukštesniam lygmeniui, kurio individai išmoksta. Darbuotojai neturintys specifinių žinių ir patirties ne visada gali pilnai įvertinti riziką ir atpažinti potencialius pavojus saugumui. Taigi neveiksnumą sukelia strategijoje nenumatytas, arba numatytas, tačiau ne iki galo įgyvendintas darbuotojų mokymas ir netinkamas pagrindinių resursų identifikavimas. Taip pat dažna politikos funkcionalumo sutrikimo priežastis yra ta, kad, organizacijos darbuotojai neįvertina ar nežino savo sukauptos informacijos vertės.

Kasdien laukti netikėtumų

Organizacijose vyksta daug ir įvairių procesų, su kuriais yra susiję daug vartotojų keliose organizacijose. Taigi kuo organizacija didesnė, tuo didesnė galimybė, kad gali įvykti, kažkas nenumatyta, kas gali įtakoti veiklos vientisumo sutrikdymą. Apie vientisumo užtikrinimą buvo kalbėta analizuojant rizikų sudėtinius elementus. Galima tik pasakyti, kad geri saugumo darbuotojai, turi kasdien tikėtis įvairių netikėtumų ir pavojų, taip pat nuolat prižiūrėti, saugiklius padėsiančius greičiau identifikuoti pavojus.[42]

Tobulų sistemų nėra

Kaip jau buvo minėta darbe, Informacinių sistemų apsauga yra ne būklė, o nuolatinis procesas. Nuolat keičiasi rinkoje siūlomos technologijos, organizacijos saugumo sistema sensta, mažėja sistemos efektingumas ir kt. Organizacijoje nevykstant jokiems saugumo incidentams, saugumo pareigūnai ir darbuotojai pradeda manyti, kad jų turima sistema tobula ir jai niekas negresia. Ir kuomet įvyksta nenumatyta krizinių situacijų politika tampa neefektyvi. Galima prisiminti saugumo pareigūnų mėgstamą teiginį „Negalima tikėtis, jog saugumo sistema yra tobula ir ramiai eiti namo. Saugumas tai darbas vykstantis 24h, jis niekada nesibaigia“.

Taigi organizacijoms rekomenduojama nepamiršti „natūraliųjų silpnumų“ ir tik tuomet stengtis įsigyti daug investicijų reikalaujančias apsaugos priemones. Dažnai organizacijos patiria nuostolius dėl darbuotojų nepatyrimo, arba tikslingo sabotažo. Galima paminėti tokius dažniausiai pasitaikančius saugumo pažeidimus: atsisakymas aptarnauti (angl. denial of service), įvairūs informacijos konfidencialumo, prieinamumo ir vientisumo pažeidimai. Nusikaltėliai norėdami gauti konfidencialius duomenis naudojasi vis tobulesnėmis technologijomis ir metodais. Toliau pateikiamas pavyzdys kuriame pavaizduojama kaip organizacijos saugumo politika tapo neveiksnia.

„ Tinklo administratorius dirbantis didelėje kompanijoje, nusprendė, kad jo prižiūrimoje organizacijoje yra pernelyg daug neaktyvių elektroninio pašto prieigų (angl. acount). Todėl jis kreipėsi į vadovybę prašydamas, kad ji patvirtintų elektroninio pašto politika, pagal kurią nauja pašto prieiga būtų kuriama tik gavus vadovybės leidimą (ją sudarė trys valdybos nariai). Taigi naujos prieigos buvo kuriamos gana dažnai, tačiau užtrukdavo kol pasirašydavo visi trys vadovai. Jie pasirašydavo net nežinodami, kad tie darbuotojai kuriem reikalingas elektroninis paštas. Vadovai norėdami, kad tas procesas būtų greitesnis, pasirašydavo dokumentus, kurie yra reikalingi, ir juo perduodavo darbuotojams atsakingiems už tą sritį.

Tačiau vieną dieną, buvo neteisėta prieita prie slaptos organizacijos informacijos. Ji buvo paskelbta Internete anoniminio vartotojo. Dėl to kompanija patyrė nuostolius, nes tie paviešinti duomenys neigiamai paveikė jos vardą ir kt.

Po šio įvyki organizacijoje buvo atliktas „logų“ ir prieigų auditas, kurio metu buvo nustatyta, kad *“JQPUBLIC“* priėjo prie duomenų kurie vėliau buvo paskelbti. Tolimesnis tyrimas parodė, kad ši prieiga buvo patvirtinta prieš kelis mėnesius, tačiau niekas nežinojo kas tas darbuotojas ir kas kreipėsi dėl jo prieigos. Iš šio pavyzdžio galima daryti išvadą, kad nebūtina padaryti didelį poveikį saugumo sistemai, kartais užtenka nedidelės spragos k Taigi kyla klausimas kokios buvo priežastys dėl kurių organizacijos saugumo politika, neatliko savo funkcijos. Matome, kad įmonė formuodama savo politiką neįvertino to kad leidimų išdavimas, bus papildomas procesas organizacijos verslo cikle. Ir vadovai tvirtinantys leidimus, neturėjo laiko tikrinti kiekvieną vartotoją. Taigi saugumo darbuotojų pasirinktas vartotojų identifikavimo ir paskyrimo metodas buvo netikslus. Buvo vykdoma netinkama komunikacija su valdybos nariais. Todėl būtina įvertinti naujai norimas panaudoti priemones, galimą riziką ir tik tuomet jas teikti tvirtinti vadovybei.

3.8 Diegiamos saugumo sistemos ir pasirinktų priemonių įvertinimas

Kai organizacija jau yra suformavusi savo saugumo politiką, parengusi saugumo dokumentaciją, įvertinusi rizikas, užtikrinus veiklos tęstinumą. Gali pradėti vykdyti esamos būklės patikrinimą, išsiaiškinti kokia būklė yra pasiekta, taip pat ko jai trūksta iki saugumo politikos dokumente pateiktų reikalavimų. Kaip ir Saugumo politikos dokumentai, šie patikrinimai gali būti tiek labai išsamūs, tiek labai paviršutiniški arba specifiniai, orientuoti į specifinius saugumo aspektus. Todėl yra skiriamos tokios pagrindinės saugumo patikrinimo grupės:

- techninis saugumo patikrinimas
- formalus procedūrinis auditas
- saugumo ekspertizė (neprocedūrinis auditas).[9]

3.8.1 Techninis saugumo patikrinimas

Šio tipo saugumo patikrinimai orientuoti į konkrečių (dažniausiai jau veikiančių) saugumo sistemų techninį patikrinimą ir neturi nieko bendra su saugumo politika. Tokių paslaugų pavyzdžiai:

- etiškas įsilaužimas;
- ugniasienės (angl.*Firewall*) konfigūracijos tikrinimas;
- pažeidžiamumo įvertinimas, tarnybinių stočių saugumo tikrinimas;
- tinklo skenavimas ieškant silpnų vietų ir pan. [9]

Visi šie patikrinimai yra veiksmingi ir gali padėti įsitikinti, kaip veikia (arba neveikia) vienas arba kitas saugumo elementas.

Naudingas yra etiškas įsilaužimas, jei jo būdu pavyksta įsilaužti į sistemą, matoma, jog ji nesaugi, ir ją reikia tobulinti. Jei įsilaužti nepavyksta, reiškia saugumui skiriamas pakankamas dėmesys. Taip lengvai galima nusakyti esamą saugumo būklę. Todėl šis būdas padeda nustatyti, netgi, atrodo, gerai

veikiančios sistemos spragas. Rekomenduojama nuolat atlikinėti tinklo pažeidimo prevenciją (skenavimą). Ši ganėtinai nebrangi paslauga leistų pastebėti visas skyles, esančias sistemoje, ir jas pašalinti dar neiškilus problemoms.

3.8.2 Formalus procedūrinis auditas

Tai formalus įvertinimas, kuris atliekamas pagal tam tikras metodologijas kompetentingų specialistų. Metodologija – tarsi formalus rinkinys principų, į kuriuos reikia atsižvelgti atliekant auditą. Labai svarbus procedūrinio audito aspektas – patikrinimas, ar veiksmingai veikia įdiegtos saugumo priemonės. Šiame etape techninių patikrinimo testų atlikinėti nebūtina.

Techninės paslaugos metu atliekami testai, bandoma įsilaužti, tikrinamos sistemos konfigūracijos. Procedūrinio audito metu tikrinama, kaip veikia ugniasienė, kaip reaguojama į pranešimus apie saugumo pažeidimus, ar atliekamos nuolatinio atnaujinimo, darbingumo užtikrinimo procedūros ir pan.

Iš tokių saugumo metodologijų šiandien pagrindiniu yra laikomas ISO 17799 standartas, prieš tai buvo naudojamas anglų sukurtas BS 7799 standartas.[16] Tačiau bus įvardijami 10 elementų kuriuos su šiuo standartu dirbantys specialistai rekomenduoja įsidiegti:

1. Turėti Saugumo politikos dokumentą.
2. Nustatyti atsakingus asmenis.
3. Informuoti ir mokyti naudotojus.
4. Reaguoti į saugumo incidentus.
5. Kontroliuoti virusus.
6. Turėti veiklos tęstinumo planą.
7. Kontroliuoti informacijos srautus.
8. Apsaugoti duomenis nuo praradimo.
9. Užtikrinti įstatymų vykdymą.
10. Turėti priemones, padedančias įrodyti atitikimą saugumo politikai. [9]

Procedūriniai auditai atliekami formaliai, užpildant visus reikiamus dokumentus, numatytus metodologijoje. Procedūrinis auditas sąlygiškai yra ilgas ir brangus procesas, galintis kainuoti net šimtus tūkstančių litų. Paprastai juos atlieka tik didelės organizacijos. Lietuvoje paskutiniu metu tokių auditų nebuvo atliekama daug. Keletas iš jų buvo atlikti užsienio organizacijų. Šiuo metu jaučiamas šias paslaugas teikiančių organizacijų poreikis, Lietuvoje yra tai galinčių atlikti specialistų (**Informacinių technologijų audito grupė, ISACA**).

3.8.3 Saugumo ekspertizė

Saugumo ekspertizė (įvertinimas) yra tarpinis variantas tarp techninių saugumo patikrinimų ir procedūrinio audito. Jo metu vertintojas gali naudotis tam tikrais procedūrinio audito elementais, taip pat patikrinti kai kurių arba visų tinklo mazgų atsparumą pažeidimams. Toks patikrinimas nėra toks išsamus kaip procedūriniais saugumo auditais, tačiau ir jis gali būti pakankamai veiksmingas siekiant patikrinti, kiek reali situacija atitinka aprašytąją Saugumo politikos dokumente, padėti parengti saugumo priemonių diegimo planą.

Paprasčiausias variantas tai padaryti, palyginti kiek reali situacija atitinka aprašytąją saugumo politikos dokumente. Tačiau tokiu atveju reikėtų nepamiršti patikrinti ir kitų svarbių saugumo elementų, kurie galbūt nepaminėti dokumente, šioje vietoje dažnai verta pasidomėti geros praktikos (angl. *good practices*) atvejais.

Šis būdas palankiausias daugumai mažų ir vidutinių įmonių, kurių pagrindinis tikslas paslaugos kaina, atlikimo greitis, veiksmingumas. Šioms įmonėms išsamus procedūrinis auditas būtų prabanga, kuri daugeliu atvejų būtų netikslinga.

3.8.4 Saugumo priemonių įdiegimo įmonėje planas

Šis planas turėtų būti sudaromas tuomet, kai audito pagalba yra išsiaiškinta kokia situacija yra įmonėje, ir kiek yra nukrypta nuo saugumo politikos dokumento reikalavimų. Už šio plano ir jo įgyvendinimo grafiką turėtų būti atsakingas IT skyriaus vadovas, ar kitas atsakingas pareigas užimantis saugumo darbuotojas. Jei diegimas bus vykdomas be plano, tuomet gero rezultato tikėtis neverta. Praktika rodo, kad parengus saugumo priemonių diegimo planą ir numačius tam resursų, saugumo diegimo veiksmingumas organizacijoje tampa nepalyginti aukštesnis, ypač jei tą planą pasirašo įmonės vadovas ir užtikrinamas stabilus finansavimas.

Kita vertus, specialistų vertinimais, užtikrinti jau veikiančios informacinės sistemos saugumą kainuoja kelis kartus daugiau, nei tai būtų kainavę kuriant sistemą.

Kai organizacija suvokia pagrindinius informacijos saugumo principus, ir kodėl informaciją reikia saugoti. Tik tuomet galima pradėti planuoti ir įgyvendinti organizacijos informacijos saugos politiką. Saugumo politikos valdymas ir kontrolė yra sudėtingas ir sunkus procesas, kurį organizacijai tenka vykdyti, dinamiškoje nuolat besikeičiančioje aplinkoje.

4.TEISINIS REGULIAVIMAS LIETUVOJE IR EUROPOS SĄJUNGOJE

Organizacijos kuriančios savo saugumo politiką svarbu žinoti, kad jų veikla turi atitikti galiojančius įstatymus ir teisės normas. Todėl dažnai įmonės diegdamos saugumo sistemą susiduria su klausimu, kokią įtaką įstatymai turės jų diegiamų informacinių saugos priemonių ir pačios politikos funkcionavimui. Tačiau taip jau susiklostė, kad valdžia daugiausiai būna ne informacinių specialistų rankose. Todėl kai kuriems žmonėms IT nėra pilnai suprantamos, todėl kelia įvairias baimes. Galima pasidžiaugti, kad Lietuvoje saugumo specialistai sistemų saugojimo srityje nemato jokių neprotingų suvaržymų, tačiau kai kuriose šalyse tokių įstatymų yra. Pavyzdžiui, Prancūzijoje be specialaus leidimo draudžiama šifruoti kompiuteryje saugomą arba kompiuterių tinklais perduodamą informaciją. Matyt, kažkada prancūzų saugumo tarnybos pamatė, kad informacijos šifravimas „trukdo" jų darbui, ir jiems pavyko nueiti „paprasčiausiu" keliu. Toks nemodernus požiūris yra naudingas nusikaltėliams. Taigi beliek pasidžiaugti kas pas mus kol kas tokių suvaržymų nėra. Todėl organizacijai plėtojant veiklą užsienio šalyse būtų naudinga susipažinti su ten galiojančiomis nuostatomis.

Lietuvoje elektroninių ryšių veikla yra reguliuojama Ryšių reguliavimo tarnybos, kuri savo veiklą vykdo remdamasi Lietuvos Respublikos „ **Elektroninių ryšių įstatymu** “. Šis įstatymas priimtas **2004 m. balandžio 15 d.** Įstatymas reglamentuoja visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu, taip pat visuomeninius santykius, susijusius su radijo įrenginiais, galiniais įrenginiais ir elektromagnetiniu suderinamumu.[17]

Šio įstatymo įgyvendinimą, prižiūri ir tuo pačiu vykdo veiklą - **Lietuvos Respublikos ryšių reguliavimo tarnyba** (**RRT**). Tai savarankiška valstybės įstaiga, veikianti pagal šį ir kitus įstatymus bei savo nuostatus, išskyrus tas įstatymo nuostatas, už kurių įgyvendinimą ir laikymosi priežiūrą pagal kompetenciją atsakingos kitos valstybės institucijos. Galima paminėti, tai , kad RRT, siekdama suteikti kuo platesnę ir aktualesnę informaciją IT saugumo klausimais, nuolat skelbs informaciją apie:

- Lietuvos IT saugumo padėties **Error! Hyperlink reference not valid.**
- teisės aktus, reglamentuojančius IT saugumą.
- elektroniniais tinklais plintančius tinklų ir informacijos saugumo incidentus.
- kompiuterinių incidentų tyrimo grupės (CERT) veiklą
- RRT bendradarbiavimą su kitomis IT saugumo srityje dirbančiomis Lietuvos **Error! Hyperlink reference not valid.**.
- Europos tinklų ir informacijos saugumo agentūros (ENISA), veiklą bei RRT dalyvavimą šios agentūros veikloje.
- bei kitą aktualią informaciją IT saugumo klausimais.[10]

Kadangi organizacijos naudojasi konfidencialiais asmens duomenimis, turi įvertinti tų duomenų apsaugos svarbą ir tai turi atsispindėti organizacijos saugos politikoje.

Lietuvoje asmens duomenų apsaugą, reglamentuoja „**Asmens duomenų teisinės apsaugos įstatymas**“ nustatantis asmeninių duomenų kaupimo ir apdorojimo reikalavimus. Remiantis šiuo įstatymu visos organizacijos, kaupiančios informaciją apie privačius asmenis kompiuterine forma (telekomunikacijų operatoriai, komunalinių paslaugų įmonės) turi registruotis kaip asmens duomenų saugotojai ir užtikrinti saugomų duomenų apsaugą.[23] Įstatymo įgyvendinimą ir duomenų apsaugą Lietuvoje prižiūri – Valstybinė duomenų apsaugos inspekcija. Pilną informaciją apie šį įstatymą ir jo taikymą, galima rasti inspekcijos internetiniame puslapyje (**www.ada.lt**).

Organizacijoms rekomenduojama saugumo politikos dokumente įvertinti asmens duomenų svarbą, ir jų apsaugai skirti atitinkamą dėmesį. Nes jeigu šie duomenys bus paviešinti arba pavogti, bendrovė gali būti atimta veiklos licencijos, o tai nulemtų didelius nuostolius ir gali būti viena iš įmonės žlugimo priežasčių.

Lietuvoje taip pat **2000 m. liepos 11 d**. buvo priimtas ***„Elektroninio parašo įstatymas“*** **.** Jis reglamentuoja šias sritis:

1. 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.

2. Šis įstatymas nereglamentuoja parašo formavimo ir tikrinimo duomenų bei elektroninio parašo įrangos naudojimo elektroninių duomenų konfidencialumui užtikrinti. [10]

Nors šis įstatymas yra priimtas, tačiau Lietuvoje kol kas nėra iki galo sutvarkyta įstatyminė bazė, ir organizacijos negali pilnai išnaudoti visų verslo galimybių. Tačiau į tai darbe toliau gilinamasi nebus.

2005 m. kovo 24 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 315 dėl Lietuvos Respublikos Vyriausybės 2004-2008 metų programos įgyvendinimo priemonių patvirtinimo buvo numatyta iki 2006 metų pabaigos **įsteigti kompiuterinių incidentų tyrimo padalinį (CERT)** Lietuvos Respublikos ryšių reguliavimo tarnyboje.

Europoje taip pat skiriamas dėmesys informacijos apsaugai. Kaip vieną svarbiausių organizacijų, dirbančių šioje srityje Europos Sąjungos šalyse, būtina paminėti 2004 m. kovo 10 d. įkurtą agentūrą ENISA.

ENISA (angl. *European Network and Information Security Agency*) - tai Europos tinklų ir informacijos saugumo agentūra, įsteigta pagal *Europos Parlamento ir Tarybos reglamentą (EB) Nr. 460/2004*. Ji siekia pagrindinio tikslo – koordinuoti elektroninių ryšių tinklų ir informacijos saugumo veiksmus Europos lygmeniu. ENISA taip pat stengiasi įgyvendinti šiuos siekius:

- stiprinti Bendrijos, šalių narių ir verslo bendruomenės pajėgumus užkirsti kelią tinklų ir informacijos saugumo problemoms, jas nustatyti ir į jas reaguoti;
- teikti pagalbą ir patarti Europos Komisijai bei šalims narėms klausimais, susijusiais su tinklų ir informacijos saugumu;
- remdamasi nacionalinėmis ir Bendrijos pastangomis, didinti kompetenciją bei skatinti aktyvų dalyvių iš valstybinio ir privataus sektorių bendradarbiavimą;
- komisijai paprašius, ENISA jai padeda atlikti techninius parengiamuosius darbus atnaujinant ir toliau tobulinant Bendrijos teisės aktus, reglamentuojančius tinklų ir informacijos saugumo sritį.[37]

Kalbant apie Europos Sąjungą reikėtų pastebėti, kad saugumo politiką, informacijos saugumo problemas reguliuojančių teisinių aktų nėra. Yra tik pateikiamos įvairios rekomendacijos, ir raginimai susirūpinti aktualiomis sritimis. Valstybinėms institucijoms, bankams, registrų centrams ir kitos specifinės paskirties objektams yra skirti specialūs teisiniai nutarimai, specifinės rekomendacijos skirtos juose saugomų duomenų apsaugai.

Taip pat būtina paminėti, kad 2005 m. lapkričio 23 d. RRT, Lietuvos bankų asociacija (LBA) ir asociacija “Infobalt” pasirašė “Pažangos informacijos ir tinklų saugumo srityje memorandumą”, kuriuo siekiama kurti bei ugdyti visuotinę, stiprią informacijos ir tinklų saugumo kultūrą Lietuvoje. Visuomenės švietimas, mokymas, informavimas, saugumo priemonių naudojimas, galimų saugumo incidentų tyrimai, bendradarbiavimas stiprinant teisinę bazę – pagrindinės priemonės, kurias įgyvendins memorandumą pasirašiusios šalys. [7]

5.SAUGUMO POLITIKOS PANAUDOJIMAS LIETUVOS ORGANIZACIJOSE

Tiriamai sričiai Lietuvoje kol kas nėra skiriamas didelis dėmesys. Buvo apžvelgti, keli šios srities tyrimai kurių duomenys pateikiami darbe. Buvo naudotasi šiais tyrimais (**Tinklų ir informacijos saugumo būklė Lietuvoje; „eEurope + 2003“ progreso ataskaita**,**Lietuvos Interneto prieigos paslaugų teikėjų tinklų ir informacijos saugumo valdymas).** Šio tyrimo metu anketinėje apklausoje tiesioginio interviu būdu dalyvavo 500 Lietuvos įmonių atstovų, atsakingų už IT administravimą įmonėse (toliau - Įmonės) bei 31 Interneto paslaugų teikėjas, atsakęs į iš anksto parengtus klausimynus. Šio tyrimo metu buvo siekiama išsiaiškinti tinklų ir informacijos saugumo valdymo politikos naudojimo Įmonėse ir IPT (Interneto paslaugų tiekėjas) mastą, kiek ir su kokiais tinklų ir informacijos saugumo incidentais susiduriama, kaip dažnai naudojamos įvairios apsaugos nuo šių incidentų priemonės bei kokia žala dėl šių incidentų yra patiriama. [20] Visi tyrimo duomenys bus pateikiami 1 darbo priede.

Todėl galime pateikti tyrimo metu nustatytą situaciją. Galima pastebėti, jog dažniausiai pasitaikantys tinklo ir informacijos saugumo incidentai, su kuriais susiduria įmonės ir Interneto paslaugų teikėjai (IPT), yra kompiuteriniai virusai ir nepageidaujami elektroniniai laiškai (angl.spam).

Kompiuterinius virusus, kaip didžiausią grėsmę, nurodė **79 proc.** Įmonių ir net **100 proc**. IPT.

Atitinkamai **76 proc.** Įmonių ir **100 proc**. IPT nurodė susiduriantys su nepageidaujamais elektroniniais laiškais.

Nedidelė dalis Įmonių minėjo įsilaužimus į įmonės kompiuterius (**5 proc**.), duomenų vagystes (**3 proc.**), taip pat atsisakymų aptarnauti (DoS) atakas (**3 proc.**).

Su šiais saugumo incidentais žymiai dažniau susiduria IPT – atitinkamai **28 proc**., **6 proc**. ir **44 proc**.

Tyrimo metu paaiškėjo, jog tik **9 proc.** įmonių nurodė nesusidūrusios su tinklų ir informacijos saugumo incidentais. Tačiau su jais susidūrė visi be išimties IPT

Dažniausiai Įmonių ir IPT naudojama apsaugos nuo tinklų ir informacijos saugumo incidentų priemonė – antivirusinės programos, skirtos kovai su kompiuteriniais virusais. Šią programinę įrangą nurodė naudojantys net **93 proc.** apklaustų įmonių ir **81 proc**. IPT.

Pastebėtas teigiamas aspektas, jog įmonės ir IPT aktyviai naudoja kitą apsaugos priemonę – nuolatinį operacinių sistemų atnaujinimą (ypač kritinių faktorių saugumui užtikrinti) – atitinkamai **80 proc**. ir **91 proc**.

Nustatyta, jog nepakankamai aktyviai įmonėse yra naudojamos šios apsaugos priemonės – ugniasienės (angl. firewall) diegimas, nepageidaujamų elektroninių laiškų (spam) blokavimo priemonės, apsaugos

priemonės nuo šnipinėjančių programų (antispyware). Šias priemones naudoja tik maždaug trečdalis Įmonių. Interneto paslaugų teikėjai šias priemones naudoja žymiai dažniau.

Nustatyta teigiama tendencija, pagal kurią tik **0,2 proc.** Įmonių nurodė nenaudojančios jokių tinklo ir informacijos saugumo priemonių.

Tiek operacinių sistemų, tiek antivirusinių programų atnaujinimas (atitinkamai **56 proc.** ir **65 proc.**) daugelyje Įmonių yra vykdomas automatiškai, pagal programos nustatymus. IPT automatinį operacinių sistemų ir antivirusinių programų atnaujinimą naudoja dažniau – atitinkamai **78 proc**. ir **84 proc.**

Iš apklaustų organizacijų tik **29 proc.** organizacijų ir **45 proc.** IPT nurodė, jog pas juos saugumo valdymo politika yra įgyvendinama, pati įmonė vykdo nuolatinę jos priežiūrą bei atnaujinimą. Net penktadalis apklausos dalyvių – **22 proc**. Įmonių ir **23 proc**. IPT - teigia, jog jų įmonėje nėra jokios saugumo valdymo politikos. [20]

Nors dauguma įmonių naudoja apsaugos priemones, visgi nemaža jų dalis yra patyrę žalos dėl saugumo incidentų - **25 proc.** Įmonių ir **68 proc.** apklausoje dalyvavusių IPT.

Įmonės, patyrusios žalos dėl saugumo incidentų nurodė, kad dažniausiai pasitaikanti žalos forma – tai sutrikusi normali įmonių komercinė veikla. Tai nurodė **52 proc**. Įmonių ir **41 proc**. IPT.

Taip pat nurodoma sugadinta kompiuterių programinė įranga - **43 proc.** Įmonių ir **41 proc**. IPT, ar sugadinti įmonės kompiuteriai – **24 proc.** Įmonių ir **3 proc**. IPT.

Tik nedidelė dalis Įmonių ir IPT naudoja elektroninį parašą konfidencialios informacijos šifravimui ir siuntimui. Dažnai elektroninį parašą naudoja **12 proc**. Įmonių ir **9 proc**. IPT, naudoja kartais – **13 proc**.

Įmonių ir **25 proc**. IPT. Net **73 proc**. Įmonių ir **66 proc**. IPT elektroninio parašo nenaudoja.

Kitas RRT atliktas su informacijos saugumu susijęs tyrimas, kurį reikėtų paminėti tai "**Lietuvos Interneto prieigos paslaugų teikėjų tinklų ir informacijos saugumo valdymas**" Šis tyrimas buvo atliktas 2005 m. sausio – vasario mėn. RRT apklausė Lietuvos Respublikos Interneto prieigos paslaugos teikėjus (toliau – IPT) dėl tinklų ir informacijos saugumo (toliau – IT saugumo) pažeidimų priežiūros elektroninių ryšių tinkluose. Anketos buvo išsiųstos 93 IPT, atsakymai gauti iš 38 IPT. Dalyviu aktyvumas buvo mažiau nei vidutiniškas - 41 %. Toliau pateikiami klausimai, kuriuos gavo IPT. Taip pat bus pateikiami apdoroti tyrimo duomenys.

1 klausimas. Ar Jūsų organizacijoje yra vykdomas tinklų ir informacijos saugumo pažeidimų valdymas?

Gauti atsakymai parodė, kad **68 proc.** IPT vykdo IT saugumo valdymą, organizacijos Interneto tinkle, kai tuo tarpu 32 % IPT tokios veiklos nevykdo ir savo tinklo bei vartotojų saugumu rūpinasi mažai.

2 klausimas. Ar yra suformuota specialiai šiam tikslui vykdyti kompiuterinių incidentų reagavimo grupe? Jeigu taip, kiek personalo įtraukta ir kaip organizuojamas darbas.

IPT atsakymai parode, kad 16 % IPT yra suformavę Kompiuteriniu incidentų reagavimo grupes (taip vadinamas CERT grupes, (angl. CERT – Computer EmergencyResponse Team), kurios gali operatyviai reaguoti į tinklų ir informacijos saugumo pažeidimus organizacijos tinkluose ir koordinuoti veiksmus, šalinant tuos pažeidimus, ypač kai yra potenciali rizika tinklo funkcionalumui ar duomenų saugumui. Asmenų sudarančių CERT grupes dydis Lietuvoje yra svyruojantis, o tuo tarpu statistinis CERT personalo vidurkis yra 8 žmonės.

Didžioji dalis IPT (sudaro 52 %) IT saugumo pažeidimu priežiūrą atlieka be CERT grupės pagalbos. Dauguma šios grupės IPT savo organizacijoje yra įdiegę tam tikras IT saugumo valdymo technines priemones, dažniausiai tai būna ugniasienes (angl. firewall) ar antivirusinės programos, o IT saugumo valdymo funkcijas priskiria organizacijos tinklo administratoriui, kuris vykdo IT saugumo pažeidimo šalinimą. Pateikti duomenys leidžia teigti, kad, kad tinklų ir informacijos saugumo priežiūra Interneto tinkluose vykdoma labai skirtingai, dėl ko kiekviename tinkle pasiekiamas nevienodas tinklo ir vartotojų informacijos saugumo lygis.[20]

3 klausimas. Ar gaunate nusiskundimu iš vartotojų dėl kompiuterinių įsilaužimų, virusų ir pan.? Jei taip, nurodykite jų kiekį bei pobūdį.

66 proc. atsakiusių į šį klausimą kompanijų, nuolat gauna nusiskundimų iš vartotojų dėl IT saugumo pažeidimų, daugiausiai nusiskundimų yra susiję su kompiuteriniais virusais. Šio tipo pažeidimų skaičius svyruoja gana žymiai, nuo keleto ir kelių šimtų per mėnesį priklausomai nuo kompanijos tinklo dydžio, vartotojų skaičiaus ir organizacijos priemonių pritaikytų IT saugumo valdymui. Statistika rodo, kad kiekviename tinkle, fiksuojama po 9 IT saugumo pažeidimus per parą. Likusi dalis įmonių teigė neužfiksavę vartotojų nusiskundimų.

4 klausimas. Kokių priemonių, Jūsų nuomone, valstybes institucijos tūrėtų imtis kovoje prieš tinklų ir informacijos saugumo pažeidimus?

Apklausoje dalyvavę organizacijos pateikė, tokius jų nuomone svarbius pasiūlymus:

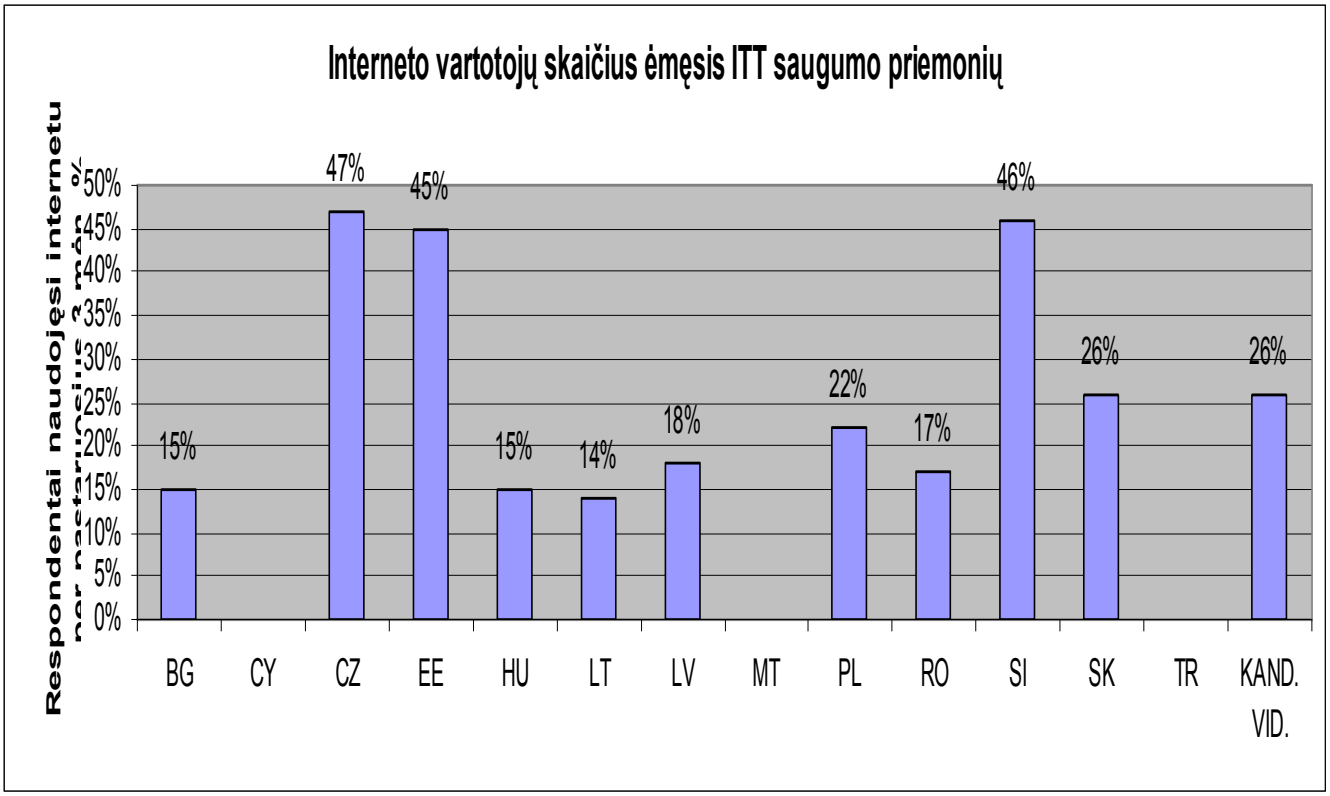
- Formuoti vieningą informacinį ir veiksmų koordinavimo centrą, kuris užsiimtų IT saugumo klausimais, vykdytų saugumo incidentų tyrimus, informuotų apie saugumo grėsmes bei teiktų techninę pagalbą sprendžiant IT saugumo problemas (tokį pasiūlymą pateikė 53 % IPT);
- Vykdyti visuomenes švietimą ir informavimą IT saugumo klausimais (tokį pasiūlymą pateikė 24 % IPT);

- Tobulinti Lietuvos Respublikos teisės aktus griežtinant atsakomybę IT saugumo pažeidėjams (tokio pasiūlymo buvo sulaukta iš 19 % IPT);
- Rengti rekomendacijas IPT dėl IT saugumo pažeidimų priežiūros (tokį pasiūlymą pateikė 10 % IPT).

Įmonės taip pat pateikė pasiūlymus, ką jų nuomone reikėtų tobulinti Lietuvoje. Jų rekomenduojamos sritys sutapo, su darbe jau aptartomis ir minėtomis problemomis: reikėtų skatinti ir didinti IT saugumo priemonių panaudojimą IPT tinkluose, taip pat ir kitose organizacijose, skirti didesnį dėmesį atvirojo kodo programinei įrangai, skirti daugiau lėšų ir didinti kompiuterinį visuomenės raštingumą. Taip pat šioje vietoje turėtų prisidėti valstybė, skirdama didesnį finansavimą, taip padėdama įsigyti IT saugumo priemones.

Tyrimo „Lietuvos pažanga IT sektoriuje“, kurį atliktos Informacinės visuomenės plėtros komitetas (IVPK)

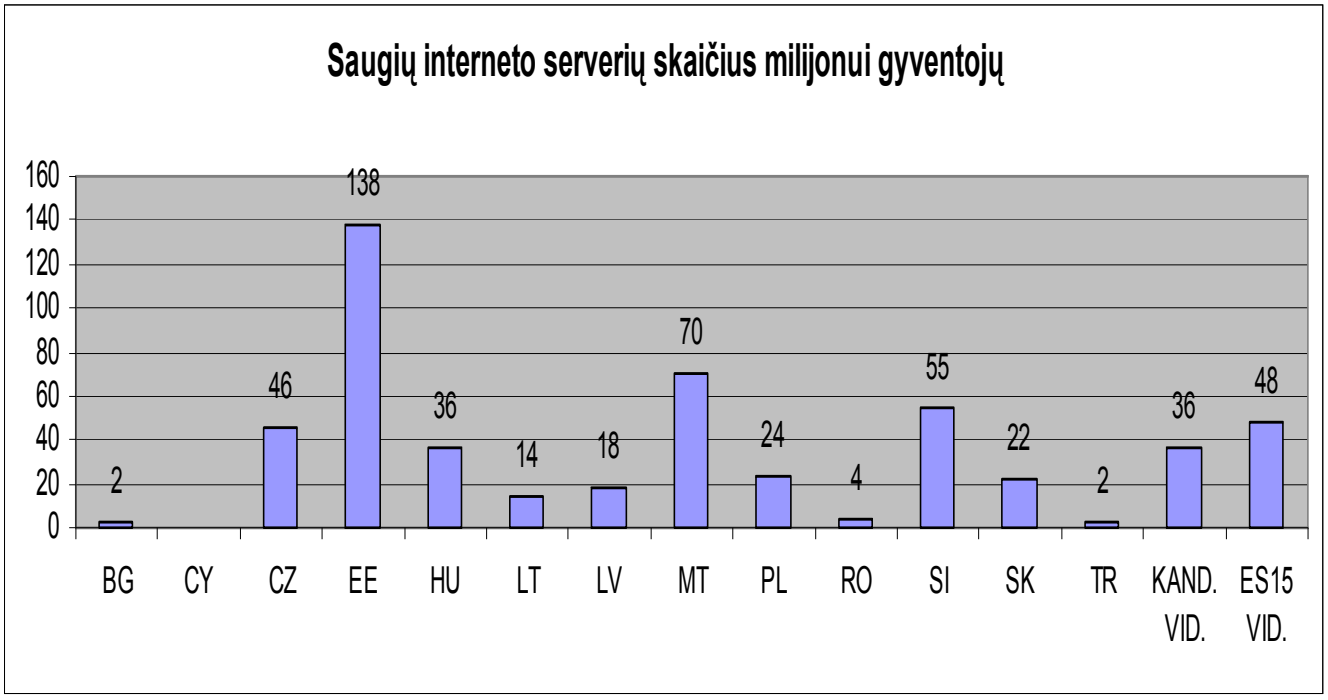
buvo vertinama Lietuvos pažanga „**eEurope + 2003“** programoje. Tyrime buvo analizuota daug įvairių faktorių, tačiau iš jų norėčiau išskirti tokius su saugumu susijusius duomenis.



4 Diagrama. Interneto vartotojų skaičius, ėmęsis ITT saugumo priemonių.[6]

Diagramoje pateikta statistika rodo, kad Lietuvoje lyginant su kitomis ES šalimis, dar nedaug Interneto vartotojų naudojasi kokiomis nors saugos priemonėmis, ši problema dažniausiai kyla dėl to kad dalis žmonių nežinos kas tas saugumas ir kodėl reikėtų saugotis, kita dalis mano kad jų tai nepalies ir

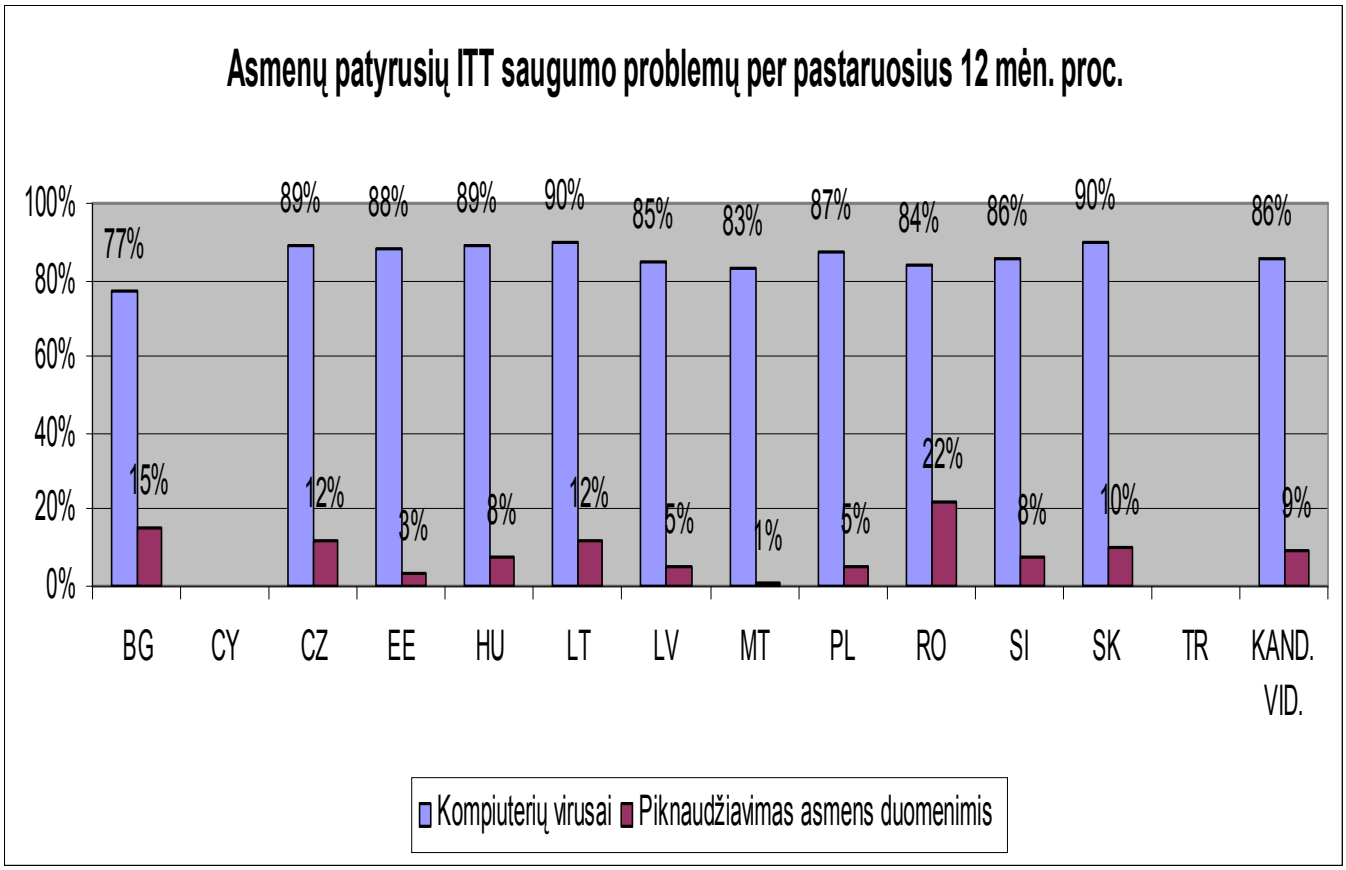
neskiria tam pakankamo dėmesio. Gyventojų informavimas dar nėra pakankamas, tačiau būtina pastebėti, kad tam skiriama vis daugiau dėmesio, rengiami įvairūs su šia tematika susiję projektai. Galima paminėti vieną iš jų, tai RRT ir saugumo spendimus siūlančių kompanijų rengiamas projektas „Apsaugok savo kompiuterį“. Šios akcijos metu bus pagaminta ir išdalinta gyventojams 100 000 nemokamų kompaktinių diskų, kuriuose bus sudėta antivirusinė, kovai su nepageidaujamais laiškais (angl. spam) ir Trojos arkliais skirta programinė įranga, ir kiti su informacijos sauga susiję sprendimai. Akciją planuojama vykdyti visoje Lietuvoje 2006 m. liepos mėnesį.



5 Diagrama. Saugių Interneto serverių skaičius milijonui gyventojų. [6]

Lietuvoje veikiančių saugių Interneto serverių yra tik 14. Tai tikrai blogas rezultatas, parodantis, kad vis dar didelė dalis įmonių neskiria pakankamo dėmesio informacijos saugai. O tai automatiškai mažina verslo pelningumą. Į šią sritį reikėtų atsižvelgti, nes vis daugiau organizacijų savo paslaugas perkelia į elektroninę erdvę. Ir jei nebus užtikrinamas pakankamas saugumas, galima tikėtis

nuostolių.



6 Diagrama. Asmenų, patyrusių ITT saugumo problemų per pastaruosius 12 mėn., proc. [6]

Pagrindinė problema su kuria susiduria tyrime dalyvavę asmenys yra – virusai. Su konfidencialios informacijos praradimu Lietuvoje susidūrė tik 12 procentų asmenų, tačiau ir toks procentas rodo, kad yra problemų, dėl tokios informacijos apsaugos. Kovojant su informacijos spragomis, pažymint. Pasaulio informacinės visuomenės dieną (gegužės 17). Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT) siūlo namų ūkių Interneto vartotojams patikrinti ir įvertinti kompiuterio ir jame saugomų duomenų saugumo lygį. RRT parengė paprastą savitikros testą, kurį atlikę vartotojai sužinos, ar pakankamai apsaugotas yra jų kompiuteris ir jame esantys duomenys. Gavę testo rezultatus, vartotojai galės sužinoti pagrindines rekomendacijas, kaip sumažinti saugumo incidentų elektroninėje erdvėje riziką. Šia iniciatyva siekiama paraginti asmeninių kompiuterių vartotojus būti budresnius ir atidžiau saugoti savo privatumą elektroninėje erdvėje.

Dar norėčiau pateikti kompanijos „IBM Lietuva“ užsakymu, visuomenės nuomonės ir rinkos tyrimų centro „Vilmorus“ atliko tyrimų rezultatus. Kurie parodė, kad Lietuvos gyventojai nesibaimina kompiuterinių įsilaužėliu. Saugumui Internete tampant vis aktualesne problema, dauguma lietuviu, tiki, kad jų kompiuteriai yra saugūs.

Net trečdalis apklaustųjų mano, kad į jų kompiuterius niekas neįsilaužinėja. Taip pat beveik trečdalis atsakė nežinantys, kiek kartų per parą į jų kompiuterį bandoma įsilaužti. **11 proc**. yra įsitikinę, kad namų kompiuteris sulaukia iki 10 įsilaužėlių per parą. Tik **2 proc.** mano, kad vadinamieji „hakeriai“ juos atakuoja nuo 11 iki 100 kartų per 24 valandas. Ir tik 0,7 proc. atsakė, kad kompiuteris kasdien kenčia nuo daugiau kaip šimto įsilaužėlių.

Vyrai drąsesni nei moterys – **36 proc**. vyrų tiki, kad niekas nebando įsilaužti, kai tokių moterų yra 27 proc. Įdomu, kad kompiuterių įsilaužėliu visai nebijo **37 proc.** kaimo gyventojų, tokių drąsių vilniečių yra **29 proc**. [19]

Tuo tarpu saugumo programinės įrangos gamintojo „Webroot Software“ 2006 metų pirmojo ketvirčio ataskaita „The State of Spyware“ parodė, kad 87 proc. namų kompiuterių yra užkrėsti nepageidaujamais programiniais objektais. Vidutinis jų skaičius viename kompiuteryje – 29, iš kurių apie 20 yra sekimo slapukai, o kiti – nepageidaujama reklama, priverstinio nukreipimo Internete priemonės arba šnipinėjanti programinė įranga.
29 proc. namų kompiuterių turi bent vieną „Trojos arklį“ – tai reiškia, jog kas ketvirtas kompiuteris internete nėra savininko pilnai kontroliuojamas. Tai akivaizdžiai rodo, kad per didelis optimizmas yra nepagrįstas ir bet kuriam kompiuteriui būtina taikyti saugumo priemones, siekiant sumažinti rizikos laipsnį.[19]
Matome, kad Lietuvoje, dar skiriamas nepakankamas dėmesys gyventojų švietimui apie pavojus, susijusius su naujausiomis technologijomis. Todėl tiek organizacijoms, tiek paprastiems gyventojams reikėtų geriau pasirūpinti savo duomenų apsauga.

5.1 Sprendimai siūlomi Lietuvos rinkai

Lietuvoje yra organizacijų kurios rinkai siūlo profesionalias „IT Outsorsingo“, saugumo audito, saugumo politikos formavimo, organizacijos veiklos tęstinumo užtikrinimo ir kitas paslaugas. Šie organizacijų sprendimai ir paslaugos yra grindžiamos visame pasaulyje naudojamomis metodikomis ir standartai. Galima paminėti keletą iš jų:

COBIT (Control Objectives for Information and Related technologies) – informacinių technologijų uždavinių, valdymo ir kontrolės gebėjimų organizacinis ugdymas strateginiame lygyje (Lietuvoje šį standartą naudoja Hansa bankas, BITĖ GSM, UAB Ingman Vega);

ISO 17799 (International Standards Organisation Information Security Guidelines) – tarptautinis rekomendacinis informacijos saugumo standartas;

ITIL (IT Infrastructure Library) –informacinių technologijų aptarnavimo ugdymas operaciniame lygyje;

MSF (Microsoft Solutions Framework) ir **MOF** (Microsoft Operations Framework) – verslo rezultatų ir IT sprendimų sugretinimo plano parengimas ir IT sprendimų operacinės priežiūros kompetencijų kūrimas.

SEI SWA CMM (Software Engineering Institute Software Acquisition Capability Maturity Model) – informacinių technologijų įsigijimo planavimas, rizikos valdymas ir IT tiekėjų parinkimas. [12]

Taip pat organizacijoms siūlomos informacijos apsaugos valdymo ciklo paslaugos(Blue bridge):

- informacijos apsaugos politikos sukūrimas,
- informacijos apsaugos būklės analizė,
- informacijos apsaugos stiprinimo plano sudarymas,
- informacijos apsaugos priemonių diegimas,
- informacijos apsaugos sistemos priežiūra.[3]

Lietuvoje paslaugas, susijusias su informacijos apsauga, teikia ir didelių tarptautinių organizacijų padaliniai. Iš jų būtų galima paminėti IBM. IBM saugos konsultantai kartu su jūsų darbuotojais sukurs išsamų darbo planą ir užtikrins, kad visi atliekami darbai atitiktų jūsų organizacijos poreikius. Siekiant užtikrinti taip sukuriamos strategijos atitikimą jūsų veiklos poreikiams ir galimybę ją realizuoti, IBM remiasi savo bendrovės vidaus saugumo programos elementais (pvz., nurodymais ir standartais) bei "geriausia praktika" iš standartų komercinei terpei šiose srityse: organizacija, personalas, fizinis valdymas, nuosavybės klasifikavimas ir valdymas, tinklų ir kompiuterių valdymas, veiklos vientisumas, taikomųjų programų kūrimas ir atitiktis.[19]

Remdamiesi informacija, gauta pokalbiuose su jūsų pagrindiniais veiklos ir IT vadybininkais, IBM saugos konsultantai sukurs bendrą saugumo strategiją, kurioje, be kita ko, pateikiama:

- informacijos saugumo apibrėžimas, aiškiai nurodant vadovybės ketinimus;
- konkrečių saugumo poreikių paaiškinimas, numatant:
    - atitikimą įstatymų bei sutarčių reikalavimams;
    - mokymą saugos srityje, virusų aptikimą ir apsaugą nuo jų, veiklos vientisumo užtikrinimo planavimą;
    - bendrųjų ir konkrečių vaidmenų bei atsakomybės už įvairius informacijos saugumo programos aspektus apibrėžimą;
    - būtinybės registruoti įtariamus saugumo pažeidimus bei atitinkamo proceso paaiškinimą;

- strategijos dokumentų tvarkymo procedūrą, numatančią vaidmenis ir atsakomybes.

Informacijos valdymo ir apsaugos sprendimus siūlo „Alna Intelligence“, taip pat UAB „Compservis“. Ši organizacija siūlo informacijos apsaugos rizikų analizės ir valdymo metodiką CRAMM. Taip pat organizacijos gali naudotis informacijos apsaugos ir sistemų audito paslaugomis, galima paminėti, jog Lietuvoje jas siūlo „**ITAG“ – Informacinių technologijų audito grupė**, taip pat „**ISACA Lietuva“ - Informacinių sistemų audito ir valdymo asociacija**.[11]

Galima pasidžiaugti, kad mūsų šalyje taip pat yra organizacijų, kurios suvokia informacijos apsaugos projektų svarbą, ir yra įsidiegę atitinkamas informacijos apsaugos sistemas. Praktika rodo, kad vidutinės įmonių investicijos į informacijos saugumą ir IT krizių prevenciją beveik visada yra mažesnės už nuostolius, patiriamus šalinant net nedideles duomenų apsaugos problemas. Neveikianti arba stringanti informacijos sistema įmonei dažniausiai reiškia prarastus klientus, negautas pajamas, baudas dėl neįvykdytų įsipareigojimų, kenkia įmonės įvaizdžiui, o nedidelėms bendrovėms rimti sistemos sutrikimai ilgesnį laiką gali reikšti net bankrotą.[3]
Kaip sėkmingą pavyzdį galima paminėti „ Lietuvos energijos“ įmonę, kuri savo veikloje naudojasi šiuolaikine informacijos valdymo ir apsaugos sistemą, skirta apsaugoti įmonės verslui svarbius duomenis. Specialistų pagalba visi darbai buvo atlikti kompleksiškai ir laikantis tarptautinių standartų, taip maksimaliai užtikrinant įmanomą duomenų saugumo lygį vienai didžiausių Lietuvos organizacijų. Šios įmonės sėkmė, galėtų būti pavyzdžiu kitoms organizacijoms, tai padėtų joms suprasti, kad informacijos saugumu būtina rūpintis nuolat, ir kad tai yra besitęsiantis procesas. Saugumo sprendimus siūlančių kompanijų duomenimis paskutinius kelis metus visoje Lietuvoje buvo ne daugiau kaip kelios dešimtys įmonių, vykdžiusių kompleksiškus informacijos saugos projektus. Didžioji dalis iš saugos projektus buvo didelės šalies draudimo, telekomunikacijų, energetikos bendrovės. Taip pat specialistai pažymi, kad pastaruoju metu saugos problematika aktyviai domėtis ėmė ir kai kurios finansinių paslaugų bei gamybos įmonės.
Praktika rodo, kad vidutinės įmonių investicijos į informacijos saugumą ir IT krizių prevenciją beveik visada yra mažesnės už nuostolius, patiriamus šalinant net nedideles duomenų apsaugos problemas. Nefunkcionali arba stringanti informacijos sistema įmonei dažniausiai reiškia prarastus klientus, negautas pajamas, baudas dėl neįvykdytų įsipareigojimų, kenkia įmonės įvaizdžiui, o nedidelėms bendrovėms rimti sistemos sutrikimai ilgesnį laiką gali reikšti net bankrotą. Todėl reikėtų vengti tokių situacijų, kuomet
„Informacijos vertė dažniausiai išaiškėja per vėlai – tik po to, kai susiduriama su problema“.[3]

IŠVADOS

Informacija, kuri buvo gauta lyginamosios analizės pagalba ir buvo pateikta darbe, leido puikiai įsitikinti įmonės sėkminga veikla ir vystymasis priklauso nuo sugebėjimo atlikti tinkamus saugumo politikos sprendimus,gebėjimo valdyti priemones ir procesus. Darbo pabaigoje, dar kartą rekomenduotina paminėti ir, vieną svarbiausių sėkmingo saugumo principų, t.y. „saugumas – tai besitęsiantis procesas, kuris niekada nesibaigia“. Labai svarbu, kad organizacijų vadovai suvoktų ne tik svarbiausius informacijos saugumo principus, bet ir tai, kad nupirkus ir įdiegus saugumo priemones, visos problemos išsispręs. Netgi įdiegus moderniausias priemones, sėkmes tikėtis būtų sunku, jei nebus žinoma, kokius organizacijos išteklius norima apsaugoti. Norint išvengti netikslingų investicijų, sutaupyti laiko, įmonių vadovams rekomenduojama, kuriant savo įmonės veiklos viziją ir strategiją, atsižvelgti į darbe analizuotas saugumo diegimo metodikas, gerų praktikų rinkinius, specialistų (Peltier, Thomas R, Palmer, I., G. Potter, Gertz M, ISF, ISACA ir kt.) pateikiamas rekomendacijas organizacija gali tikėtis sukurti savo organizacijai tinkamą apsaugos politiką, kuri bus funkcionali, atitinkanti jos poreikius, apsaugoti svarbiausius įmonės resursus ir kartu prisidedanti prie sėkmingos įmonės plėtros ir jos veiklos tęstinumo užtikrinimo.

Visa informacija, kuri buvo surinkta rašant šį darbą leido įsitikinti, kad svarbų vaidmenį informacijos apsaugos procese atlieka žmogus. Žmogaus turimos žinios, sugebėjimai vertinti informaciją kuriant saugumo politiką, gali turėti didelę reikšmę. Todėl žmonės, kuriantys saugumo politiką, turi būti sukaupę pakankamą žinių bagažą, kuris padėtų jiems sėkmingai pasinaudoti moderniomis technologijomis, metodikomis ir jas efektyviai panaudoti. Technologijos turi būti žmogaus darbo ir kūrybos įnagis. Todėl ne veltui rekomenduojama skirti atitinkamą dėmesį darbuotojų mokymui, jų kvalifikacijos kėlimui. Manytina viena iš nesėkmių priežasčių yra nepakankamas dėmesys darbuotojų mokymui, tokias išvadas leidžia daryti darbe apžvelgta Lietuvos įmonių situacija. Todėl šiai sričiai reikėtų skirti daugiau dėmesio.

Rašant darbą buvo pasiektas darbo įvade apibrėžtas tikslas įgyvendinti užsibrėžti uždaviniai. Darbe pateiktos dažniausiai su pagrindinėmis saugumo formavimo procese sutinkamos sąvokos, terminai. Išanalizuoti ir pateikti, svarbiausi saugumo politikos formavimo etapai, apžvelgtos dažniausiai sutinkamos ir naudojamos saugumo metodikos, paminėti privalumai ir pavojai, kuriuos suteikia “IT outsorsingas“, taip pat atskleista, kodėl toks svarbus yra įmonės veiklos tęstinumo užtikrinimas, išvardinti veiksniai, dėl kurių kartais nefunkcionalios tampa ir atrodytų geros saugos politikos.

Siekiant, kad darbas būtų naudingesnis, apžvelgtos Lietuvos ir ES teisinės normos ir rekomendacijos. Rašant darbą buvo ieškota ir pasiremta aktualiais 2004-2006 m. tyrimų duomenimis,

kurių pagrindu buvo stengtasi apžvelgti saugumo situaciją, išskirti ir paminėti aktualiausias problemas mūsų šalyje veikiančioms įmonėms.

Darbe analizuota sritis yra aktuali ir problematiška. Nuolat besikeičiant technologijoms, didėjant pasaulio globalizacijai, įmonių sugebėjimas vertinti ir valdyti informacijos saugumą, tampa vienu iš veiksnių garantuojančių įmonės išlikimą. Pastebėta, kad tam tikru laikotarpiu organizacijų vadovybė didžiausią dėmesį skyrė modernių technologijų įsigijimui.. Tačiau organizacijos pastebėjo, tik sukūrus tinkamą planą, apmokius darbuotojus, parengus organizaciją pokyčiams galime tikėtis.

Rašant darbą buvo analizuoti šaltiniai anglų ir lietuvių kalbomis. Anglų kalba pateikiama daug naudingos informacijos tiek apie techninius, tiek bendrus dalykus, tyrinėtojai yra parengę gerų praktikų ir kitų rekomendacijų. Taip pat pastebėtas didelis šios tematikos knygų ir vadovėlių trūkumas. Lietuvoje yra ne viena įmonė teikianti saugumo valdymo, diegimo paslaugas ir tam pasitelkianti tarptautines metodikas. Tačiau didžioji dalis tos informacijos yra mokama ir paprastam vartotojui ją gauti sudėtinga. Manyčiau, saugumo srities problemų, sprendimų populiarinimui turėtų skirti tiek privatus, tiek valstybinis sektorius.

Galima paminėti, kad šioje srityje vyksta teigiami procesai, kuriami specialūs saugumo tematiką nagrinėjantys portalai. Informacija, pateikiama tuose portaluose, gali būti naudinga tiek asmenims besidomintiems saugumo problemomis, tiek specialistams.

Šis darbas galėtų būti panaudojamas, kaip apibendrinta ir susisteminta teorinė priemonė apie pagrindinius saugumo procesus ir etapus. Ji gali būti naudinga visiems besidomintiems informacijos saugumu. Bibliografiniame sąraše pateikiamos papildomos nuorodos į platesnius ir specifinius informacijos šaltinius.

Analizuojant darbe pateiktą informaciją, taip pat remiantis asmenine patirtimi, įgyta dirbant realiai veikiančioje organizacijoje, kasdien dirbant su įmonės informaciniais resursais. Galima pastebėti, kad Lietuvoje dar didelė dalis darbuotojų, vadovų ir klientų nežino apie informacijos saugą ir galimus nuostolius, jei bus pažeisti pagrindiniai informacijos saugumo principai. Taip pat gana didelė dalis įmonių vadovų informacijos apsaugą laiko nereikalingomis investicijomis, nesukuriančiomis jokios apčiuopiamos pridėtinės vertės. Taipogi darbe jau minėtas per didelis pasitikėjimas technologijomis, nesugebėjimas įvertinti savo esminių resursų, įmonės veiklai netinkančių sprendimų pasirinkimas. Darbe buvo analizuoti saugumo specialistų (Peltier, Thomas, R, Palmer. I.G. Potter) darbai, taip pat apžvelgtos ir pristatytos tarptautinių saugumo organizacijų (ISF, ISACA, CSI ir kt.) saugumo diegimo metodikos, gerų praktikų rinkiniai. Todėl darbo gale norėčiau pateikti savo rekomendacijas, kurios iš visų apžvelgtų, atrodo svarbiausios sėkmingam organizacijos saugumo įgyvendinimui:

- Prieš pradėdama formuoti savo saugos politiką organizacija turėtų išanalizuoti dabartinę organizacijos būklę, identifikuoti pagrindinius informacijos išteklius, įvertinti potencialias rizikas, organizacijos situaciją rinkoje ir tik tuomet pradėti saugos politikos formavimą.
- Pasitikrinti, ar tikrai gerai organizacija įvertino, kokį poveikį jos funkcionavimui turės saugumo įdiegimas. Negalima pamiršti, kad bet koks saugumas verslo procesus padarys šiek tiek sudėtingesnius.
- Stengtis, kad saugos politika, būtų vienas iš sudėtinių įmonės strategijos ir vizijos elementų, o ne priverstinai sukurtas taisyklių rinkinys.
- Įvertinti ir pasirinkti įmonės veiklos specifiką ir norimos apsaugoti informacijos vertę atitinkančias technologijas. Taip pat naudoti laiko patikrintas ir pasiteisinusias metodikas, taip pat rekomenduojama išanalizuoti savo partnerių, klientų naudojamas metodikas ir sistemas. Todėl patartina naudoti panašius, lengviau suderinamus saugumo sprendimus.
- Įvertinti savo sugebėjimus ir resursus, sėkmingai įsidiegti saugumo sistemą. Ir jei manoma, kad organizacija bus nepajėgi tai padaryti, apsvarstyti galimybes šiuos procesus perduoti kitai organizacijai.
- Nuolat rengti mokymus darbuotojams, taip suteikiant jiems naujausią informaciją apie paskutines saugumo naujienas ir tendencijas, kartu tai padės išvengti įvairių netikėtumų.
- Ir nepamiršti, kad šimtaprocentinis saugumas yra neįmanomas. Tai procesas vykstantis 24 valandas per parą ir 7 dienas per savaitę.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS:

1. Fiske.J. *Įvadas į komunikacijos studijas*.-Vilnius: Baltos lankos.-1998.-239p.[1]

2. Rizikos analizės vadovas. *Administracinių ir techninių gebėjimų stiprinimas užtikrinant duomenų informacinių technologijų ir jomis perduodamų duomenų apsaugą.* Lietuvos Respublikos Vidaus Reikalu Ministerija.-Vilnius: Vaga.- 2005. – 161 p. ISBN 54150118271. [2], p. 15-21.

3. UAB „Blue Bridge“ IT sprendimai ir paslaugos verslui. [iinteraktyvus]. [žiūrėta 2006 m. Gegužės 10 d.]. Prieiga per internetą:<http://www.bluebridge.lt/lt.php?show_content_id=2032>. [3]

4. COBIT Methodology. Iš *ISACA Serving IT governanse profesionals.* [interaktyvus]. [žiūrėta 2006 m. Kovo 14 d.] Prieiga per Internetą:< http://www.isaca.org/>.[4]

5. UAB „Compservis“. Informacijos apsaugos ir IT paslaugų valdymo skyrius. [interaktyvus]. [žiūrėta 2006 m. Vasario 10 d.]. Prieiga per Internetą:< http://www.cramm.lt/index.php/lt/34651/> .[5]

6. eEurope + 2003, Progreso ataskaita. Iš *Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės.* [interaktyvus]. [žiūrėta 2006 m. Gegužės 2 d.]. Prieiga per Internetą:< www.infobalt.lt/docs/040219_eEurope_plus_20031.ppt.>. [6]

7. Infobalt Lietuva. [interaktyvus]. [žiūrėta 2006 m. Sausio 10 d.]. Prieiga per Internetą:< http://www.infobalt.lt/konferencija/2001/IV2001/index.php?g=&r=59&i=6677>. [7]

8. Informacijos apsaugos standartai. Iš *esaugumas* [interaktyvus], [žiūrėta 2006 m. Gegužės 5 d.]. Prieiga per internetą:<http://www.esaugumas.lt/index.php?539320965>. [8]

9. Informacijos saugumo aspektai. Iš *Verslo žinios, Konsultacijos vadovui.* [interaktyvus]. [žiūrėta 2005 m. Gegužės 5 d.]. Prieiga per internetą:< http://www.vz.lt/konferencijos/konsultacijos/it/index.php>. [9]

10. Rizikos valdymo projektai. [interaktyvus]. [žiūrėta 2006 m. Gegužės 29 d.]. Prieiga per internetą:<www.elm.lt/lt/ vadybos_konsultacijos/rizikos_valdymo_p.php >. [10]

11. ISACA. Paslaugos IT valdymo profesionalams. [interaktyvus]. [žiūrėta 2006 m. Kovo 28 d.]. Prieiga per internetą:< http://www.isaca.lt/lt/cobit/>. [11]

12. ITAG Informacinių technologijų audito grupė. [interaktyvus]. [žiūrėta 2006 m. Balandžio 27 d.]. Prieiga per internetą:< http://www.itag.lt/xid.php?xid=1010>. [12]

13. ITIL. Iš *ITIL IT service management* [interaktyvus] [žiūrėta 2006 m. Balandžio 12 d.] Prieiga per internetą:< http://www.itil.co.uk/about.htm>.[13]

14. ITIL Forumas. Iš *IT paslaugų valdymo forumas* [interaktyvus]. [žiūrėta 2006 m. Kovo 14 d.] Prieiga per internetą:< http://itsm.lt/phpBB2/viewtopic.php?p>. [14]

15. Įvadas į informacinę saugą. *Iš E-servisas-Dirbame jūsų verslui.* [interaktyvus]. [žiūrėta 2006 m. Balandžio 25 d.] Prieiga per internetą:< http://www.e-servisas.lt/index.php?option=com_content&task=view&id=23&Itemid=28>. [15]

16. Kas yra standartas 7799? Iš *Infosec.lt* [interaktyvus]. [žiūrėta 2006 m. Gegužės 10 d.]. Prieiga per internetą:< http://www.infosec.lt/standartas-7799.php>. [16]

17. Lietuvos Respublikos Seimas. [interaktyvus], [žiūrėta 2006 m. Gegužės 5 d.]. Prieiga per internetą:< http://www3.lrs.lt/dokpaieska/forma_l.htm.>. [17]

18. Standartai 7799. Iš *eSecurity* [Interektyvus] [žiūrėta 2006 m. Balandžio 25 d.] Prieiga per internetą:<http://www.esecurity.lt/article/1567.html>. [18]

19. Saugos ir privatumo paslaugos. Iš IBM Lietuva. [Interaktyvus] [žiūrėta 2006 m. Balandžio 14 d.] Prieiga per internetą:http://www-5.ibm.com/lt/services/security.html>. [19]

20. Tinklų ir informacijos saugumo būklės Lietuvoje tyrimas. Įmonių ir IPT apklausa Iš *Lietuvos respublikos ryšių reguliavimo tarnyba*. [interaktyvus]. [žiūrėta 2006 m. Gegužės 10 d.]. Prieiga per internetą:< http://www.rrt.lt/index.php?174255322>. [20]

21. TNS Gallup. [interektyvus]. [žiūrėta 2006 m. Gegužės 25 d.] Prieiga per internetą:< http://www.tns-gallup.lt/lt/disp.php/lt_news/lt_news_grp5_>. [21]

22. Vageris R. Informacijos apsauga įmonėje. Iš *Infobalt 2003, Spalio 23 d*. [Interaktyvus] [žiūrėta 2006 m. Balandžio 25 d.] Prieiga per internetą:< https://www.infobalt.lt/docs/Robertas_Vageris.ppt.> [22]

23. Valstybinė asmens duomenų inspekcija. [interaktyvus]. [žiūrėta 2006 m. Gegužės 10 d.]. Prieiga per internetą:< http://www.ada.lt/index.php?lng=lt&action=page&id=65>. [23]

24. Ellof Jan. H.P. *Advaces in information security management & small systems security*. 2001.[24]

25. Fine, N. *The economic espionage act: Turning fear into compliance. Competitive intelligence review*. Volume 8, number 3, fall 1997. [25]

26. Gertz M. *Integrity, internal control and security in information systems/ Connecting Governance and technology*. Kluwer Academic Publishers. - 2002. 214 p. ISBN 1402070055.[26]

27. Gritzalis. D, Sokratis K. Katsikas (Editor.): S*ecurity and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003)*, May 26-28, 2003, Athens: Kluwer Academic Publishers. – 2003. 250 p. ISBN 1-4020-7449-2, p. 107. [27].

28. Guttman, B. and E. Roback. *An introduction to computer security: NIST Handbook, U.S. National Institute of Standards and Technology, NIST Special Publication*. Gaithersburg: U.S Department of commerce. -1995. 180 p. [28], p. 57.

29. Krause, M., Tipton, H.F. (Editors). *Handbook of Information Security Management*. Boca Raton: CRC Press LLC. – 1998. [29]

30. Palmer, I., and G. Potter. *Computer Security Risk Management*. New York: Van Nostrand Reinhold. - 1989. 317 p. ISBN 0442302908. [30]

31. Peltier Thomas R. *Information security policies, procedures, and standarts/guidelines for effective information security management*. Boca Ratos: Auerbach. - 2001. 350 p. ISBN 0849311373. p. 110.[31]

32. Peltier, Thomas R. *Information security policies and Procedures: A Practitioner's reference*. Boca Raton: CRC Pres. – 2004. 448 p. ISBN 0849319587, p. 108, [32]

33. A 6-step strategy for Information Security Management. Iš IsecT Ltd. [interaktyvus], [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.isect.com/html/strategy.html>.[33]

34. Cybercecurity gateway. [interaktyvus], [žiūrėta 2006 m. balandžio 12 d.]. Prieiga per internetą:< http://www.itu.int/cybersecurity/index.html>.[34]

35. 2005 CSI/FBI Computer crime and security survey Iš *Computer Security Institute.* [interaktyvus], [žiūrėta 2006 m. balandžio 12 d.]. Prieiga per internetą:< http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml />. [35]

36. COBIT 4. Iš ISACA Serving IT Governance Profesionals. [interaktyvus], [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.isaca.org/>. [36]

37. ENISA, European network and informatikon security agency. [interaktyvus], [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.enisa.eu.int/>. [37]

38. Informaction security. IT Examination handbook. Iš *Federal Financial Institutions Examination Council.*[interaktyvus]. [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security_low_res.pdf>.[38]

39. SF – The informatikon security forum standart of good practice. Iš The standart for informatikon security. [Interaktyvus], [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.isfsecuritystandard.com/index_ns.htm>. [39]

40. NIST 800. Iš Computer security division: Computer security resource center. [interaktyvus], [žiūrėta 2006 m. Gegužės 5 d.]. Prieiga per internetą:<http://csrc.nist.gov/publications/nistpubs/>. [40]

41. The Systems Security Engineering Capability Maturity Model (SSE-CMM) Iš The International Systems Security Engineering Association. [interaktyvus]. [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.sse-cmm.org/index.html>. [41]

42. Why security policy fails? Iš *global networked IT services*. [interaktyvus]. [žiūrėta 2006 m. Gegužės 18d.]. Prieiga per internetą:< http://www.btglobalservices.com/business/global/en/index.html >. [42]

THE FORMATION OF INFORMATION SECURITY POLICY IN A MODERN ORGANIZATION

SUMMARY

The main object of work – creation of information security policy, in modern organization. The main purpose of this work – to analyze and in the end of this work give recomendations, that wuold be useful and wil help organization to know better what is security policy and implement this policy in organizaton. Main tasks, determined in the final work are: determinate conception of information security policy, to explore the main stages of security policy creation; review and introduce internationals standarts and formats which are available on market, to familiaraise with most imoportan steps of security strategy and documentaition; determinate main organization maturity models, which are used in security threats analysis. To analize, what size investition are allocated to secure company's information; to explore that situation is in Lithuanian market, which security metodics and products are available for Lithuanian organization.

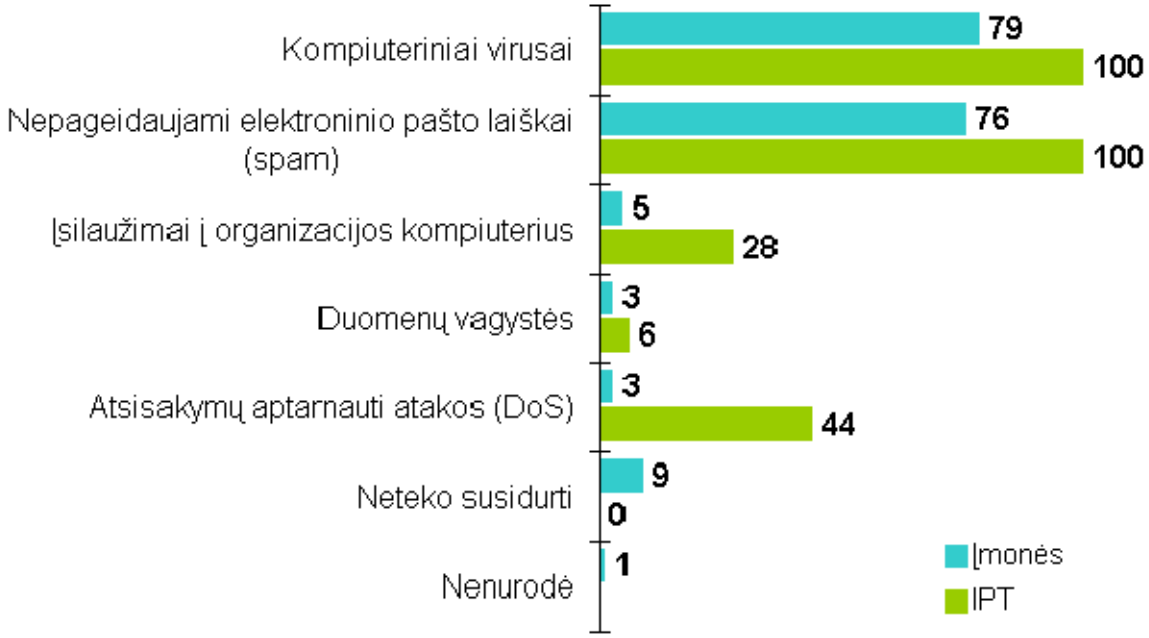
Successful implementation of security policy in organization depends, from that, how organization will perceive security importance, how they will identify most important information resources, and forecast how this new policy will impact business activity. Also very important is not to make mistakes, choosing methodic ant technologies, which would be adequate to organizations activity. According to the analysis of security methodic and most important security policy steps, is easier to asses the main problems in security process, and to identify reasons which may make security policy inefficient. Successful implementation of security policy, employees training, good manager's security understanding will help to avoid many problems.

This work is systematized information about main security policy steps and process, most popular standards, occurring problems ant recommendations how to avoid them. So this work, can be used as a broad – brush and structures theoretical tool, about mains security process. It can be useful, to everyone who is interested in information security.

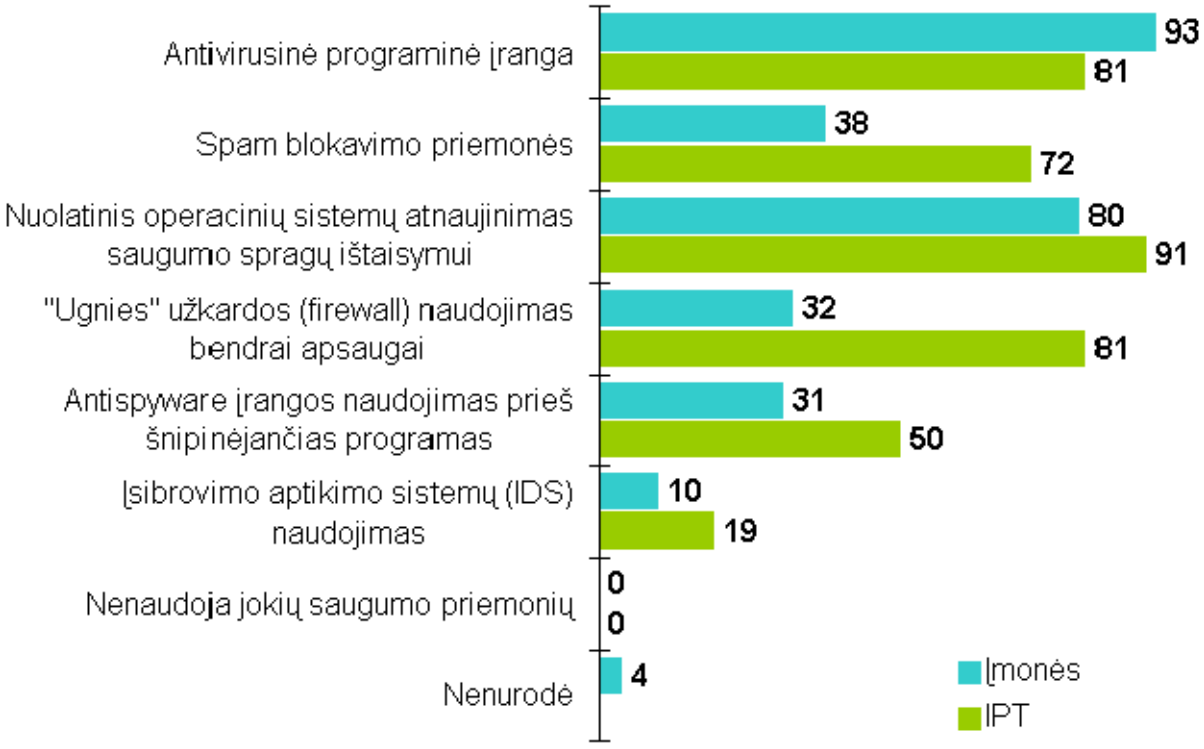
PRIEDAI

1 Priedas. Tinklų ir informacijos saugumo būklės Lietuvoje tyrimas. Įmonių ir IPT apklausa.

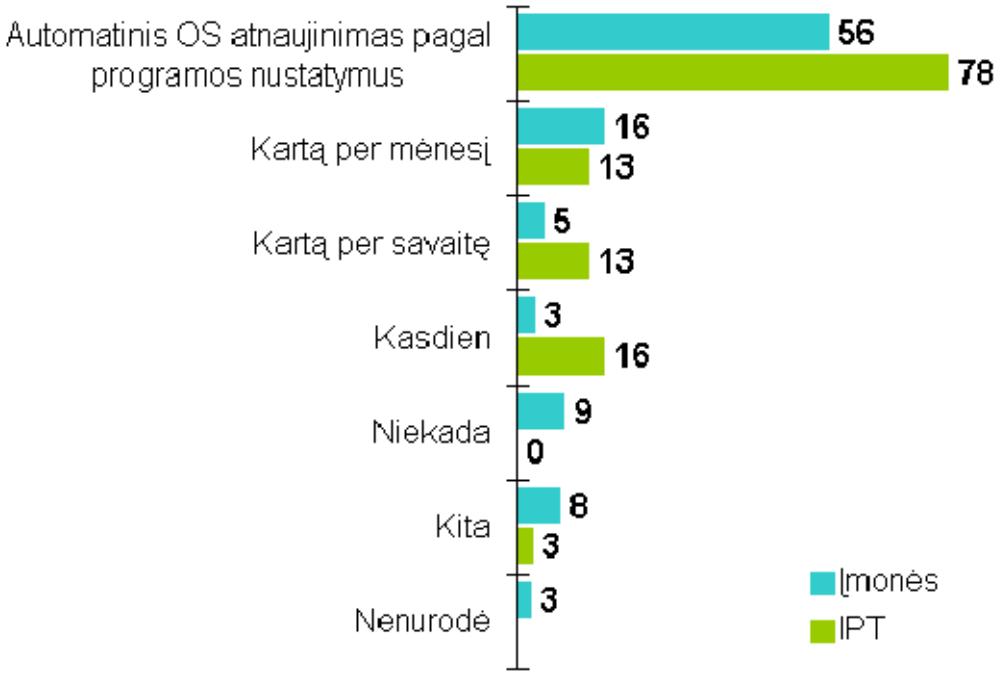
Tinklų ir informacijos saugumo incidentų tipai, su kuriais susiduria Įmonės ir IPT (procentais)[20]



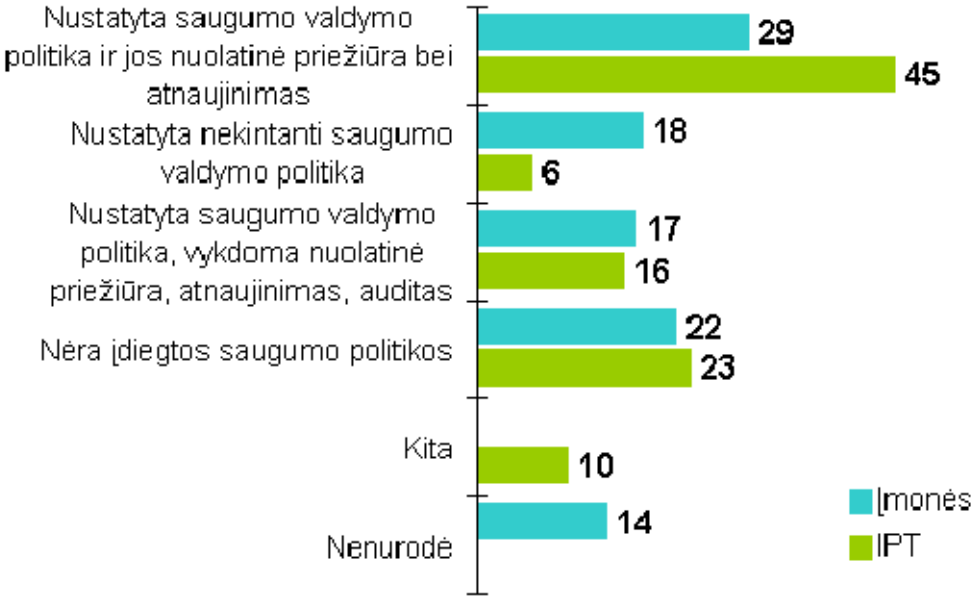
Tinklų ir informacijos saugumui užtikrinti naudojamos priemonės (procentais)[20]



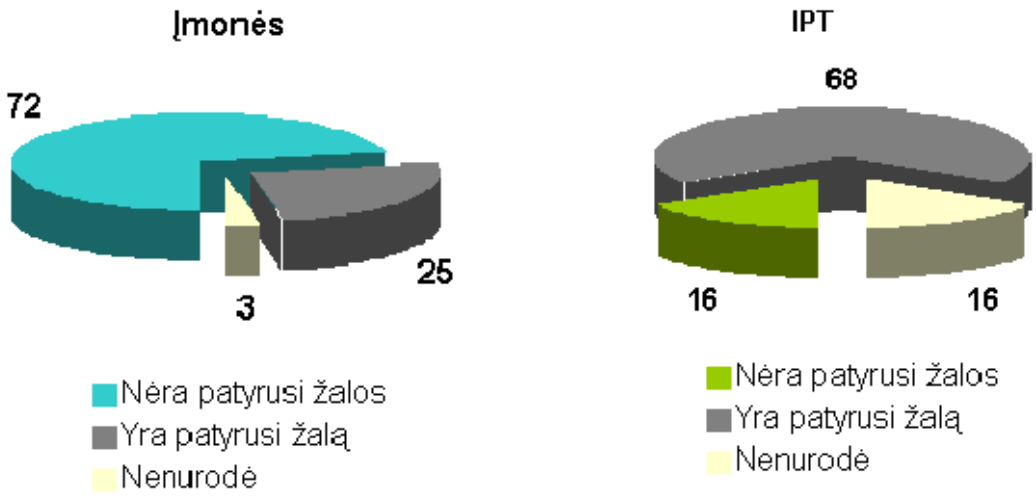
Operacinių sistemų atnaujinimo Įmonių ir IPT kompiuteriuose dažnumas (procentais)[20]



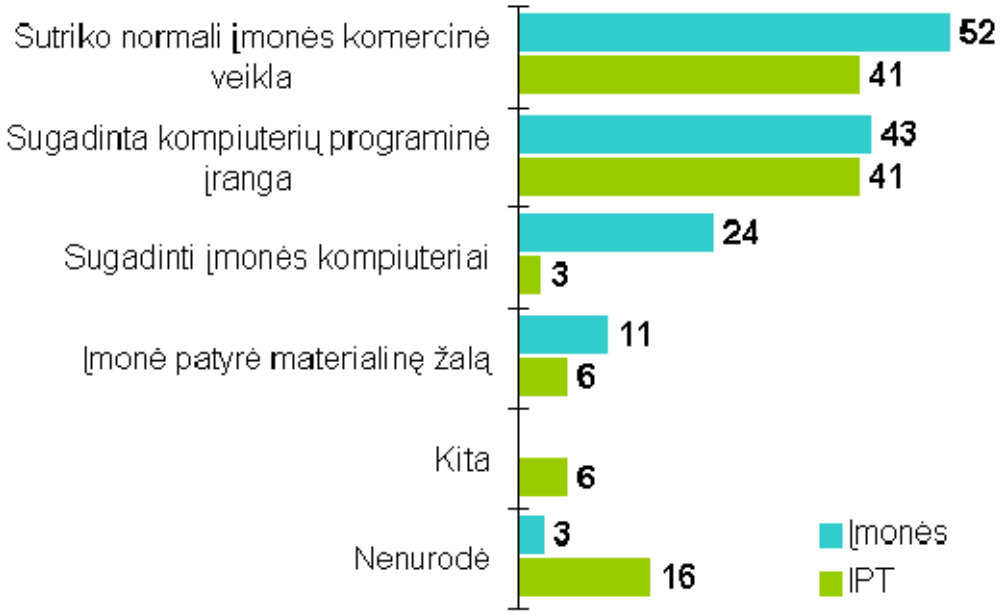
Saugumo valdymo politikos naudojimas Įmonėse ir IPT (procentais)[20]



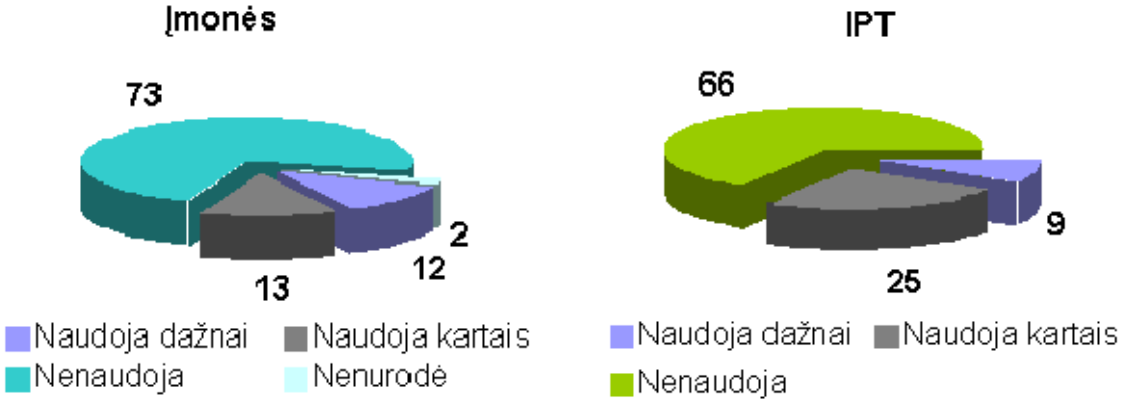
Įmonės ir IPT, patyrusios žalos dėl tinklų ir informacijos saugumo incidentų (procentais)[20]



Įmonių ir IPT patirtos žalos dėl tinklų ir informacijos saugumo incidentų pobūdis (procentais)[20]

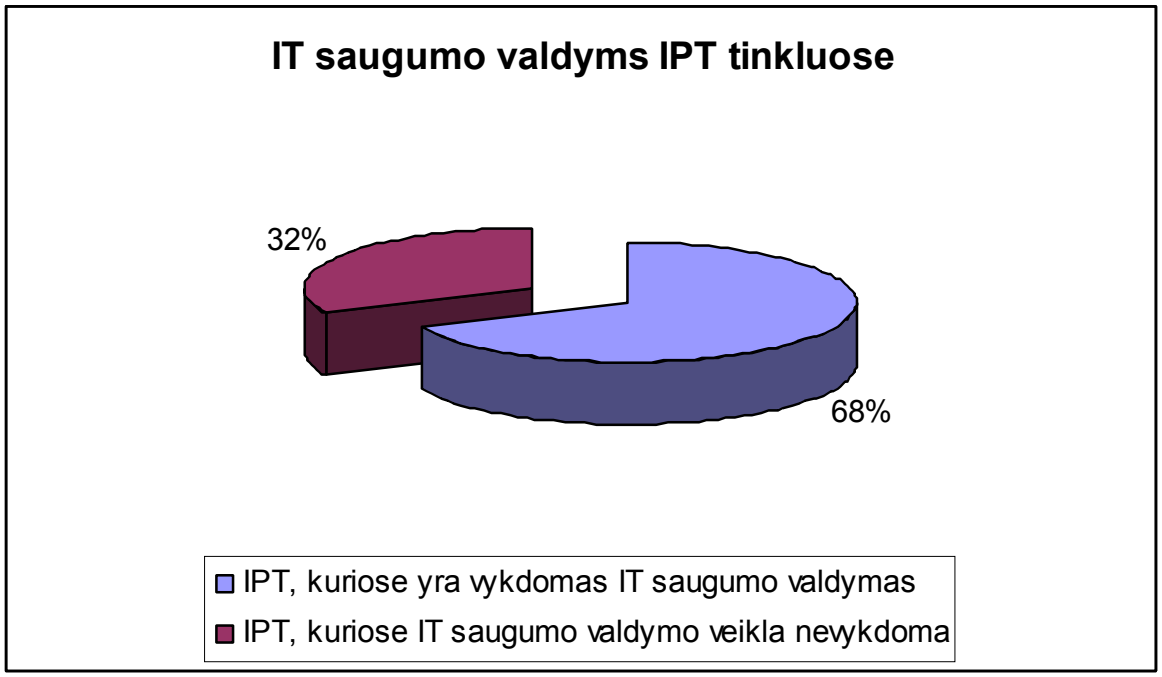


Įmonės ir IPT, naudojančios elektroninį parašą konfidencialios informacijos šifravimui ir siuntimui (procentais) [20]

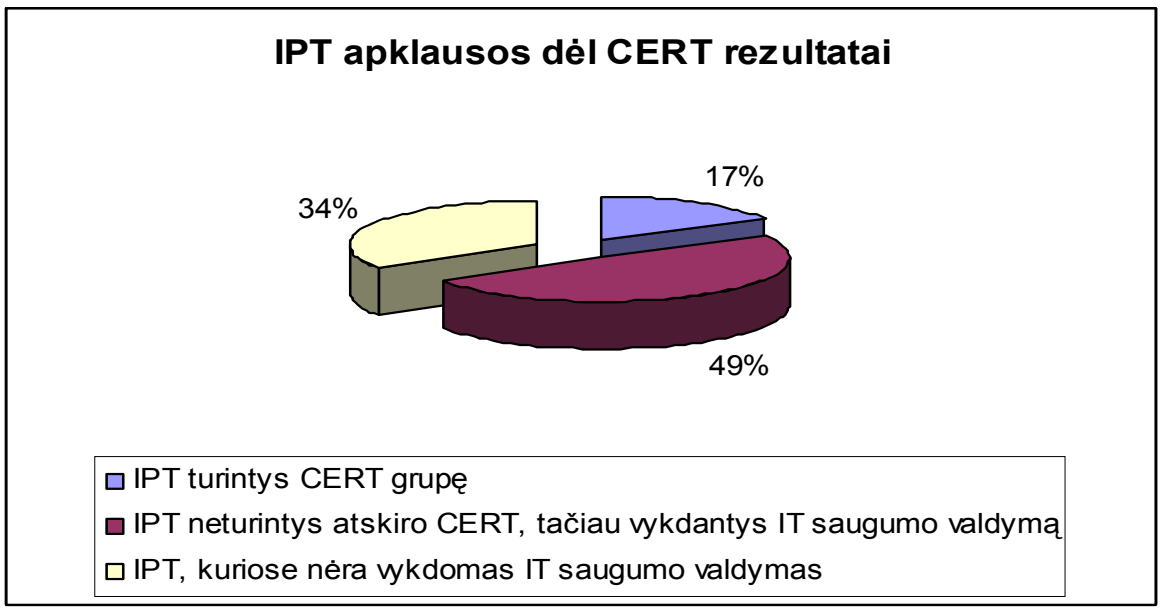


2 Priedas. Lietuvos Interneto prieigos paslaugų teikėjų tinklų ir informacijos saugumo valdymo tyrimas

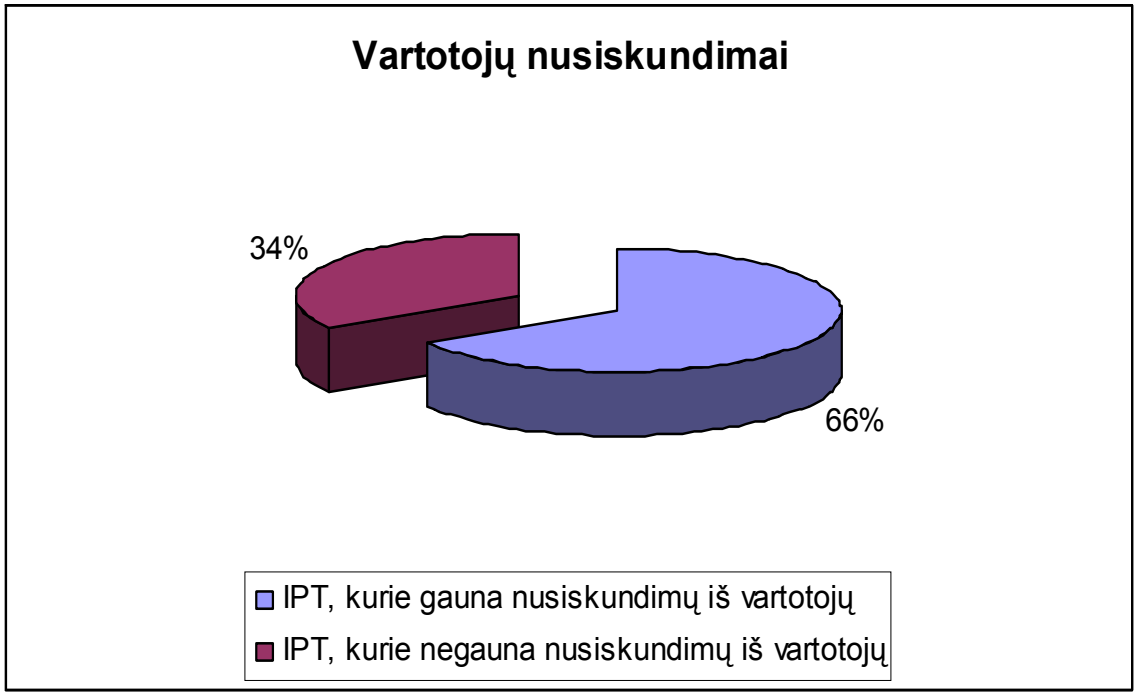
IT saugumo valdymo IPT tinkluose tyrimo rezultatai [RRT]



IPT apklausos dėl kompiuterinių incidentų reagavimo grupės rezultatai [RRT]



Vartotojų nusiskundimų tyrimo rezultatai[RRT]



3 Priedas. ISO/IEC 17799:2005 apsaugos standarto priemonių sąrašas su trumpu paaiškinimu.

ISO/IEC 17799:2005 [8]

1. **Saugumo politika**
    1. Informacijos apsaugos politika
        i. (1) Informacijos apsaugos politikos dokumentas (patvirtintas organizacijos vadovybės politikos dokumentas, su kuriuo supažindinami visi darbuotojai)
        ii. (2) Informacijos apsaugos politikos peržiūra (dokumentas peržiūrimas periodiškai arba atsiradus didesniems pokyčiams organizacijoje ar aplinkoje)
2. **Informacijos apsaugos organizavimas**
    1. Vidinis organizavimas
        i. (3) Vadovybės įsipareigojimai informacijos apsaugai (vadovybė užtikrina saugumą organizacijoje, demonstruodama palaikymą, bei numatydama atsakomybes)
        ii. (4) Informacijos apsaugos koordinavimas (informacijos apsaugos veiksmai turi būti koordinuojami, dalyvaujant atstovams iš skirtingų organizacijos skyrių)
        iii. (5) Informacijos apsaugos atsakomybių priskyrimas (visos atsakomybės, užtikrinant informacijos apsaugą, turi būti aiškiai apibrėžtos)
        iv. (6) Informacijos apdorojimo priemonių autorizavimo procesas (valdomas informacijos apdorojimo priemonių autorizavimo procesas turi būti nustatytas ir įgyvendintas)
        v. (7) Konfidencialumo reikalavimai (turėtų būti nustatyti ir reguliariai peržiūrimi konfidencialumo reikalavimai, atspindintys organizacijos poreikius)
        vi. (8) Kontaktai su informacijos apsaugos priežiūros institucijomis (turi būti palaikomi ryšiai su atitinkamomis priežiūros institucijomis)
        vii. (9) Kontaktai su specialistais (turi būti palaikomi ryšiai su informacijos apsaugos specialistais)
        viii. (10) Nepriklausomas informacijos apsaugos auditas (organizacijos informacijos apsaugos būklė turį būti reguliariai peržiūrima nepriklausomų ekspertų)
    2. Saugumas, susijęs su trečiosiomis šalimis

i. (11) Rizikų, susijusių su trečiosiomis šalimis, identifikavimas (prieš suteikiant prieigą trečiosioms šalims, turi būti įvertintos rizikos ir priimtos atitinkamos priemonės)
ii. (12) Saugumo aspektai dirbant su klientais (turi būti įvertinti visi saugumo reikalavimai, prieš suteikiant klientams prieigą prie organizacijos informacijos ar vertybių)
iii. (13) Saugumo reikalavimai sutartyse su trečiosiomis šalimis (sutartyse su trečiosiomis šalimis turi būti įtraukti visi reikalingi saugumo reikalavimai)

3. Vertybių valdymas

1. Atsakomybė už vertybes
   i. (14) Vertybių inventorizacija (visos organizacijos vertybės turi būti inventorizuotos)
   ii. (15) Vertybių savininkai (visos organizacijos vertybės turi turėti savininką)
   iii. (16) Tinkamas vertybių naudojimas (turi būti nustatytos, dokumentuotos ir įgyvendintos tinkamo vertybių naudojimo taisyklės)
2. Informacijos klasifikavimas
   i. (17) Klasifikavimo gairės (informacija turi būti klasifikuojama jos vertės, teisinių reikalavimų, svarbumo bei kritiškumo organizacijai aspektais)
   ii. (18) Informacijos žymėjimas ir naudojimas (atsižvelgiant į organizacijos priimtą informacijos klasifikavimo schemą, turi būti parengtos ir įgyvendintos informacijos žymėjimo ir naudojimo procedūros)

4. Personalo saugumo aspektai

1. Iki įdarbinant
   i. (19) Vaidmenys ir atsakomybės (atsižvelgiant į organizacijos saugumo politiką, turi būti nustatyti ir apibrėžti su informacijos apsauga susiję darbuotojų vaidmenys ir atsakomybės)
   ii. (20) Patikrinimas (turi būti atliekamas darbuotojų, rangovų, ar trečiųjų šalių pateiktų faktų, biografijos patikrinimas, atitinkantis teisinių aktų ir etikos reikalavimus)
   iii. (21) Terminai ir sąvokos darbo sutartyse (darbuotojai, rangovai ar trečiosios šalys turi pasirašyti sutartis, kuriose numatyta jų atsakomybė, susijusi su informacijos apsauga)
2. Įdarbinus

i. (22) Vadovybinė atsakomybė (organizacijos vadovybė turi užtikrinti, kad darbuotojai, rangovai ar trečios šalys laikytųsi saugumo reikalavimų, atsižvelgiant į organizacijos politiką ir atitinkamas procedūras)
ii. (23) Informacijos apsaugos švietimas ir mokymas (visi organizacijos darbuotojai turi būti mokomi ir šviečiami informacijos apsaugos klausimais, atsižvelgiant į jų atliekamas funkcijas)
iii. (24) Disciplinarinis procesas (turėtu būti numatytas formalus disciplinarinis procesas darbuotojams, pažeidusiems saugumo reikalavimus)

3. Sutarties nutraukimas/pakeitimas
   i. (25) Atsakomybės, nutraukiant darbo sutartį (turi būti aiškiai apibrėžtos ir priskirtos atsakomybės, nutraukiant darbo sutartį)
   ii. (26) Vertybių gražinimas (visi darbuotojai, rangovai ar trečios šalys privalo gražinti organizacijai informacines vertybes iki nutraukiant sutartį)
   iii. (27) Prieigos teisių panaikinimas (darbuotojams, rangovams ar trečiosioms šalims suteiktos prieigos teisės turi būti panaikintos iki nutraukiant sutartį)

5. Fizinis ir aplinkos saugumas

1. Saugios zonos
   i. (28) Fizinė perimetro apsauga (turi būti užtikrinama zonų, kuriose randasi informacija ar jos apdorojimo priemonės, perimetro fizinė apsauga)
   ii. (29) Fizinė praėjimo kontrolė (saugiose zonose turi būti numatyta atitinkama praėjimo kontrolė , siekiant užtikrinti praėjimą tiktai autorizuotam personalui)
   iii. (30) Biurų, kabinetų ir informacijos apdorojimo priemonių apsauga (turi būti numatytos *fizinės* patalpų ir įrangos apsaugos priemonės)
   iv. (40) Fizinė apsauga nuo išorinių ir aplinkos grėsmių (turi būti numatyta fizinė apsauga nuo išorinių ir aplinkos grėsmių, tokių kaip gaisrai, užliejimas vandeniu ir kt.)
   v. (50) Darbas saugiose zonose (turi būti numatyta darbo tvarka saugiose zonose)
   vi. (60) Viešos prieigos, pristatymo ir iškrovimo zonos (viešos prieigos, pakrovimo ir iškrovimo zonos, t.y. zonos, į kurias patenka neautorizuoti asmenys, turi būti kontroliuojamos ir, jei tai įmanoma, izoliuotos nuo informacijos apdorojimo įrengimų)
2. Informacijos apdorojimo įrangos apsauga
   i. (61) Saugus įrangos išdėstymas (planuojant įrangos išdėstymą, pastatymo vietas turi būti numatyta jos apsauga nuo aplinkos grėsmių ir nuo neautorizuotos prieigos)

ii. (62) Palaikymas (turi būti numatytos apsaugos priemonės, apsaugančios nuo elektros tiekimo sutrikimų, kondicionavimo sutrikimų, kitų informacijos apdorojimo priemonių veiklą palaikančių funkcijų sutrikimų)

iii. (63) Elektros ir duomenų perdavimo linijų apsauga (elektros ir duomenų perdavimo linijos, kabeliai turį būti apsaugoti nuo pažeidimų)

iv. (64) Įrangos priežiūra (įranga turi būti atitinkamai prižiūrima, užtikrinant jos prieinamumą ir vientisumą)

v. (65) Įrangos už organizacijos ribų apsauga (turi būti įvertintos rizikos ir užtikrinta įrangos, esančios už organizacijos ribų, apsauga)

vi. (66) Saugus įrangos utilizavimas ir pakartotinis panaudojimas (visa įranga, turinti galimybę saugoti informaciją, turi būti patikrinama prieš utilizuojant ar pakartotinai panaudojant)

vii. (67) Nuosavybės apsauga (negalimas neautorizuotas įrangos ar informacijos patekimas už organizacijos ribų)

6. Ryšiai ir operacijų valdymas

1. Veiklos procedūros ir atsakomybės

i. (68) Dokumentuotos veiklos procedūros (veiklos procedūros turi būti dokumentuotos, prižiūrimos ir prieinamos vartotojams, kuriems jos reikalingos)

ii. (69) Pokyčių valdymas (turi būti valdomi informacijos apdorojimo priemonių ir sistemų pokyčiai)

iii. (70) Pareigų atskyrimas (pareigos ir atsakomybių ribos organizacijoje turi būti atskirtos)

iv. (71) Kūrimo, testavimo ir veiklos aplinkų atskyrimas (turi būti numatytas šių aplinkų atskyrimas, siekiant apsaugoti nuo neautorizuotos prieigos prie sistemos ar jos pakeitimo)

2. Trečiųjų šalių paslaugų teikimo valdymas

i. (72) Paslaugų teikimas (turi būti užtikrinta, kad trečiosios šalys, teikiančios paslaugas, laikytųsi sutartyje apibrėžtų paslaugų lygio ir saugumo priemonių)

ii. (73) Trečiųjų šalių teikiamų paslaugų stebėjimas ir peržiūra (turi būti atliekamas teikiamų paslaugų stebėjimas ir kontrolė)

iii. (74) Trečiųjų šalių teikiamų paslaugų keitimų valdymas (turi būti atliekamas teikiamų paslaugų pokyčių stebėjimas ir kontrolė)

3. Sistemų planavimas ir priėmimas

i. (75) Pajėgumų valdymas (turi būti stebimas resursų panaudojimas, ir atliekamas pajėgumų planavimas, siekiant užtikrinti reikalaujamą sistemos našumą)

ii. (76) Sistemų priėmimas (turi būti numatyti naujų sistemų, atnaujinamų sistemų priėmimo naudojimui kriterijai)

4. Apsauga nuo kenksmingos programinės įrangos ir mobilaus kodo
   i. (77) Apsauga nuo kenksmingos programinės įrangos (turi būti įgyvendintos stebėjimo, prevencijos ir atstatymo priemonės apsaugai nuo kenksmingos programinės įrangos, taip pat turi būti numatytas vartotojų švietimas)
   ii. (78) Apsauga nuo mobilaus kodo, angl. - mobile code (turi būti užtikrinama, kad mobilaus kodo naudojimas būtų autorizuotas ir atitiktų saugumo politiką. Mobilaus kodo pavyzdžiai - JavaScript, VBScript, Java appletai, ActiveX priemonės)
5. Atsarginės kopijos
   i. (79) Informacijos atsarginės kopijos (turi būti reguliariai daromos informacijos kopijos, ir išbandomas atstatymas atsižvelgiant į patvirtintą atsarginių kopijų darymo politiką)
6. Tinklo saugumo valdymas
   i. (80) Tinklo valdymas (organizacijos tinklas turi būti valdomas tam, kad būtų užtikrinta apsauga nuo grėsmių, užtikrintas sistemų ir informacijos tinkle saugumas)
   ii. (81) Tinklo paslaugų (servisų) apsauga (turi būti nustatyti saugumo reikalavimai, paslaugų lygiai ir valdymo reikalavimai visoms tinklo paslaugoms)
7. Laikmenų naudojimas
   i. (82) Pernešamų informacijos laikmenų valdymas (turi būti parengtos pernešamų laikmenų valdymo procedūros)
   ii. (83) Laikmenų utilizavimas (informacijos laikmenos turi būti saugiai utilizuojamos, laikantis formalių procedūrų)
   iii. (84) Informacijos naudojimo procedūros (turi būti parengtos informacijos naudojimo ir saugojimo procedūros)
   iv. (85) Sisteminės dokumentacijos apsauga (sisteminė dokumentacija turi būti apsaugota nuo neautorizuotos prieigos)
8. Informacijos apsikeitimas
   i. (86) Informacijos apsikeitimo politika ir procedūros (siekiant užtikrinti informacijos apsikeitimo apsaugą, turi būti parengtos formalios politikos procedūros ir priemonės)

ii. (87) Informacijos apsikeitimo sutartys (informacijos apsikeitimas tarp organizacijos ir kitų šalių turi būti reglamentuotas sutartyse)

iii. (88) Fizinė laikmenų apsauga (transportuojant informacijos laikmenas už organizacijos ribų, turi būti užtikrinta laikmenų apsauga nuo neautorizuotos prieigos ar praradimo)

iv. (89) Elektroninis susirašinėjimas (informacija, perduodama elektroninio susirašinėjimo metu, turi būti tinkamai apsaugota)

v. (90) Biznio/biuro informacinės sistemos (turi būti numatytos politikos ir procedūros, siekiant apsaugoti biznio/biuro informacinėse sistemose esančią informaciją)

9. Elektroninės komercijos paslaugos

i. (91) Elektroninė komercija (elektroninės komercijos informacija, perduodama viešaisiais tinklais, turi būti apsaugota nuo jai kylančių grėsmių)

ii. (92) Elektroniniai mokėjimai (elektroninių mokėjimų informacija turi būti apsaugota nuo jai kylančių grėsmių)

iii. (93) Viešai prieinama informacija (turi būti užtikrinta viešai prieinamos informacijos vientisumo apsauga)

10. Stebėjimas

i. (94) Žurnaliniai įrašai (turi būti pildomi ir nustatytą laiko tarpą saugomi žurnaliniai įrašai apie vartotojų veiksmus ir saugumo įvykius)

ii. (95) Sistemų naudojimas (turi būti parengtos procedūros, leidžiančios registruoti informacijos apdorojimo priemonių panaudojimą)

iii. (96) Žurnalinių įrašų apsauga (žurnaliniai įrašai turi būti apsaugoti nuo neautorizuotos prieigos ir pakeitimo)

iv. (97) Administratorių ir operatorių veiksmų žurnaliniai įrašai (sistemų administratorių ir operatorių veiksmai turi būti registruojami)

v. (98) Gedimų registravimas (gedimai turi būti registruojami, analizuojami ir priimamos atitinkamos priemonės)

vi. (99) Laiko sinchronizavimas (laikas visose organizacijos informacijos apdorojimo priemonėse turi būti sinchronizuotas)

7. Prieigos valdymas

1. Veiklos reikalavimai prieigos valdymui

i. (100) Prieigos valdymo politika

2. Vartotojo prieigos valdymas

i. (101) Vartotojo registravimas

ii. (102) Teisių valdymas
iii. (103) Vartotojo slaptažodžio valdymas
iv. (104) Vartotojo teisių peržiūra

3. Vartotojo atsakomybės
   i. (105) Slaptažodžio naudojimas
   ii. (106) Įranga palikta be priežiūros
   iii. (107) Švaraus stalo ir švaraus ekrano politika
4. Tinklo prieigos valdymas
   i. (108) Tinklo paslaugų (servisų) naudojimo politika
   ii. (109) Vartotojo autentifikavimas išoriniams prisijungimams
   iii. (110) Įrangos tinkle identifikavimas
   iv. (111) Nuotolinių priežiūros ir administravimo prieigų apsauga
   v. (112) Tinklų atskyrimas
   vi. (113) Tinklų sujungimo valdymas
   vii. (114) Tinklų maršrutizavimo valdymas
5. Prieigos prie operacinės sistemos valdymas
   i. (115) Saugi įsiregistravimo procedūra
   ii. (116) Vartotojo identifikavimas ir autentifikavimas
   iii. (117) Slaptažodžių valdymo sistema
   iv. (118) Sisteminių programinių priemonių naudojimas
   v. (119) Sesijos time-out‘as
   vi. (120) Sujungimo laiko apribojimas
6. Prieigos prie aplikacijų ir informacijos valdymas
   i. (121) Prieigos prie informacijos ribojimas
   ii. (122)Svarbių sistemų izoliavimas
7. Mobilūs įtaisai ir nuotolinis darbas
   i. (123) Mobilūs įtaisai ir komunikacijos
   ii. (124) Nuotolinis darbas

8. Informacinių sistemų įsigijimas, kūrimas ir priežiūra

1. Saugumo reikalavimai informacinėms sistemoms
   i. (125) Saugumo reikalavimų analizė ir specifikavimas
2. Tikslus programinės įrangos duomenų apdorojimas
   i. (126) Įvedamų duomenų tikrinimas
   ii. (127) Vidinio duomenų apdorojimo kontrolė
   iii. (128) Duomenų vientisumas

iv. (129) Rezultato sutikrinimas

3. Kriptografinės priemonės
    i. (130) Kriptografinių priemonių naudojimo politika
    ii. (131) Raktų valdymas
4. Sisteminių bylų apsauga
    i. Operacinės programinės įrangos kontrolė
    ii. Sistemos testavimo duomenų apsauga
    iii. Prieigos prie programinio kodo valdymas
5. Apsauga kūrimo ir palaikymo procese
    i. Pokyčių valdymo procedūra
    ii. Techninė sistemų peržiūra pakeitus operacinę sistemą
    iii. Programinės įrangos paketų keitimo ribojimai
    iv. Informacijos nutekėjimas
    v. Trečioms šalims perduotos programinės įrangos (outsourced) kūrimas
6. Techninių pažeidžiamumų valdymas
    i. Techninių pažeidžiamumų valdymas

Šį standartą galimą įsigyti Lietuvos standartizacijos departamente arba kitose platinimo vietose. Reikėtų pažymėti, kad daugelis standarte naudojamų priemonių nėra labai išsamiai detalizuojamos, todėl, įgyvendinant pagal ši standartą parinktas priemonės, rekomenduojama naudotis ir detalesniais, techniniais atskirų sričių standartais ar metodikomis, kaip pavyzdžiui IT saugumo „techninis“ standartas ISO/IEC 13335.