RIZIKOS ANALIZĖS VADOVAS

FINANSUOTA ES PHARE PROGRAMOS IR LIETUVOS RESPUBLIKOS LĖŠOMIS

vaga

RIZIKOS

ANALIZĖS VADOVAS

ADMINISTRACINIŲ IR TECHNINIŲ GEBĖJIMŲ STIPRINIMAS UŽTIKRINANT DUOMENŲ, INFORMACINIŲ TECHNOLOGIJŲ IR JOMIS PERDUODAMŲ DUOMENŲ APSAUGĄ

UDK 65.011
Va42

Šis leidinys sukurtas ir atspausdintas
ES Phare programos lėšomis.

Creation and publishing of this manual
was paid by EU Phare programme.

ISBN 5-415-01827-1

Turinys

ĮVADAS

Rizikos analizės vadovas parengtas įgyvendinant PHARE programos projektą „Administracinių ir techninių gebėjimų stiprinimas užtikrinant duomenų, informacinių technologijų ir jomis perduodamų duomenų apsaugą“. Vadovas padės analizuoti nurodytas rizikos grupes:

- Saugos priemonių diegimo riziką;
- Asmens saugumo riziką;
- Fizinę ir aplinkosaugos riziką;
- Ryšių, sujungimų ir veiklos riziką;
- Sistemos plėtros ir jos palaikymo riziką.

Rizikos analizės vadovas turi būti naudojamas valstybinėse institucijose, valdančiose IT išteklius ir dirbančiose su įvairios svarbos elektroniniais duomenimis. Taip pat reikės atsižvelgti į tai, kad informacijos sauga ir rizikos analizė daugeliui institucijų yra palyginti nauji procesai. Tad tikėtina, kad rizikos analizę vykdys darbuotojai, kurių žinios šioje sferoje ribotos.

Efektyviam rizikos valdymui užtikrinti būtina taikyti nuolatinės rizikos analizės metodą. Rizikos analizė turi atitikti aplinkos pobūdį (įvertinti, ar nagrinėjama organizacija, ar jos dalis, ar jos techninės sistemos, ar konkrečių duomenų saugumas), taip pat leisti priimti efektyvius sprendimus, kurie sumažintų nepriimtiną riziką iki leistino lygio.

Informacijos sistemų turtas (vertybės) [20, p. 8, sk. 5.1.1]:

a) informacija: duomenų bazės ir duomenų rinkmenos, sistemos dokumentai, vartotojo vadovai, mokymo medžiaga, naudojimo arba palaikymo procedūros, veiklos tęstinumo planai, kopijavimo priemonės, archyvo informacija;

b) programinė įranga: taikomoji programinė įranga, sistemos programinė įranga, plėtros priemonės ir paslaugų programos;

c) fizinė įranga: kompiuterio įranga (procesoriai, monitoriai, nešiojamieji kompiuteriai, modemai), ryšių įranga (maršrutizatorius, privatūs automatiniai linijų komutatoriai, fakso aparatai, automatiniai atsakikliai), magnetinės duomenų laikmenos (juostos ir diskai), kita techninė įranga (maitinimo šaltiniai, oro kondicionavimo įtaisai), baldai, patalpos;

d) paslaugos: skaičiavimo ir ryšių paslaugos, bendrosios komunalinės paslaugos, pavyzdžiui, šildymas, apšvietimas, elektros tiekimas, oro kondicionavimas.

Toliau nurodytos sąvokos pateiktos ISO vadove 72 [11]:

Nenumatyta prieiga – techninė prieiga yra programavimo elementai, leidžiantys taikomųjų programų specialistams naudotis jomis, apeinant įprastines apsaugos procedūras ir priemones. Nors ši funkcija labai naudinga programos palaikymui ir prie-

žiūrai, saugos specialistai turi atsižvelgti į nenumatytas prieigas ir pritaikyti jų vartotojams tinkamas kontrolės ir atskaitomybės priemones.

Įvykis – konkrečių aplinkybių derinys.

1 pastaba. Įvykis gali būti neabejotinas arba abejotinas. 2 pastaba. Įvykis gali būti vienetinis arba jų seka. 3 pastaba. Įvykio **tikimybė** gali būti skaičiuojama konkrečiam laikotarpiui.

Informavimas apie riziką – apsikeitimas arba pasidalijimas informacija apie **riziką** tarp asmens, priimančio sprendimus, ir rizikos **subjektų**.

Pastaba. Informacija gali būti susijusi su konkrečios rizikos egzistavimu, pobūdžiu, forma, tikimybe, reikšmingumu, priimtinumu, kontrole ar kitais jos aspektais.

Pasekmė – **įvykio** rezultatas.

1 pastaba. Įvykio pasekmės gali būti kelios. 2 pastaba. Pasekmės gali būti teigiamos ir neigiamos, tačiau saugos požiūriu pasekmės visada yra neigiamos. 3 pastaba. Pasekmės gali būti išreiškiamos kokybiškai arba kiekybiškai.

Rizika – įvykio tikimybė ir jo **pasekmių** derinys.

1 pastaba. Terminas „rizika“ paprastai vartojamas tik tada, kai yra bent jau neigiamų pasekmių tikimybė.

2 pastaba. Kai kuriais atvejais rizika kyla dėl nukrypimo laukiamo rezultato arba įvykio tikimybės.

Rizikos analizė – sisteminis informacijos panaudojimas, siekiant nustatyti **šaltinius** ir įvertinti **riziką.**

1 pastaba. Rizikos analizė sukuria pagrindą **rizikos vertinimui**, **rizikos valdymui** ir **rizikos priėmimui.**

2 pastaba. Informacija apima faktinius duomenis, teorinę analizę, autoritetingas nuomones ir **subjektų** interesus.

Rizikos vertinimas – procesas, kurio metu **rizikos tikimybė** ir **pasekmės** išreiškiamos konkrečia verte.

Pastaba. Rizikai vertinti gali būti pasitelkiami kaštai, nauda, **subjektų** interesai ir kiti kintamieji, atitinkantys **rizikos vertinimo** metodą.

Rizikos išlaikymas – susitaikymas su konkrečios **rizikos** sąlygojamais nuostoliais arba nauda.

1 pastaba. Rizikos išlaikymas apima neidentifikuotos rizikos priėmimą. 2 pastaba. Į rizikos išlaikymą neįeina tokios kontrolės priemonės, kaip draudimas arba rizikos perdavimas kitais būdais. 3 pastaba. Rizikos priėmimo laipsnis gali kisti priklausomai nuo **rizikos kriterijų**.

Rizikos vengimas – sprendimas nedalyvauti ar pasitraukti iš rizikingos situacijos.

Pastaba. Sprendimas gali būti priimtas, remiantis **rizikos įvertinimo** rezultatais.

Rizikos įvertinimas – procesas, kurio metu apskaičiuota **rizika** įvertinama pagal **rizikos kriterijus**, siekiant nustatyti rizikos reikšmingumą.

Pastaba. Rizika įvertinama siekiant priimti sprendimą dėl rizikos kontrolės

Rizikos kriterijai – veiksniai, įvertinantys **rizikos** reikšmingumą.

Pastaba. Rizikos kriterijai gali apimti susijusius su rizika kaštus ir naudą, teisinius ir norminius reikalavimus, socialinius-ekonominius ir aplinkos aspektus, **subjektų** interesus, prioritetus ir kitą informaciją.

Rizikos optimizacija – su **rizikos kontrole** susijęs procesas, kuriuo siekiama sumažinti neigiamų pasekmių **tikimybę** ir padidinti teigiamų pasekmių atsiradimo **tikimybę.**

Pastaba. Rizikos optimizacija priklauso nuo rizikos kriterijų, įskaitant kaštus ir teisinius reikalavimus.

Rizikos perdavimas – konkrečios **rizikos** sąlygojamų nuostolių naštos arba naudos pasidalijimas su kita šalimi.

1 pastaba. Teisiniai ir norminiai reikalavimai gali apriboti, uždrausti arba priversti perduoti konkrečią riziką. 2 pastaba. Rizikos perdavimas galimas apdraudžiant arba kitokiais susitarimais. 3 pastaba. Rizikos perdavimas gali sukurti naują riziką arba pakeisti egzistuojančią. 4 pastaba. **Šaltinio** perkėlimas nėra rizikos perdavimas.

Rizikos priėmimas – sprendimas prisiimti **riziką.**

Pastaba. Rizikos priimtinumas priklauso nuo **rizikos kriterijų.**

Rizikos tvarkymas – procesas, kurio metu pasirenkamos ir įdiegiamos priemonės, keičiančios **rizikos** tikimybę.

Pastaba. Rizikos kontrolės priemonės gali būti rizikos vengimas, optimizacija, rizikos perdavimas ir išlaikymas.

Rizikos valdymas – koordinuoti veiksmai, kuriais siekiama valdyti ir kontroliuoti organizacijos **rizikas**. Paprastai rizikos valdymas apima **rizikos analizę, rizikos priežiūrą**, **rizikos priėmimą** ir **informavimą apie riziką**.

Rizikos vertinimas – bendras **rizikos analizės** ir **rizikos įvertinimo** procesas.

Subjektas – asmuo, grupė arba organizacija, galinti patirti **riziką**, būti jos paveikta arba mananti, kad gali būti jos paveikta.

1 pastaba. Asmuo, priimantis sprendimus, taip pat yra ir subjektas. 2 pastaba. **Subjekto** terminas apima **suinteresuotąsias šalis** (apibrėžtas ISO 9000:2000), bet aiškinamas plačiau.

Suinteresuotoji šalis – asmuo arba grupė, suinteresuota organizacijos veikla arba jos sėkmingumu. Pvz., klientai, savininkai, organizacijoje dirbantys asmenys, tiekėjai, bankininkai, sąjungos, partneriai arba visuomenė.

Šaltinio nustatymas – procesas, kurio metu nustatomi, fiksuojami ir atpažįstami **šaltiniai**.

Šaltinis – elementas arba veiksmas, potencialiai galintis turėti **pasekmių.**

Pastaba. Saugos kontekste šaltinis yra pavojus.

Tikimybė – **įvykio** tikimumo laipsnis.

1 pastaba. ISO 3534-1:1993 apibrėžimas 1.1 pateikia matematinę tikimybę kaip „realų skaičių nuo 0 iki 1, priskiriamą retam įvykiui. Jis gali būti priskiriamas pagal santykinį įvykio dažnumą per ilgą laikotarpį arba pagal tikimumo laipsnį, kad tai įvyks. Esant dideliam tikimumo laipsniui, tikimybė artima 1“. 2 pastaba. Apibūdinant **riziką**, gali būti vartojamas ne tikimybės, o dažnumo terminas. 3 pastaba. Įvykio tikimumo laipsnis gali būti nurodomas kaip klasė arba lygis, pvz., retas / mažai tikėtinas / vidutinio tikimumo / tikėtinas / beveik neabejotinas arba neįmanomas / mažai tikėtinas / retas / pasitaikantis / tikėtinas / dažnas.

1. Rizikos analizės problema

Sėkminga rizikos analizė priklauso nuo daugelio įvairių veiksnių. Tai aiškiai apibrėžta apimtis, galiojantys dokumentai, nešališkumas, rizikos analizės proceso brandumas, informacijos ir duomenų saugos užtikrinimo metodai bei organizavimas, rizikos analizėje dalyvaujančių darbuotojų kompetencija, patirtis ir jų vaidmuo organizacijoje.

Rizikos analizė yra privalomas procesas kiekvienai organizacijai, siekiančiai valdomosios saugos. Tačiau saugos valdymo procesas turi būti nukreiptas į kritinę reikšmę turinčius veiksnius, kurių nepaisant iškyla didelė nesėkmės tikimybė [20, p.ix].

Rizikos analizės privalomo proceso savybės:

a) saugos politika, uždaviniai ir veiksmai turi atspindėti organizacijos uždavinius;
b) diegiamos saugos priemonės turi atitikti organizacijos kultūrą;
c) būtina akivaizdi vadovybės parama ir dėmesys;
d) būtinas geras saugos reikalavimų, rizikos analizės ir rizikos valdymo supratimas;
e) būtinas efektyvus saugos reikšmės išaiškinimas visiems vadovams ir darbuotojams;
f) informacija apie informacijos saugos politiką ir standartus turi būti išplatinta visiems darbuotojams ir rangovams;
g) būtina užtikrinti reikalingą švietimą ir mokymus;

h) būtina visapusė ir gerai subalansuota vertinimo sistema, kuria būtų galima įvertinti informacijos saugos valdymo funkcionavimą ir priimti atsakomuosius pasiūlymus dėl jo tobulinimo.

Be to, prieš pradedant rizikos analizę, būtina įvertinti pačios organizacijos brandumą. Organizacijos brandumas – tai įgūdžių visuma, leidžianti efektyviai įgyvendinti procesus. Organizacijos brandumo modelio tikslas nustatyti organizacijos pajėgumą įgyvendinti procesus, planuoti tų procesų tobulinimo būdus ir taikyti procesų įgyvendinimo priemones, atitinkančias jos brandumo lygį. Brandumo modelis 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 uždavinys buvo užtikrinti sistemingą požiūrį į programinės įrangos kūrimo procesų tobulinimą. Tačiau dėl modelio paprastumo ir jo patogumo nustatant organizacijos brandumą, jį pradėjo taikyti daugelis kitų organizacijų (pvz., CobIT IT valdymo metodologija). Jis išaiškino, kodėl vienoje organizacijoje veiksminga procedūra, kitoje pasirodo visiškai neefektyvi ar net kenksminga. Atsakymas slypi pačioje formuluotėje – atitinkamos priemonės atitinkamai aplinkai. Problemos neišvengiamos, jeigu nebrandi organizacija mėgins įdiegti arba pritaikyti procesus ar technines priemones, taikytinas tik labai brandžioms organizacijoms. Pavyzdžiui, diegiant sudėtingą procesą arba technologiją nesubrendusioje aplinkoje, ypač didelė rizika, kad įdiegimas nepavyks. Brandumo modelis apima penkis lygius [5, p. 21], [6], [22, p.31]:

0. Nesantis. Visiškas bet kokių procesų nebuvimas. Organizacija net nesuvokia, kad egzistuoja problema, kurią reikia spręsti. Politika (arba procesai) nėra aprašyti, ir anksčiau orga-

nizacija nesuvokė veiklos rizikos, susijusios su tokiu rizikos valdymu. Todėl problema nebuvo svarstoma. Procesų ir veiklos sprendimų rizikos analizė neatliekama. Organizacija neįvertino saugos pažeidimų rizikų poveikio veiklai. Rizikos valdymas nebuvo identifikuotas kaip IT sprendimų įsigijimo ir IT paslaugų tiekimo sudėtinė dalis.

1. **Pradinis.** Organizacija pripažino, kad problema egzistuoja ir ją reikia spręsti. Tačiau nėra standartizuotų procesų, yra tik *ad hoc* (specialūs) sprendimai, taikomi tam tikriems asmenims arba tam tikrais atvejais. Bendras požiūris į rizikos valdymą dezorganizuotas. Akivaizdu, kad kai kurie organizacijos nariai jau pripažino rizikos valdymo naudą. Tačiau rizikos valdymas atliekamas *ad hoc* principu. Nėra nei formaliai aprašytos politikos, nei procesų, procesai įgyvendinami nenuosekliai. Apskritai rizikos valdymo projektai atrodo chaotiški ir nekoordinuojami, o rezultatai nei įvertinami, nei audituojami. Organizacija suvokia savo teisinius ir sutartinius įsipareigojimus, bet tvarko IT riziką *ad hoc* principu, neturėdama įvardytos politikos ir procesų. Neformali projekto rizikos analizė atliekama kiekvienam projektui atskirai ir kiekvieną kartą savaip. Rizikos analizė nėra išskiriama projekto plane ir nėra pavedama konkretiems projekte dalyvaujantiems vadovams. IT vadovybė nenurodo atsakomybės už rizikos valdymą pareiginiais nuostatais ir išsamiau neaiškina jos kitokiais būdais. Specifinė IT rizika, tokia kaip slaptumas, prieinamumas ir vientisumas, kartais analizuojama kiekvieno konkretaus projekto atveju. IT rizika, veikianti kasdienes darbines operacijas, kartais aptariama vadovybės susirinkimuose, bet rizikos prevencijos priemonės nenuoseklios.

2. Kartotinis. Procesai išplėtoti tokiu lygiu, kad skirtingi žmonės, atliekantys identiškas užduotis, laikosi panašių procedūrų. Formalūs mokymai ir informavimas apie standartines procedūras nėra organizuojami, o atsakomybė paliekama kiekvienam asmeniui atskirai. Kai kurių asmenų žiniomis labai pasitikima, todėl galimos klaidos. Rizikos valdymas suvokiamas visos organizacijos mastu. Rizikos valdymo procesas kartotinis, bet nebrandus. Procesas visiškai neaprašytas, 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 nevykdomi, atsakomybė už jų įgyvendinimą paliekama tam tikriems darbuotojams. 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 aukščiausiu organizaciniu lygiu 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, formaliai sisteminančių rizikos valdymą.

3 Apibrėžtas. Procedūros yra standartizuotos ir aprašytos, o darbuotojai supažindinti su jomis mokymų metu. Tačiau šių procedūrų laikymasis paliktas darbuotojų nuožiūrai, ir nukrypimų fiksavimas mažai tikėtinas. Pačios procedūros nėra išplėtotos, jos tiesiog formalizuoja esančią praktiką. Organizacija priėmusi formalų sprendimą im-

tis rizikos valdymo ir įgyvendinti savo informacijos saugos programą. Pamatiniai procesai sukurti, jie turi aiškiai apibrėžtus tikslus, taip pat apima procedūras, leidžiančias juos pasiekti ir įvertinti procesų sėkmingumą. Be to, tam tikri rudimentiniai rizikos valdymo mokymai rengiami visam personalui. Pagaliau organizacija aktyviai įgyvendina formaliai aprašytus rizikos valdymo procesus. Rizikos valdymo politika, taikoma visai organizacijai, nustato, kada ir kaip reikia atlikti rizikos analizę. Rizikos analizė vykdoma, laikantis nustatytų procedūrų, kurios yra aprašytos 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 nustatyti. Procedūrinių reikalavimų laikymasis paliktas atskiro IT vadovo nuožiūrai, nėra procedūros, užtikrinančios, kad rizikos analizė bus atliekama kiekvieno projekto atveju, ir kad jau vykdomos operacijos bus reguliariai įvertinamos rizikos požiūriu.

4 Valdomas. Galima prižiūrėti ir kontroliuoti procedūrų laikymąsi, taip pat imtis veiksmų, paaiškėjus, kad procesas nėra pakankamai efektyvus. Procesai nuolat tobulinami, atsižvelgiant į pasiteisinusią praktiką. Automatizacija ir techninės priemonės naudojami ribotai arba fragmentiškai. Visuose organizacijos lygiuose egzistuoja išsamus rizikos valdymo supratimas. Rizikos valdymo procedūros sukurtos, procesas yra aiškiai apibrėžtas, plačiai skatinamas sąmoningumas, rengiami privalomi mokymai, taip pat egzistuoja kai kurios pradinės priemonės, leidžiančios

įvertinti sėkmingumą. Rizikos valdymo programai skirti pakankami ištekliai, daugelis organizacijos padalinių jau patyrė jos naudingumą, o saugos rizikos valdymo grupė pajėgi nuolat tobulinti procesus ir priemones. Naudojamos kai kurios technologinės rizikos valdymo priemonės, tačiau dauguma, jei ne visos rizikos analizės, kontrolės, identifikavimo ir kaštų-naudos analizės procedūros atliekamos rankiniu būdu. Rizikos analizė yra standartinė procedūra, ir jos nesilaikymo atvejus gali pastebėti IT vadovybė. Tikėtina, kad IT rizikos valdymas yra formalizuota aukščiausio lygio vadovybės funkcija. Procesas išplėtotas, rizika analizuojama tiek tam tikro projekto lygiu, tiek reguliariai visos IT sistemos požiūriu. Vadovybė informuojama apie IT aplinkos pakyčius, galinčius iš esmės paveikti rizikos scenarijus, tokius kaip padidintas duomenų tinklo pavojus arba techniniai spendimai, darantys įtaką IT strategijos vidinei logikai. Vadovybė pajėgi prižiūrėti rizikos situaciją ir priimti pagrįstus sprendimus dėl rizikos lygio priimtinumo. Aukščiausioji vadovybė ir IT vadovybė yra nustačiusi organizacijos toleruojamą rizikos lygį ir turi standartines priemones rizikos ir rezultatų santykiui įvertinti. Vadovybė skiria biudžetinių lėšų operacinės rizikos analizės projektams, kurie leidžia reguliariai pervertinti riziką. Yra sukurta rizikos valdymo duomenų bazė.

5 Optimizuotas. Procesai ištobulinti iki geriausios praktikos lygio, remiantis nuolatinio tobulinimo rezultatais ir brandumo modeliavimu kartu su kitomis organizacijomis. IT nuosekliai naudojamos darbui automatizuoti, jos teikia kokybės ir efektyvumo gerinimo priemones ir leidžia įmonei greitai prie jų prisitaikyti. Organizacija saugos rizikos

valdymui skiria pakankamai lėšų, o darbuotojai siekia užtikrinti, kad problemos ir jų sprendimai būtų numatomi prieš kelis mėnesius ir metus. Rizikos valdymo procesas gerai įsimintinas ir maksimaliai automatizuotas, pasitelkus atitinkamas priemones (sukurtas pačios organizacijos arba įsigytas iš nepriklausomų programinės įrangos tiekėjų). Nustatoma kiekvieno saugos įvykio pirminė priežastis ir imamasi tinkamų veiksmų, leidžiančių išvengti jo pasikartojimo. Darbuotojams rengiami įvairaus kvalifikacinio lygio mokymai. Rizikos analizė išplėtota tokiu lygiu, kad visos organizacijos mastu yra įgyvendinamas struktūrinis, reguliariai prižiūrimas ir gerai valdomas procesas. Pasitelkus specialistus, kolektyvinis rizikos svarstymas ir pirminių priežasčių analizė atliekami visoje organizacijoje. Rizikos valdymo duomenų fiksavimas, analizavimas ir pranešimas gerai automatizuotas. Specialistai parengę instrukcijas, o IT organizacija dalyvauja patirties keitimosi grupių darbe. Rizikos valdymas realiai integruotas į visą organizacijos veiklą ir IT operacijas, jį pripažįsta ir jame plačiai dalyvauja IT paslaugų vartotojai.

Brandumo lygį lemia trys pagrindiniai veiksniai – žmonių kompetencija, organizacija ir taikomos technologijos. Tik nustačius brandumo lygį, galima identifikuoti tinkamus rizikos analizės metodus [22, p.31]. Kuo žemesnis brandumo lygis, tuo paprastesni rizikos analizės metodai turėtų būti taikomi.

2. Rizikos analizė ir rizikos valdymas

Rizikos valdymo ir rizikos analizės procesai gali atrodyti identiški, tačiau būtina suprasti jų skirtumus ir bendrumus. Rizikos valdymo proceso tikslas sumažinti riziką iki priimtino lygio, tuo tarpu rizikos analizė atliekama tam, kad jos rezultatai būtų panaudoti kaip pagrindas rizikos mažinimo procesams įgyvendinti ir jų veiksmingumui įvertinti, pvz., atsisakant neveiksmingų priemonių, diegiant naujas ir palaikant esamas rizikos valdymo priemones. Rizikos valdymą ir rizikos analizę gerai atspindi tarpusavyje susijusios sąvokos, pateiktos ISO vadove 72 (2.1 pav.).

2.1 pav. Sąvokų sąsajos, remiantis jų apibrėžimais ISO vadove 72 [11, p. 10].

Sprendimas pasirinkti vieną ar kitą rizikos vertinimo arba analizės metodą turi būti grindžiamas tokiais veiksniais:

1. Analizės tikslas;
2. Analizės apimtis;
3. Prieinami organizacijos ištekliai ir analizei skiriamas laikas.

Aptarkime kiekvieną iš šių veiksnių. Kiekvieną rizikos analizę turi lydėti atitinkami sprendimai, kadangi vienintelis bet kokios analizės tikslas yra pagrįsti racionalius sprendimus. Sprendimams, pagrįstiems rizikos analize, priklauso:

- Konkrečių saugos kontrolės priemonių pasirinkimas;
- Konkrečių saugos kontrolės priemonių įdiegimas;
- Duomenų saugai skiriamo finansavimo suma;
- Aplinkos keitimas arba nekeitimas ateityje (organizacinių ir (arba) techninių pokyčių).

Kiekybinė rizikos analizė reikalinga tais atvejais, kai saugos sprendimai daro įtaką finansiniams sprendimams, pvz., biudžetui arba kaštams. Kiekybinės analizės rezultatas yra finansinė išraiška (tokia kaip tikėtinas metinis nuostolis). Vadovybei jos lengvai suprantamos ir todėl sukuria pagrindą finansiniams sprendimams. Vis dėlto, jeigu analizė nėra susijusi su finansinėmis priemonėmis (pvz., analizuojamas klientų pasitenkinimas arba organizacijos reputacija) arba trūksta duomenų apie praeities saugos įvykius, didelė tikimybė, kad kiekybinė analizė nepateisins vilčių ir paralyžiuos sprendimų priėmimą.

Kiekybinė rizikos analizė geriausiai tinka tuomet, kai analizės apimtis apsiriboja viena sistema arba viena verte, ir yra pakankamai duomenų bei ekspertizės išvadų, leidžiančių apskaičiuoti tikimybę ir galimą poveikį. Be abejo, analizuojamos infrastruktū-

ros vertei būtina finansinė išraiška, o analizuojami procesai turi būti susiję su kokiais nors finansiniais srautais, pvz., pajamomis, išlaidomis arba investicijomis.

Jeigu priimami sprendimai susiję su vadinamosios bazinės saugos sukūrimu, pvz., bazinio saugos lygio užtikrinimu visoje organizacijoje arba kompleksinės tinklo infrastruktūros plėtote, kokybinė rizikos analizė gali būti veiksmingesnė.

Rizikos analizės metodas priklauso nuo esamų organizacijos išteklių. Pavyzdžiui, norint atlikti kokybinę rizikos analizę, reikia sukurti rizikos analizės grupę, neapsiribojant vien tik veiklos procesų valdytojais, technikos specialistais ir teisės ekspertais. Nesugebėjus organizuoti efektyviai veikiančios grupės arba nepakankamai suprantant saugos problemas, rizikos analizė gali būti nesėkminga. Esant ribotiems ištekliams, galima rinktis bazinę kokybinę analizę arba sumažinti analizės apimtį iki vieno sistemos elemento, kad būtų išvengta vadinamojo „analizės paralyžiaus“.

Visos pirmiau išdėstytos rekomendacijos apibendrintos 2.1 lentelėje:

2.1 lentelė

RIZIKOS ANALIZĖS METODO PASIRINKIMO MATRICA

	Siauros apimties analizė	**Plačios apimties analizė**
Sprendimai dėl finansavimo/ biudžetinių lėšų skyrimo	Atakos medžio metodas TMN (žr. 44 p.)	TMN (žr. 44 p.) KURAP (žr. 73 p.)
Prioritetų nustatymas/ procedūriniai sprendimai	BS 7799 (žr. 102 p.) KURAP (žr. 73 p.) Atakos medžio metodas	BS 7799 KRA (žr. 60 p.) KURAP (žr. 73 p.)

3. Rizikos analizė – procesas

Pirma, be vadovybės paramos ir palaikymo, saugos rizikos valdymas nebus veiksmingas. Kai saugos rizikos valdymui vadovaujama aukščiausiu lygiu, organizacija gali įvertinti saugą, remdamasi jos reikšmingumu veiklai. Antra, proceso sėkmingumui esminę reikšmę turi aiškus vaidmenų ir atsakomybės apibrėžimas. Veiklos procesų valdytojai atsako už rizikos poveikio nustatymą. Be to, jie geriausiai gali nusakyti operacinėms funkcijoms atlikti reikalingos infrastruktūros naudingumą pagal veiklą. Kiti svarbiausi sėkmės veiksniai yra:

- Tinkamai sudarytas rizikos valdymo subjektų sąrašas;
- Rizikos valdymo organizacijos brandumas;
- Atviro bendravimo atmosfera;
- Komandinio darbo dvasia;
- Kompleksinis organizacijos požiūris į rizikos valdymą;
- Saugos rizikos valdymo grupės autoritetas.

Rizikos analizės procesas paprastai gali būti apibūdintas kaip trijų pakopų procesas:

1. Informacinės infrastruktūros elementų nustatymas ir klasifikacija;
2. Rizikos analizė;
3. Rizikos valdymo priemonių pasirinkimas.

Tas pats principas yra išsamiau išdėstytas tokiuose standartuose kaip ISO 13335 ir ISO 17799.

Saugos rizikos analizavimas

Saugos reikalavimai nustatomi metodiškai analizuojant saugos riziką. Kontrolės priemonių išlaidos turi atitikti veiklos nuostolius, kuriuos galėtų sukelti saugos pažeidimas. Rizikos analizės metodai gali būti taikomi visai organizacijai, taip pat kuriam nors vienam jos padaliniui, informacinei sistemai, specifiniams sistemos komponentams arba paslaugoms, jeigu tai praktiška, realu ir veiksminga [20, p. viii].

Rizikos analizė yra sisteminis šių nurodytų elementų įvertinimas:

a) veiklos nuostoliai, kuriuos galėtų sukelti saugos pažeidimas, atsižvelgiant į potencialias informacijos konfidencialumo ir (arba) kitų vertybių vientisumo ar prieinamumo pažeidimo pasekmes;
b) reali tokio pažeidimo tikimybė, atsižvelgiant į dominuojančias grėsmes ir pažeidžiamumus, taip pat į jau įdiegtas saugos kontrolės priemones.

Tokios analizės rezultatai padės susiorientuoti, apsispręsti dėl tinkamiausių vadovybės veiksmų, nustatyti informacijos saugos rizikos valdymo prioritetus ir įdiegti tinkamas kontrolės priemones, padėsiančias išvengti minėtos rizikos. Rizikos analizės ir kontrolės priemonių pasirinkimo procesą gali tekti kartoti keletą kartų, kad būtų galima įvertinti skirtingus organizacijos padalinius arba konkrečias informacines sistemas.

Labai svarbu periodiškai peržiūrėti įdiegtas saugos rizikos kontrolės priemones, kad būtų galima:

a) įvertinti veiklos poreikių ir prioritetų pasikeitimus;
b) atsižvelgti į naujas grėsmes ir pažeidžiamumus;
c) įsitikinti, ar kontrolės priemonės yra tinkamos ir veiksmingos.

Priklausomai nuo ankstesnių analizių rezultatų, rizikos lygio pasikeitimų ir vadovybės pasirengimo juos priimti, turėtų būti atliekamos skirtingo išsamumo pakartotinės rizikos analizės. Paprastai rizikos analizė vykdoma pradedant aukščiausiuoju vadovų lygiu, siekiant nustatyti prioritetines didžiausios rizikos sritis ir skirti joms atitinkamus išteklius, o vėliau einama prie žemesniųjų vadybos lygių, kad būtų galima išsamiau išanalizuoti specifines grėsmes.

Atnaujinta BS 7799-2:2002 standarto versija apibrėžia informacijos saugos valdymą tomis pačiomis kategorijomis, kaip ir ISO 9000 serijos standartai. Rizikos analizės procesas aptariamas 4.2.1 skyriuje *„Establish the ISMS" (Sukurkite ISVS)**: [1, p. 5]:

. . . . . .

c) *Nustatykite sisteminės rizikos analizės metodą*
Nustatykite rizikos analizės metodą, kuris geriausiai tiktų jūsų ISVS, ir jūsų informacijai taikomus teisinius bei norminius saugos reikalavimus. Kad būtų galima sumažinti riziką iki priimtino lygio, apibrėžkite politiką ir ISVS uždavinius. Nustatykite rizikos priimtinumo kriterijus ir priimtiną rizikos lygį.

d) *Nustatykite riziką*
1) Identifikuokite vertybes, kurios priklausytų ISMS, ir jų valdytojus;

* Informacijos saugos valdymo sistema. (*Aut.*)

2) Nustatykite grėsmes, kylančias šiems elementams;
3) Identifikuokite pažeidžiamumus, kurie gali būti išnaudoti grėsmėms realizuoti;
4) Nustatykite poveikį, kurį turėtų informacijos saugos (konfidencialumo ir (arba) kitų vertybių vientisumo ar prieinamumo) praradimas.

e) *Išanalizuokite riziką*
1) Išanalizuokite nuostolius, kuriuos galėtų patirti jūsų veikla dėl saugos pažeidimo, atsižvelgdami į potencialias informacijos saugos pasekmes.
2) Įvertinkite realaus saugos pažeidimo tikimybę, atsižvelgdami į dominuojančias grėsmes, vertybių pažeidžiamumą ir jų praradimo poveikį, taip pat į jau įdiegtas saugos priemones.
3) Apskaičiuokite rizikos lygius.
4) Remdamiesi „c“ dalyje nustatytais kriterijais, įvertinkite, ar rizika yra priimtino lygio, ar reikia imtis veiksmų jai sumažinti.

f) *Nustatykite ir įvertinkite rizikos tvarkymo alternatyvas*
Galimi veiksmai:
1) įdiegti atitinkamas saugos priemones;
2) sąmoningai ir objektyviai prisiimti riziką su sąlyga, kad jos lygis atitinka organizacijos politikos nuostatas ir rizikos priimtinumo kriterijus (žr. „c“);
3) išvengti rizikos;
4) kelti veiklos riziką kitoms šalims, pvz., draudimo bendrovėms, tiekėjams.

g) *Nustatykite kontrolės uždavinius ir pasirinkite rizikos kontrolės priemones*
Atitinkami kontrolės uždaviniai ir kontrolės priemonės turi būti pasirenkami iš šio standarto A priedo. Jų pasirinkimas turi būti grindžiamas rizikos analizės išvadomis ir rizikos tvarkymo procesu.
PASTABA. Standarto A priede išvardytų kontrolės uždavinių ir kontrolės priemonių sąrašas nėra išsamus, todėl galima pasirinkti ir papildomus kontrolės uždavinius bei priemones.

Šios struktūros turi būti laikomasi, rengiant rizikos analizės ataskaitą pagal BS 7799-2:2002 C dalies 4.3.1 („Documentation requirements“ – „Dokumentacijos reikalavimai“) [1, p. 7] reikalavimus.

T. Peltier [23, p. 5] apibrėžia rizikos analizės procesą kaip toliau nurodytus žingsnius:

1. Apžvelgiamų elementų nustatymas;
2. Su elementu susijusių grėsmių, rizikos, rūpesčių ir kitų klausimų nustatymas;
3. Prioritetinės rizikos arba svarbiausių elemento pažeidžiamumų nustatymas;
4. Korekcinių, kontrolės arba saugos priemonių įdiegimas ar rizikos priėmimas;
5. Įdiegtų kontrolės priemonių efektyvumo stebėsena ir jo įvertinimas.

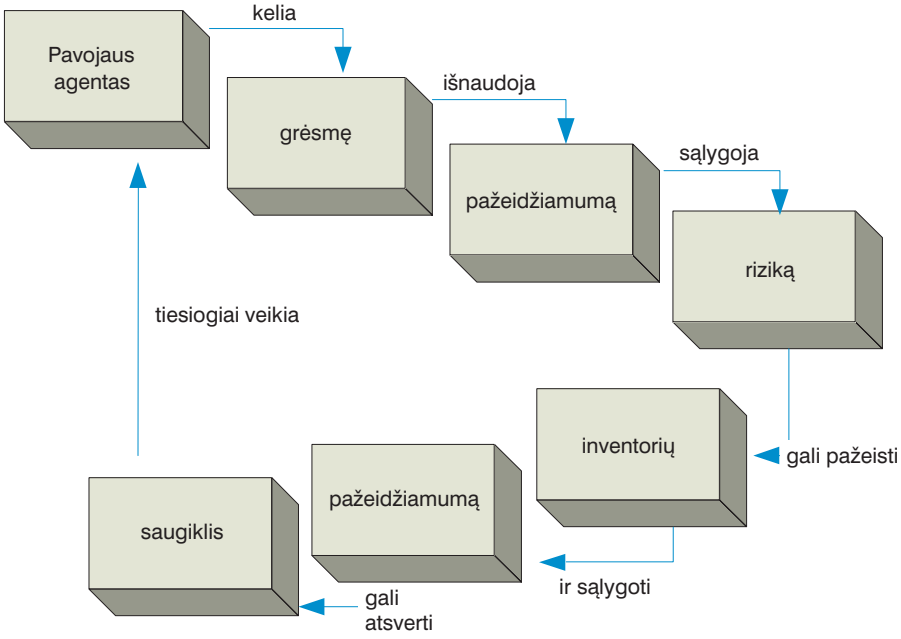
„Microsoft“ rizikos analizės vadove [22, p. 26] pateikta rizikos analizės fazė yra šiek tiek paprastesnė:

- Svarbiausių duomenų surinkimas – aptarkite sėkmės veiksnius ir parenkite instrukcijas.
- Surinkite rizikos duomenis – apibrėžkite duomenų rinkimo ir analizės procesą.
- Nustatykite rizikos prioritetus – apibrėžkite kiekybinio ir kokybinio rizikos įvertinimo žingsnius.

Rizikos analizės procesas atrodo paprastas, tačiau jo įgyvendinimas gali pareikalauti didelių pastangų, aukštos kompetencijos ir abstraktaus mąstymo įgūdžių. Atlikdamas rizikos analizę, vertintojas turi sugebėti tinkamai vartoti tokias sąvokas, kaip *rizika, grėsmė, nematerialių vertybių pažeidžiamumas,* orientuotis vertybių ir jų vertinimo ypatumuose, numatyti vertes ir rizikos tikimybę.

4. Rizikos analizės strategijos

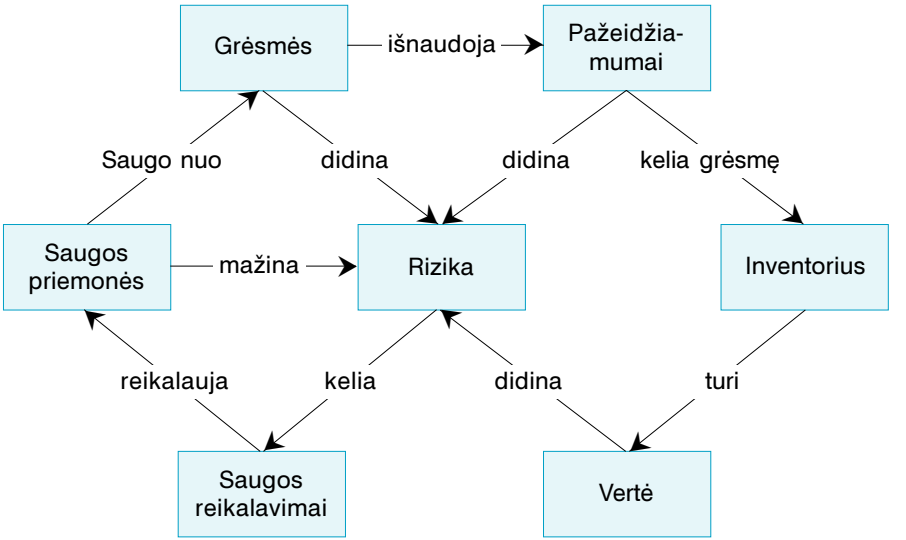
Atliekant rizikos analizę, būtina įvertinti rizikos pavojaus, pažeidžiamumo, verčių, saugos valdymo priemonių ir rizikos tarpusavio sąsajas. Šios sąsajos grafiškai pavaizduotos 4.1 ir 4.2 pav.



4.1 pav. Skirtingų saugos komponentų tarpusavio sąsajos.

Standarto LST ISO/IEC TR 13335-1:2000 [15, p. 15] dalis parodo tarpusavio sąsajas rizikos valdymo požiūriu (3 pav.). Be to, priklausomai nuo aptariamos aplinkos ir organizacijos brandumo lygio, gali būti taikomi arba bendrojo pobūdžio, arba giluminės rizikos analizės metodai. Bendrojo pobūdžio metodai paprastai remiasi kiekybiniais metodais, tuo tarpu giluminė analizė gali būti grindžiama ir kokybiniais metodais. Standarte LST ISO/IEC 13335-2:2000 išvardyti keturi rizikos analizės metodai [16, p.9]:

1. Pagrindinis metodas,
2. Neformalus metodas,
3. Detali rizikos analizė,
4. Kombinuotas metodas.



4.2 pav. Rizikos valdymo elementų tarpusavio santykiai [15, p. 15].

Organizacija, norinti padidinti savo saugą, privalo sukurti rizikos valdymo strategiją, tinkančią aplinkai ir efektyviai rizikos prevencijai. Būtina tokia strategija, kuri suvienytų visas saugos užtikrinimo pastangas ir leistų efektyviai panaudoti išteklius bei laiką.

Pagrindinis metodas reiškia, kad bendras sistemos saugos lygis užtikrinamas, taikant įprastinę praktiką ir priemones, išvardytas įvairiais standartais.

Pagrindinio metodo privalumas yra tas, kad jis nereikalauja skirti jokių išteklių detalizuotai rizikos analizei, saugos priemonių pasirinkimui reikalingas laikas ir jų kaštai sumažėja, o pagrindinės saugos priemonės nereikalauja didelių išteklių. Pavyzdžiui, rekomenduojama įdiegti antivirusinę programinę įrangą visuose asmeniniuose kompiuteriuose, neatsižvelgiant į konkretaus kompiuterio panaudojimo pobūdį (t. y., ar jis prijungtas prie interneto, kokia yra kompiuterinio tinklo paslaugų parametrų konfigūracija ir t. t.).

Tačiau šis metodas turi ir trūkumų. Pirma, bendras privalomos saugos lygis tampa pernelyg aukštas, tam tikrų sistemų saugos priemonių įdiegimas gali būti labai brangus arba riboti veiklą. Jeigu pasirenkamas pernelyg žemas saugos lygis, sauga gali būti nepakankama. Antra, gali būti sudėtinga valdyti saugos prasme svarbius pakeitimus. Pavyzdžiui, atnaujinant sistemos įrangą bus sudėtinga nustatyti, ar atnaujinimas paveiks esamas saugos priemones ir ar jos bus tinkamos.

Pagrindinio metodo strategija geriausiai tinka diegiant saugos valdymo standartus, tokius kaip LST ISO/IEC 17799:2002 [20] (Bendrasis administravimas ir informacijos sauga), LST ISO/IEC TR 13335 [15, 16, 17, 18, 19] (informacinių technologijų ir kompiuterinių tinklų saugos valdymas), CobIT (bendrasis IT valdymas), ITIL (bendrasis IT valdymas), Baselio standartas (ban-

kų informacinių sistemų valdymas) ir kiti, įskaitant daugybę reguliariai atnaujinamų specifinių praktikų, pavyzdžiui, www.cert.org, www.isaca.org, www.securityforum.com ir t.t.

Neformalus metodas reiškia, kad remiantis asmeninėmis žiniomis ir patirtimi, atliekama neformali, tačiau pragmatiška visų sistemų rizikos analizė. Jeigu negalima atlikti vidinės saugos patikros, gali būti pakviečiami konsultantai iš šalies.

Šios strategijos privalumas yra tai, kad neformalios analizės atlikimas nereikalauja įgyti papildomų įgūdžių, todėl ji atliekama greičiau, negu *detali rizikos analizė* ir yra efektyvesnė mažoms organizacijoms. Tačiau ji taip pat turi trūkumų. Pavyzdžiui, rezultatams įtaką daro subjektyvūs požiūriai ir nuostatos, nepakankamai pagrįstai pasirenkamos priemonės, todėl gali būti sunku pateisinti išlaidas saugos priemonėms, o be pakartotinės analizės būna sunku valdyti saugai svarbius pakeitimus.

Nors standartas ISO IEC TR 13335-2:2000 nurodo, kad šio metodo trūkumas yra sistemingos analizės nebuvimas, buvo paskelbti keli struktūriniai neformalios kokybinės analizės metodai, tokie kaip KURAP, dešimties žingsnių KRA, KRA+ ir kiti [23].

Detali rizikos analizė reiškia nustatomo turto vertę, jo patiriamas grėsmes ir pažeidžiamumus. Detali rizikos analizė yra daug darbo reikalaujantis procesas, todėl reikia tiksliai nustatyti analizės ribas, o vadovybė privalo jai nuolat skirti dėmesio. Šios alternatyvos privalumas tai, kad galima nustatyti kiekvienai sistemai reikalingą saugos lygį, o analizės išvados suteikia puikų pagrindą, valdant saugos pakeitimus. Tačiau siekiant gauti apčiuopiamų rezultatų, reikia gana daug laiko, patikimos informacijos ir nemažai pastangų.

Detalios rizikos analizės metodų pasirinkimas labai platus, ir jai paprastai taikomi kiekybiniai metodai arba detalūs kokybiniai metodai.

Kombinuotas metodas reiškia, kad iš pradžių, pasitelkus bendrojo lygio analizę (pavyzdžiui, atlikus atitikimo saugos valdymo standartams analizę), nustatomos sistemos, reikšmingiausios organizacijos veiklai arba galinčios patirti didžiausias grėsmes. Tokioms sistemoms paprastai taikoma kombinuota rizikos analizė. Šis metodas suderina pagrindinio ir detalios rizikos analizės metodų privalumus, kadangi analizei reikalingos laiko ir išteklių sąnaudos sumažėja, o tinkama sauga užtikrinama visoms sistemoms.

Kombinuoto metodo privalumai yra tokie: didesnė tikimybė, kad rizikos valdymo programa bus patvirtinta, prieš panaudojant ženklesnius išteklius; galima sukurti bendrą visai organizacijai tinkantį metodą, neturintį spragų; ištekliai ir lėšos naudojamos tada, kai iš tikrųjų būtina, o didžiausią riziką patiriančios sistemos gali būti įvertintos iš anksto.

Kombinuoto metodo trūkumas tas, kad taikant bendrojo lygio rizikos analizę galimi netikslūs rezultatai ir neteisingai parinktos sistemos, kurioms būtina detali analizė.

Visų sistemų detali analizė būtų neefektyvi laiko prasme, bet, antra vertus, negalima neatsižvelgti į rimtas grėsmes. Metodas, galintis išlyginti šiuos du kraštutinumus, reikalauja: a) atlikti bendrojo lygio IT sistemų saugos poreikių revizijas ir b) pateikti smulkias ataskaitas apie tokių poreikių tenkinimą. Todėl prieš pradedant bet kokio pobūdžio analizę, būtina kiek galima išsamiau apibrėžti nagrinėjamą aplinką. Kuo sudėtingesnė aplinka ir kuo blogiau apibrėžtos jos vertės, tuo mažesnis bus detalios analizės efektyvumas. Pasirinkus rizikos analizės metodą, reikia apibrėžti ir vėlesnius įvertinimus. Jeigu siekiama įdiegti technines saugos valdymo priemones ir pateisinti investicijas, tinkamiausia pasirinkti bendrąją arba detaliąją kiekybinę rizikos analizę, kadangi analizės rezultatai būtų skaitiniai arba piniginiai vienetai, kurie

leistų nustatyti rizikos valdymo priemonių prioritetus pagal kainą. Jeigu siekiama įdiegti procedūras arba atlikti organizacinius pakeitimus, kokybinė analizė būtų efektyvesnis būdas. Jeigu organizacija arba institucija atlieka visos organizacijos rizikos analizę pirmą kartą, geriausia rinktis pagrindinį analizės metodą.

Sėkminga rizikos analizė ne tik rodo potencialios rizikos ir jos priežasčių sąsajas (4.1 ir 4.2 pav.), bet ir leidžia vadovybei priimti pagrįstus sprendimus dėl tinkamiausių saugos valdymo priemonių.

Informacijos šaltinių įvertinimas rizikos analizės metu

Rengiantis rizikos analizei, būtina labai gerai suvokti pagrindinius informacijos šaltinius, jų privalumus ir trūkumus, taip pat nustatyti informacijos gavimo būdus ir jos parametrus. Informacijos šaltiniai gali būti įvertinti pagal tikslumą, tinkamumą ir patikimumą. Informacijos tikslumas reiškia pirminio reiškinio atspindėjimo laipsnį. Tinkamumas parodo, kaip informacija susijusi su analizės objektu, o patikimumas išreiškia tikimumą, kad atlikus pakartotinį tikrinimą, bus gauti tokie patys rezultatai. Pagal informacijos tikslumą, tinkamumą ir patikimumą informacijos šaltiniai skirstomi į pirminius, antrinius ir tretinius. Informacijos tinkamumas nustatomas, remiantis analizės objekto apibrėžimu, ir tai įeina į analizę atliekančio asmens pareigas.

Vertinant tinkamumą informacijos, kurią rengiamasi panaudoti rizikos analizei, būtina atlikti tinkamumo testą (4.1 lentelė).

4.1 lentelė

INFORMACIJOS TINKAMUMO ĮVERTINIMAS

	Pirminiai	**Antriniai**	**Tretiniai**
Apibrėžimai	Šaltiniai, kuriuose yra neapdorota, originali, neinterpretuota ir neįvertinta informacija.	Šaltiniai, kurie sumuoja, analizuoja, vertina ir interpretuoja informaciją, paimtą iš pirminių šaltinių. Paprastai jie būna aiškinamojo pobūdžio.	Šaltiniai, kurie kompiliuoja, analizuoja ir sumuoja antrinius šaltinius. Paprastai jie faktiniai.
Pavyzdžiai	Įvykių registras, operatoriaus prisijungimų registras ir pastabos, tinklo skanavimo duomenys, techninė dokumentacija, atvejai, korespondencija, interviu	Kritika ir interpretacija, istorija, istorija ir kritika, vyriausybės politika, įstatymai,moraliniai ir etiniai aspektai,politiniai aspektai, politika ir vyriausybės sprendimai, psichologiniai aspektai, viešoji nuomonė, religija,religiniai aspektai, socialinė politika, studijos ir mokymai.	Santraukos,bibliografija,chronologija, klasifikacija, žodynai, žodynai ir enciklopedijos, direktorijos, enciklopedijos, vadovėliai, instrukcijos, vadovai ir pan., identifikacijos indeksai, registrai, statistika, lentelės, indeksai.

5. Kiekybiniai rizikos analizės metodai

Skirtumas tarp kiekybinių ir kokybinių rizikos analizės metodų yra labai paprastas: kiekybinės rizikos analizės metu analizuojamiems komponentams ir potencialiems nuostoliams siekiama suteikti objektyvias skaitines vertes (pvz., išreiškiant jas eurais). Tuo tarpu kokybinės rizikos analizės metu taikomos nematerialiosios verčių išraiškos, tokios kaip duomenų praradimas, ir orientuojamasi į kitus veiksnius, užuot naudojant pinigines išraiškas.

Jeigu suklasifikuojami ir įvertinami visi elementai (turto vienetų vertė, poveikis, grėsmės dažnumas, saugos priemonių efektyvumas, jų kaštai, abejotinumas ir tikimybė), ir jiems priskiriamos vertės, rizikos analizės procesas laikomas kiekybiniu. Grynai kiekybinė rizikos analizė neįmanoma, nes tenka taikyti ir kokybinius metodus. Taigi skaitytojas turi suprasti, net jei „popieriniai skaičiai“ atrodo objektyvūs, kad tiksliai nuspėti ateities neįmanoma.

Kiekybinės rizikos analizės procesas – tai didelis projektas, todėl jam reikalingas projekto arba programos vadovas, kuris koordinuotų pagrindinius analizės etapus. Didžiąją kiekybinės rizikos analizės pirminio planavimo dalį sudaro reikalingo laiko apskaičiavimas. Be to, būtina parengti detalų analizės procedūros planą ir paskirstyti įpareigojimus rizikos analizės grupės nariams.

Prieš pradedant kiekybinę rizikos analizę, paprastai atliekamas *preliminarus saugos įvertinimas* (PSĮ). PSĮ leidžia pasirengti kie-

kybinei rizikos analizei. Preliminarus saugos įvertinimas taip pat padeda susikoncentruoti ties rizikos analize. Šio etapo metu identifikuoti elementai turėtų apimti turto vertę, įvairių organizacijai kylančių grėsmių sąrašą (grėsmių, kylančių tiek iš aplinkos, tiek iš personalo), taip pat egzistuojančių saugos priemonių dokumentaciją. Prieš pradedant realią kiekybinę rizikos analizę, preliminarius saugos įvertinimo rezultatus paprastai peržiūri organizacijos vadovybė.

Rinka siūlo keletą gerų automatizuotų rizikos analizės priemonių. Pagrindinis šių priemonių uždavinys – sumažinti rizikos analizei būtinų žmogiškųjų sąnaudų poreikį ir suteikti įmonėms galimybę operatyviai prognozuoti numatomus nuostolius, naudojant skirtingas duomenų įvestis. Duomenų bazės sukūrimas pradinėje automatizuotoje proceso fazėje leidžia operatoriams pakartoti analizę, taikant skirtingus parametrus, t.y, kurti scenarijus „o kas, jeigu..?“. Šios priemonės padeda vartotojams greitai apskaičiuoti galimus nuostolius ir tokiu būdu įvertinti įdiegtų saugos priemonių naudingumą.

Pažeidžiamumo veiksnys (PV)

PV yra žalos, kurią patirtų konkrečios vertybės grėsmės realizavimo atveju, procentinė išraiška. Ši reikšmė reikalinga, kad būtų galima apskaičiuoti *Tikėtiną vienkartinį nuostolį* (TVN), o šis reikalingas apskaičiuoti *Tikėtiną metinį nuostolį* (TMN). PV procentinė vertė gali būti ir labai maža, pvz., tam tikros techninės įrangos gedimo sąlygotas nuostolis, ir labai didelė, pvz., katastrofiškas visų kompiuterinių išteklių praradimas.

Tikėtinas vienkartinis nuostolis (TVN)

TVN – tai piniginė vertė, priskiriama vienam saugos įvykiui. Ji išreiškia nuostolį, kurį organizacija gali patirti dėl vienos grėsmės. TVN apskaičiuojamas pagal tokią formulę:

turto vertė (EUR) x Pažeidžiamumo veiksnys (PV) = TVN

Pavyzdžiui, turto vertė yra 100 000 EUR, jo pažeidžiamumo veiksnys – 30 procentų, vadinasi, TVN lygus 30 000 EUR. Nors šis rodiklis dažniausiai apskaičiuojamas siekiant gauti *Tikėtiną metinį nuostolį* (TMN), kartais jis naudojamas ir atskirai, nusakant katastrofišką įvykį *Poveikio veiklai analize* (PVA).

Metinis dažnumo rodiklis (MDR)

MDR – tai skaičius, kuris išreiškia apskaičiuotą grėsmės iškilimo dažnumą per metus. Jo reikšmė gali būti nuo 0,0 (niekada) iki didelio skaičiaus (pvz., smulkūs pavojai, neteisingai užrašytas vardas duomenų laukelyje). Objektyviai apskaičiuoti šį rodiklį gali būti labai sunku. Paprastai jis nustatomas remiantis įvykio tikimumu ir skaičiumi darbuotojų, kurių klaida galėtų sukelti saugos įvykį. Įvykio sąlygojama žala šiuo atveju **nėra** įvertinama, vertinamas tik įvykio **dažnumas**.

Pavyzdžiui, tikimybė, kad į duomenų centrą pataikys meteoritas, yra kartas per 100 000 metų, taigi tokio įvykio MDR yra 0,00001. Tuo tarpu tikimybės, kad 100 duomenų operatorių mėgins neleistinai prisijungti prie sistemos, gali būti apskaičiuojama po šešiskart per metus kiekvienam operatoriui, taigi viso Metinis dažnumo rodiklis sudarys 600.

Tikėtinas metinis nuostolis (TMN)

TMN – tai piniginė išraiška, apskaičiuojama pagal tokią formulę:

Tikėtinas vienkartinis nuostolis (TVN) x
Metinis dažnumo rodiklis (MDR) = TMN

Kitaip tariant, TMN yra tikėtinas metinis nuostolis, kurį gali patirti organizacija dėl vienokios arba kitokios grėsmės. Pavyzdžiui, grėsmės, kurios vertė (TVN) sudaro 100 000 EUR ir kurios tikimybė yra kartas per tūkstantį metų (MDR = 0,001), TMN bus 100 EUR. Tai leidžia geriau atlikti kaštų-naudos analizę. Būtina atsiminti, kad TVN apskaičiuojama pagal turto vertę ir jo *Pažeidžiamumo veiksnį* (PV).

5.1 lentelė

KIEKYBINĖS ANALIZĖS FORMULĖS

Pažeidžiamumo veiksnys (PV)	Žalos procentas vertybei, kurią gali sąlygoti grėsmė.
Tikėtinas vienkartinis nuostolis (TVN)	Turto vertė x Pažeidžiamumo veiksnys (PV).
Metinis dažnumo rodiklis (MDR)	Įvykio dažnumas per metus.
Tikėtinas metinis nuostolis (TMN)	Tikėtinas vienkartinis nuostolis (TVN) x Metinis dažnumo rodiklis (MDR).

Kiekybinės rizikos analizės etapai

Trys pirmieji rizikos analizės žingsniai yra panašūs į *Poveikio veiklai analizės* etapus. Tačiau kokybinė rizikos analizė paprastai išsa-

mesnė ir ji konstruojama taip, kad būtų kiekybiškai įvertinti komplikuoti ir įvairūs rizikos scenarijai. Trys pirmieji žingsniai tokie:

1. Apskaičiuokite potencialią žalą turtui, nustatydami jo vertę;
2. Išanalizuokite potencialias grėsmes vertybei;
3. Apskaičiuokite *Tikėtiną metinį nuostolį* (TMN).

Potencialios žalos apskaičiavimas

Kad būtų galima apskaičiuoti potencialią žalą, kurią gali patirti organizacija grėsmės realizacijos atveju, turtas turi būti įvertintas, pasitelkus kokį nors plačiai naudojamą standartinį turto įvertinimo metodą (vėliau šis klausimas bus aptartas išsamiau). Kai turtas bus išreikštas finansine verte, *Pažeidžiamumo veiksniu* bus galima apskaičiuoti *Tikėtiną metinį nuostolį.*

Potencialių grėsmių analizė

Šiame etape nustatomos grėsmės, jų tikimybė ir dažnumas. Kad galėtume nustatyti grėsmes, privalome taip pat suprasti vertybės pažeidžiamumus ir atlikti Metinio dažnumo rodiklio skaičiavimus.

Šiame etape turi būti įvertintos visų pobūdžių grėsmės, nepriklausomai nuo to, ar jos atrodo tikėtinos, ar ne. Būtų naudinga sugrupuoti grėsmes pagal tipus, šaltinius arba pagal jų numanomą mastą. Kai kurios organizacijos gali pateikti jų veikloje iškylančių grėsmių dažnumo statistiką. Be to, yra keletas grėsmių kategorijų grupių.

Šiame skyriuje pateikiamos kelios grėsmių kategorijos:

Duomenų klasifikacija. Duomenų rinkimas arba koncentracija, kuri gali sudaryti sąlygas neteisingam duomenų interpretavi-

mui, slaptam manipuliavimui kanalais, piktybinio kodo/viruso/Trojos arklio/kirmino/loginės bombos panaudojimui, arba atsakomybės koncentracija (nepakankamas pareigų atskyrimas);

Informacinis karas. Technologinis terorizmas, piktybinis kodas arba logika ar įsiskverbimas karinio arba pramoninio šnipinėjimo tikslu;

Personalas. Neteisėtas arba nekontroliuojamas prisijungimas prie sistemų, įgaliotųjų vartotojų piktnaudžiavimas technologija, nepatenkintų darbuotojų kenkėjiški veiksmai arba suklastotos informacinių duomenų įvestys;

Programinė įranga/veikimas. Neefektyvi saugos programa, sąlygojanti procedūrines klaidas arba neteisingas duomenų įvestis;

Kriminaliniai atvejai. Fizinis sunaikinimas arba vandalizmo aktai, vertybės arba informacijos vagystė, organizuota vidaus vagystė, ginkluotas apiplėšimas arba fizinė žala personalui;

Aplinka. Infrastruktūros gedimai, paslaugų neteikimas, stichinės nelaimės ar panašūs pavojai;

Kompiuterinė infrastruktūra. Techninės įrangos gedimai, programinės įrangos veikimo sutrikimai, operacinės sistemos „lūžiai“ arba ryšių sistemos gedimai;

Pavėluotas apdorojimas. Sumažėjęs produktyvumas arba pavėluotai gautos lėšos, lemiančios pajamų mažėjimą, išlaidų augimą arba delspinigius;

Tikėtino metinio nuostolio (TMN) apskaičiavimas

Nustačius Tikėtiną vienkartinį nuostolį (TVN) ir Metinį dažnumo rodiklį (MDR), naudojantis anksčiau nurodyta formule, galima apskaičiuoti TMN.

Rezultatai

Atlikus rizikos analizę galutiniai rezultatai turi atspindėti:

- kritinės reikšmės vertybių finansinį įvertinimą;
- detalų svarbiausių grėsmių sąrašą;
- kiekvienos grėsmės tikimybę ir galimą jos iškilimo dažnumą;
- grėsmės sąlygojamus potencialius nuostolius – finansinį poveikį, kuris gali grėsti vertybei, eurais;
- rekomenduojamus sprendimus ir saugos priemones arba kontrpriemones.

Sprendimai

Pagrindiniai sprendimai, kuriuos galima taikyti po vieną arba kombinuojant tarpusavyje, yra trys:

- *Rizikos mažinimas.* Priemonės, mažinančios rizikos lygį ir jos poveikį vertybėms, visos organizacijos mastu;
- *Rizikos perkėlimas.* Potencialių kaštų arba nuostolių perkėlimas kitai šaliai (pvz., draudimo bendrovei);
- *Rizikos priėmimas.* Priimamas galimos rizikos lygis, o galimi nuostoliai absorbuojami.

Paprastai pasirenkamas toks sprendimas, kuris labiausiai sumažina riziką ir užtikrina mažiausius metinius eksploatavimo kaštus.

Saugos priemonių pasirinkimo kriterijai

Atlikus rizikos analizę, būtina įvertinti ir rekomenduoti saugos priemones ir kontrpriemones. Yra keletas standartinių saugos priemonių pasirinkimo principų, kurie garantuoja tinkamą grėsmės prevenciją ir kontrolę. Norint pasirinkti veiksmingiausią kontrpriemonę, būtina išnagrinėti svarbiausius kriterijus. Taip pat žr. skyrių dėl dizaino.

Kaštų-naudos analizė

Vienas saugos priemonių pasirinkimo kriterijų yra diegiamų priemonių kaštų efektyvumas, kuris įvertinamas pasitelkus kaštų-naudos analizės metodą. Norint nustatyti bendruosius saugos priemonės kaštus, būtina įvertinti daugybę elementų, įskaitant:

- saugos priemonės įsigijimo, sukūrimo ir (arba) licencijos kaštus;
- fizinio įdiegimo kaštus ir normalaus darbo proceso sutrikimo saugos priemonės diegimo ir testavimo metu patirsiamus kaštus;
- įprastines eksploatacines išlaidas, išteklių skyrimą, priežiūros-remonto išlaidas.

Paprasčiausias būdas apskaičiuoti konkrečios saugos priemonės kaštus-naudą yra toks:

(TMN prieš saugos priemonės įdiegimą) – (TMN po saugos priemonės įdiegimo) – (metiniai saugos priemonės kaštai) = saugos priemonės naudingumas organizacijai

Pavyzdžiui, jeigu nustatytas grėsmės TMN yra 10 000 EUR, TMN po saugos priemonės įdiegimo yra 1 000 EUR, o metinės saugos priemonės eksploatavimo išlaidos viso sudaro 500 EUR, tuomet saugos priemonės teikiama nauda bus 8 500 EUR per metus. Ši suma lyginama su pradinėmis išlaidomis ir nustatomas naudingumas arba jo stoka.

Gali būti skaičiuojama vienos saugos priemonės vertė arba, pasitelkus sudėtingas formules, viso saugos priemonių komplekto vertė. Be apskaičiuoto finansinio kaštų-naudos santykio, kiti veiksniai taip pat gali daryti įtaką sprendimui dėl konkrečios saugos priemonės įdiegimo.

Darbo sąnaudų lygis

Prieš pasirenkant saugos priemonę, turi būti įvertintos saugos priemonei eksploatuoti reikalingos darbo sąnaudos. Kiekvienu atveju dėl žmogiškųjų klaidų arba programos trūkumų atsiranda papildomų pažeidžiamumų. Faktiškai automatinėms sistemoms reikalingas nustatymas „gedimas-saugu“ (t.y. gedimo atveju sistema pereina į saugų režimą), išaiškėjus pažeidžiamumui leidžia sistemą išjungti rankiniu būdu. Kuo labiau automatizuotas procesas, tuo jis nuoseklesnis ir patikimesnis.

Be to, saugos priemonės turi būti lengvai valdomos ir be priežasties netrukdyti įprastiniams veiklos procesams. Šios savybės būtinos, kad saugos priemonei pritartų aptarnaujantis personalas ir kad organizacijos vadovybė užtikrintų saugos priemonės sėkmingam darbui reikalingą palaikymą.

Atskaitomybės ir auditavimo savybės

Saugos priemonė turi leisti atlikti auditavimo ir atskaitomybės funkcijas. Auditoriams turi būti sudaryta galimybė audituoti ir tikrinti saugos priemonę, taip pat turi būti atskaitomybės funkcija, leidžianti efektyviai stebėti kiekvieną asmenį, kuris prisijungia prie kontrpriemonių arba jų nustatymų.

Atkūrimo galimybė

Saugos priemonė turi būti įvertinta, atsižvelgiant į jos funkcionavimą po aktyvavimo arba perkrovimo. Atliekant perkrovimą ir po jo techninė saugos priemonė turi tenkinti šias sąlygas:

- nesukelti destrukcijos aktyvavimo arba perkrovimo metu;
- nesukurti slaptų kanalų perkrovimo metu arba kontrolės tikslais;

- neprarasti saugos funkcijos ir nepadidinti pažeidžiamumo po aktyvavimo arba perkrovimo;
- standartinis nustatymas turi būti toks, kad operatoriaus prieiga arba teisės nebūtų aktyvuotos tol, kol saugos priemonė nebus visiškai parengta darbui.

Santykiai su tiekėjais

Turi būti patikrintas saugos priemonės tiekėjo patikimumas ir jo darbas praeityje. Be to, turi būti žinomas programinės įrangos atviras kodas, kad būtų galima išvengti slaptų priemonių, užkertančių kelią vėlesnei modifikacijai arba leidžiančių nežinomoms programoms slapta įsiskverbti į sistemą. Turi būti atsižvelgta ir į tiekėjo siūlomas aptarnavimo paslaugas bei dokumentus.

6. Kokybinės rizikos analizės metodai

6.1. KRA – dešimties žingsnių metodas

Tai dešimties žingsnių metodas, apimantis rizikos analizės procesą nuo projekto planavimo stadijos iki pat galutinės ataskaitos. Kiekvieno ankstesnio žingsnio rezultatai naudojami kaip duomenys kitam etapui.

1 žingsnis. Rizikos analizės apimties nustatymas

Kiekvienas sėkmingas projektas prasideda nuo apibrėžimo, nurodančio, kas turi būti atlikta, pvz., tikslai, rezultatai ir darbų apimtis.

Darbų apimties nustatymas prasideda suradus rėmėją. Paprastai rėmėjas yra sistemos, duomenų arba proceso valdytojas. Valdytojas – tai asmuo, atsakingas už bendrą atitinkamos vertybės saugą. Daugumoje organizacijų rėmėjas nėra IT skyriaus darbuotojas.

Kitu etapu būtina nustatyti rizikos analizės ribas. Ribų apibrėžimas turėtų būti orientuotas į procesus, kuriems organizacija gali daryti įtaką.

Rizikos analizės apibrėžime turėtų būti nurodyti pagrindiniai bendrieji analizės uždaviniai. Informacijos saugos srityje uždaviniai apibrėžiami kaip galimų nuostolių įvertinimas, atsižvelgiant į informacijos konfidencialumui, vientisumui ir prieinamumui kylančius pavojus.

2 žingsnis. Kompetentingos grupės suformavimas

Labai svarbu užtikrinti, kad į *Kokybinės rizikos analizės grupę* (KRAG) būtų įtraukti tik kompetentingi asmenys. Siekiant užtikrinti rizikos analizės veiksmingumą, KRAG turi būti atstovaujami šie organizacijos padaliniai arba interesų grupės:

- Funkciniai vertybių valdytojai;
- Sistemos vartotojai;
- Sistemos analizės padalinys;
- Taikomųjų programų kūrimo ir plėtojimo padalinys;
- Duomenų bazių administravimo padalinys;
- Audito padalinys (jeigu reikia);
- Fizinės saugos kontrolė;
- Ryšių padalinys;
- Teisininkai (jeigu reikia);
- Duomenų apdorojimo valdymo padalinys;
- Sistemos programavimo padalinys (operacinės sistemos);
- Informacijos saugos padalinys.

Svarbu, kad kiekvienas organizacijos padalinys, kuriam analizuojama sistema daro įtaką, atstovautų grupei.

3 žingsnis. Rizikos nustatymas

KRA grupės nariai turi nustatyti rizikas, kylančias nagrinėjamam analizės objektui. Rizikai nustatyti gali būti taikoma keletas metodų. Vienas iš metodų yra pateikto rizikos tipų sąrašo analizė ir nustatymas, kurie iš nurodytų rizikos tipų galėtų būti aktualūs konkrečiu atveju. Šiuo tikslu KRA grupės nariai turėtų sudaryti rizikos sąrašą su komentarais. Atliekant rizikos analizę pirmą kartą, šis darbas gali užimti daug laiko, bet sudarytas ir patikrintas sąrašas gali būti naudojamas kitoms rizikos analizėms.

Tačiau metodas turi trūkumų: ieškodami atsakymų, grupės nariai linkę naudotis tik rizikos sąrašais, ir neieško naujų idėjų. Šiuo atveju sprendimas galėtų būti „idėjų vėtra“ – visi grupės nariai turi užrašyti savo idėjas ant popieriaus lapų, o paskui tos idėjos pristatomos kitiems grupės nariams. Vėliau šios idėjos sisteminamos ir klasifikuojamos.

Kai nustatomos visos realios rizikos, jos turi būti surašytos į rizikos veiksnių 6.1.1 lentelę:

6.1.1 lentelė

RIZIKOS VEIKSNIAI

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Žalos pobūdis**	**Rizikos veiksnys**

4 žingsnis. Rizikos klasifikacija

Nustačius riziką ir surašius ją į rizikos veiksnių lentelę, KRAG turi atlikti tikimybės įvertinimą. Kiekvienos rizikos tikimybė turi būti išreikšta skaitine verte, pradedant nuo mažiausios iki didžiausios (žr. 6.1.2 klasifikavimo lentelę).

6.1.2 lentelė

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

Kiekvienas grupės narys kiekvienos rizikos tikimybei turi priskirti skaitinę vertę.

Įvertinus kiekvienos rizikos tikimybę, duomenys surašomi į rizikos kategorijos stulpelį:

6.1.3 lentelė

RIZIKOS ĮVERTINIMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Žalos pobūdis**	**Rizikos veiksnys**
Gaisras	3		
Užliejimas vandeniu	2		
Vagystė	2		
Uraganas	3		

5 žingsnis. Rizikos klasifikacija

Šiame etape KRA grupės nariai turi įvertinti žalą, kurią gali sukelti rizika, pvz., rizikos poveikį vertybei. Kad gautų rezultatus, grupės nariai turi įvertinti žalą, kurią gali sukelti kiekviena rizika, darydami prielaidą, kad nebuvo imtasi jokių saugos priemonių. Tolesni žingsniai leidžia įvertinti jau įdiegtas saugos priemones ir apskaičiuoti jų rizikos prevencijos poveikį.

Po to, kai grupės nariai suderina atliktus žalos įvertinimus, informacija turi būti įrašyta į lentelę (žr. 6.1.4 lentelę):

6.1.4 lentelė

RIZIKOS ĮVERTINIMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Rizika**	**Rizikos kategorija**
Gaisras	3	5	
Užliejimas vandeniu	2	5	
Vagystė	2	3	
Uraganas	3	5	

6 žingsnis. Bendros rizikos sąlygojamos žalos apskaičiavimas

Šiame etape KRA grupė susumuoja rizikos įvertinimo ir žalos vertes, gaudami kiekvienos nustatytos rizikos veiksnį (žr.6.1.5 lentelę). Rizikos veiksnio įvertinimai būna nuo 2 iki 10.

6.1.5 lentelė

RIZIKOS VEIKSNIAI

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Rizika**	**Rizikos kategorija**
Gaisras	3	5	8
Užliejimas vandeniu	2	5	7
Vagystė	2	3	5
Uraganas	3	5	8

Įvertinusi visus rizikos veiksnius, KRA grupė turi pertvarkyti lentelę ir surašyti rizikos veiksnius pagal jų vertę mažėjančia tvarka. Rizikos rūšys, kurių rizikos veiksnys yra didesnis už 6, turi būti perkelti į saugos priemonių identifikavimo lentelę.

6.1.6 lentelė

SAUGOS PRIEMONIŲ IDENTIFIKAVIMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos veiksnys**	**Galima saugos priemonė**	**Priemonės kaštai**
Gaisras	8		
Uraganas	8		
Užliejimas vandeniu	7		

7 žingsnis. Saugos priemonių nustatymas

Šiame etape KRA grupė analizuoja nustatytus trūkumus ir ieško techninių, administracinių ar fizinių priemonių, kurios užtikrintų priimtiną ir rentabilų vertybės saugos lygį.

Informacijos saugos priemonės gali būti suskirstytos pagal keturis saugos užtikrinimo lygius į išvengimo, papildomos kontrolės, susekimo ir atkūrimo priemones.

1. *Rizikos išvengimo priemonės* reiškia saugos priemones (aktyvias priemones), kurių imamasi iš anksto ir kurios yra nukreiptos į atsitiktinių ar sąmoningų rizikos priežasčių prevenciją.

2. *Papildomos kontrolės priemonės* užtikrina esamų saugos priemonių efektyvumą.

3. *Susekimo priemonės* reiškia priemones, užtikrinančias savalaikį saugos spragų susekimą, blokavimą ir reagavimą į jas.

4. *Atkūrimo priemonės* reiškia planavimo ir reagavimo funkcijas, kuriomis atkuriama aplinkos sauga ir ištiriamos saugos spragos.

Saugos priemonių pavyzdžiai ir jų pasiskirstymas pagal saugos lygius:

1. Išvengimo priemonės
    a) Šifravimas ir tapatybės nustatymas;
    b) Saugi sistemos architektūra;
    c) Rizikos analizės procesas;
    d) Informacinė švietimo programa;
    e) Informacijos saugos programa;
    f) Politika ir standartai;
    g) Viešojo rakto infrastruktūra;
    h) Saugi programinės įrangos architektūra;
    i) Saugus ryšių planavimas.
2. Papildomos kontrolės priemonės
    a) Programinės įrangos saugos auditas;
    b) Dokumentacijos auditas;
    c) Įsiskverbimo galimybės patikrinimas;
    d) Periodiški parametrų skenavimai;
    e) Saugos spragų įvertinimas.
3. Susekimo priemonės
    a) Įsiskverbimo aptikimas;
    b) Nuotolinių įsiskverbimų nuolatinis stebėjimas.
4. Atkūrimo priemonės
    a) Veiklos tęstinumo planavimas;
    b) Poveikio veiklai analizė;
    c) Krizių valdymo planavimas;
    d) Sistemų atkūrimo po katastrofos planavimas;
    e) Reagavimo į saugos įvykius procedūros;
    f) Tyrimo priemonės.

Po to, kai grupė nustato tinkamas saugos priemones, jos turi būti surašomos į saugos priemonių identifikavimo 6.1.7 lentelę. Į lentelę taip pat turi būti surašyti saugos priemonių kaštai.

8 žingsnis. Kaštų-naudos analizė

Tai vienas iš svarbiausių rizikos analizės proceso etapų. Analizė turi būti atliekama labai išsamiai bei kruopščiai ir užtikrinti informacijos saugos priemonių atitikimą organizacijos veiklos tikslams bei garantuoti reikiamą vertybių saugos lygį. Analizės metu gali prireikti grįžti prie 6 žingsnio ir atlikti jo procedūras dar kartą, pvz., kad būtų galima įvertinti galimą žalą, atsižvelgiant į planuojamas priemones.

Analizės procesas turi padėti nustatyti, kurios saugos priemonės būtų veiksmingiausios ir pigiausios.

6.1.7 lentelė

SAUGOS PRIEMONIŲ NUSTATYMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos veiksnys**	**Galimos saugos priemonės**	**Priemonių kaštai**
Gaisras	8	Priešgaisrinė sistema	15 000 EUR
Uraganas	8	Veiklos tęstinumo planavimas	75 000 EUR
Užliejimas vandeniu	7	Veiklos tęstinumo planavimas	75 000 EUR

9 žingsnis. Saugos priemonių klasifikacija

Atlikusi kaštų-naudos analizę ir pateikusi saugos priemonių sąrašą vertybių valdytojui, KRA grupė turi suklasifikuoti planuojamas saugos priemones pagal jų diegimo pirmumą. Nustatant

prioritetines priemones, KRA grupė turėtų įvertinti, nuo kokių rizikos rūšių galėtų apsaugoti konkreti priemonė, taip pat priemonės įdiegimo kaštus, jos poveikį organizacijos darbui, ar organizacija turi pakankamai vidaus išteklių priemonei įdiegti, t. y., ar bus reikalinga pagalba iš šalies.

10 žingsnis. Rizikos analizės ataskaita

Rizikos analizės rezultatai turi būti pateikti organizacijos vadovybei ataskaitos forma. Rizikos analizės ataskaitos turinio pavyzdys pateikiamas toliau:

1. Įvadas:

a) Pagrindai: šioje dalyje turi būti paaiškinta, kodėl buvo atlikta rizikos analizė ir dėl kokių priežasčių ištekliai buvo skirti vykdyti kokybinei rizikos analizei;

b) Rizikos analizės apimties apibrėžimas. (1 žingsnis) turi būti pateiktas kartu su paaiškinimais, dėl kokių priežasčių buvo nustatyta pasirinktoji rizikos analizės apimtis;

c) Metodų išaiškinimas: pasirinkto metodo išaiškinimas turi būti pateiktas kartu su trumpu jo etapų apibūdinimu.

2. Bendra apžvalga: viename-dviejuose puslapiuose turėtų būti pateiktas visos procedūros apibūdinimas ir santrauka. Tekste turi būti nurodytas priedas, kuriame pateikiamas visų KRA grupės narių sąrašas.

3. Rizikos nustatymas: šioje dalyje turi būti pateiktas rizikos nustatymo procedūros aprašymas ir informacija apie metodą, panaudotą rizikos klasifikacijai.

4. Rizikos veiksnių nustatymas.

5. Saugos priemonių nustatymas.

6. Kaštų-naudos analizė.

7. Rekomendacijos: šioje dalyje turėtų būti pateikiamos KRA grupės rekomendacijos dėl taikytinų priemonių ir galimų alternatyvų.

8. Priedai (rekomenduojami priedai):

a) Grupės narių sąrašas,

b) Sąvokos ir apibrėžimai,

c) Rizikos klasifikacija,

d) Ataskaitos.

Rizikos analizės ataskaita turi būti konfidencialus dokumentas, todėl ji turi būti prieinama tik vertybių valdytojo nurodytiems asmenims.

Kokybinė rizikos analizė yra vienas iš mažiausiai komplikuotų ir subjektyviausių analizės metodų. Rizikos analizės rezultatų kokybė tiesiogiai priklauso nuo KRA grupės narių kompetencijos ir žinių lygio. Taikant šį metodą, profesionaliai sudarytos grupės darbo rezultatai kokybės prasme gali prilygti *kiekybinės* rizikos analizės, kuri reikalauja daugiau darbo ir laiko, rezultatams.

6.2. KRA – trijų žingsnių metodas

Trijų žingsnių metodas – tai nedidelė pirmojo metodo modifikacija. Modifikacijos tikslas įvertinti mažiau apčiuopiamas rizikos rūšis ir grėsmes tokioms organizacijos vertybėms, kaip jos reputacija, klientų pasitikėjimas arba pozityvus žiniasklaidos požiūris. Metodui taikoma taškų sistema, kuri leidžia palyginti finansinę ir nefinansinę rizikas. Metodas skiriasi nuo dešimties žingsnių metodo, nes jį sudaro trys etapai: vertybių įvertinimas, rizikos įvertinimas ir rizikos valdymas. Svarbu atkreipti dėmesį į

faktą, kad rizikos analizės metodai prasideda tais pačiais žingsniais, pvz., vertybių identifikavimu ir analizės grupės sudarymu.

Pradiniame analizės apimties apibrėžimo etape būtina nustatyti funkcinį vertybių valdytoją. Paprastai funkciniu vertybių valdytoju nurodomas vadovas to organizacijos struktūrinio padalinio, kuriame buvo sukurtos vertybės arba dažniausiai naudojamos.

Labai svarbu nustatyti, kokios vertybės ir kokios veiklos sferos turėtų būti nagrinėjamos, kadangi rizikos analizė gali būti vykdoma prieinamumo, integralumo ir konfidencialumo, taip pat žalos, kurią galėtų padaryti informacijos paskelbimas, pakeitimas, neprieinamumas arba praradimas, požiūriais.

Yra daug rizikos identifikavimo metodų, bet visi metodai duoda iš esmės tokį patį rezultatą. Užbaigus procedūrą, turi būti nustatytos analizuotinos vertybės ir apibrėžtos rizikos analizės apimtys.

Kitas rizikos analizės etapas yra *Kokybinės rizikos analizės grupės* (KRA grupės) sukūrimas. Labai svarbu, kad grupė atstovautų organizacijos tikslams. Vertybių valdytojas ir jų naudotojai turi tapti svarbiausiais grupės nariais. Labai svarbu, kad grupę sudarytų profesionalai, turintys pakankamai patirties organizacijos darbe, išmanantys ir suprantantys joje vykstančius procesus bei sugebantys nustatyti potencialias problemas.

1 etapas: Vertybių įvertinimas

Užbaigus pasirengimus ir sudarius KRA grupę, pirmoji užduotis – nustatyti žalą, kurią patirtų organizacija pažeidusi vertybę. Kaip parodyta toliau pateiktuose pavyzdžiuose, KRA grupė gali naudoti keletą lentelių, padedančių nustatyti žalą, kurią organizacija galėtų patirti dėl įvairių rizikos įvykių.

6.2.1 lentelė

FINANSINIAI NUOSTOLIAI

Nuostoliai	Įvertinimas taškais
Mažiau nei 2 tūkstančiai EUR	1
Tarp 2 ir 15 tūkstančių EUR	2
Tarp 15 ir 40 tūkstančių EUR	3
Tarp 40 ir 100 tūkstančių EUR	4
Tarp 100 ir 300 tūkstančių EUR	5
Tarp 300 tūkstančių ir 1 milijono EUR	6
Tarp 1 ir 3 milijonų EUR	7
Tarp 3 ir 10 milijonų EUR	8
Tarp 10 ir 30 milijonų EUR	9
Daugiau kaip 30 milijonų EUR	10

Lentelės įvertinimai nustatomi po susitikimo ir diskusijų su įvairių organizacijos padalinių bei skyrių darbuotojais. 6.2.1 lentelėje pateikiamus finansinius nuostolius ir jų įvertinimo lygius nustato finansų skyrius. Aukščiausia ir žemiausia įvertinimo riba turi būti nustatyta, aptarus šį klausimą su atitinkamais darbuotojais. Mažiausias tikėtinas nuostolis, dėl kurio organizacija turėtų imtis kokių nors korekcinių veiksmų, turėtų būti žemutinė riba. Nuostolis, kurio pasekmės organizacijos veiklai būtų pražūtingos, turėtų būti viršutinė riba. Nustačius žemutinę ir viršutinę ribas, lentelėje turi būti nustatytos tarpinės reikšmės.

Pateiktame pavyzdyje naudojama 10 lygių; priklausomai nuo organizacijos poreikių, tokių lygių skaičius gali būti mažesnis.

Atlikdami kokybinę rizikos analizę, grupės nariai įvertinimą tokiais lygiais priskiria tam tikroms kategorijoms, remdamiesi lentelėmis, sukurtomis bendradarbiaujant su atsakingais organizacijos skyriais ir padaliniais, kurie atsakingi už tam tikros veiklos sritis.

Įvertinimą grupė atlieka, naudodama matricą (žr. 6.2.2 pavyzdį). Duomenys surašomi į lentelę, naudojant kitų lentelių duomenis (žr. 6.2.3, 6.2.4, 6.2.5 pavyzdžius).

6.2.2 lentelė

KOKYBINĖS RIZIKOS ANALIZĖS PAVYZDYS

Vertybių grupių įvertinimas, atsižvelgiant į poveikį jų prieinamumui, konfidencialumui ir vientisumui	**Finansiniai nuostoliai**	**Teisinės pasekmės**	**Konfidencialumas**	**Veiklos sutrikdymas**	
Paskelbimas					
Pakeitimas					
Neprieinamumas					
Praradimas					

6.2.3 lentelė

TEISINIŲ PASEKMIŲ LENTELĖ

Teisinės pasekmės	**Įvertinimas taškais**
Mažiau nei 5 tūkstančiai EUR	1
Tarp 5 ir 10 tūkstančių EUR	4
Tarp 10 ir 50 tūkstančių EUR	5
Tarp 50 tūkstančių ir 1 milijono EUR ir (arba) bausmė IT vadovui	8
Per 1 milijoną EUR ir (arba) bausmė bendrovės vadovybei	10

6.2.4 lentelė

VERTINGUMO KONKURENTAMS LENTELĖ

Vertingumas konkurentams	Įvertinimas taškais
Mažiau nei 50 tūkstančių EUR	1
Tarp 50 ir 100 tūkstančių EUR	4
Tarp 100 tūkstančių ir 10 milijonų EUR	5
Per 10 milijonų EUR ir (arba) bausmė bendrovės vadovams	7

6.2.5 lentelė

VEIKLOS SUTRIKDYMO LENTELĖ

Veiklos sutrikdymas	Įvertinimas taškais
Veiklos sutrikimas, apsiribojantis vienu projektu arba objektu	1
Veiklos sutrikimas, veikiantis kitas grupes arba visą padalinį	2
Veiklos sutrikimas, veikiantis visą organizaciją	3
Veiklos sutrikimas, kuris gali būti paskelbtas vietinėje žiniasklaidoje	5
Veiklos sutrikimas, kuris gali būti paskelbtas nacionalinėje žiniasklaidoje	7
Veiklos sutrikimas, veikiantis akcijų kursą	10

KRA grupė turi užpildyti lentelę, naudodama kitas lenteles, sudarytas bendradarbiaujant su įvairiais organizacijos padaliniais.

2 etapas: Rizikos įvertinimas

Įvertinimo stadijoje grupė turi identifikuoti vertybėms kylančią riziką bei grėsmes ir įvertinti saugos spragas, kurios gali būti išnaudotos grėsmių realizacijai. Grėsmių identifikavimo metodų yra daug. Tikslas: sudaryti kuo išsamesnį grėsmių ir pavojų sąrašą.

Sudariusi sąrašą, KRA grupė, atsižvelgdama į įvairių įvykių kilimo tikimybę, privalo atlikti rizikos įvertinimą, taip pat įvertinti galimą įvykių poveikį vertybėms. Kad atliktų įvertinimą, kiekvienas grupės narys privalo gerai suprasti tokias nurodytas sąvokas:

- rizika,
- įvykio tikimybė,
- galima žala (poveikis vertybėms).

Toliau pateikiamas užpildytos saugos spragų (pažeidžiamumų) lentelės pavyzdys (6.2.6 lentelė):

6.2.6 lentelė

PARENGIAMOJI LENTELĖ, PARODANTI SAUGOS SPRAGAS (PAŽEIDŽIAMUMUS)

		Žala (poveikis)		
		Maža	**Vidutinė**	**Didelė**
Tikimybė	**Didelė**	3	6	9
	Vidutinė	2	5	8
	Maža	1	4	7

Jeigu rizika nėra susijusi su nagrinėjama vertybe, 6.2.7 lentelėje, parodančioje saugos spragas (pažeidžiamumus), grupė turi įrašyti „nesusijusi“.

Paprastai lengviau analizuoti riziką, neatsižvelgiant į jau įdiegtas saugos priemones; šias priemones geriau įvertinti tolesnių analizių metu. Tokių analizių metu svarbu identifikuoti priemones, užtikrinančias rizikos prevenciją. Tokios rizikos ir jos prevencijos priemonės pavyzdys: gaisras – priešgaisrinė sistema.

3 etapas: Rizikos valdymas

Informacijos saugos priemonių, kurios būtų naudojamos rizikos prevencijai užtikrinti ir jai sumažinti iki priimtino lygio, parinkimas yra svarbiausias bet kokios rizikos analizės etapas. Naudodamasi pirmojo etapo duomenimis, grupė turėtų įvertinti vertybes ir jų reikšmę, o naudodamasi nustatytais antrojo etapo duomenimis – nepriimtiną riziką.

6.2.7 lentelė

SAUGOS SPRAGŲ ANALIZĖ

	Taškai					
	Publikacija	Pakeitimas	Praradimas	Neprieinamumas	Pažeidžiami taškai	
Analizuojama vertybė:					**Jeigu saugos priemonės netaikomos**	**Jeigu saugos priemonės taikomos**
Rizika:						

Grupė turi įvertinti jau įdiegtas informacijos saugos priemones ir surašyti duomenis į lentelę. Po to grupė turi susikoncentruoti ties pavojais, kurių prevencijos priemonės dar nėra įdiegtos. Šiame etape parengtos išvados ir rekomendacijos organizacijos vadovybei yra svarbiausios.

Siūlomos priemonės turi užtikrinti organizacijos pageidaujamą saugos lygį; tuo pačiu priemonės turi būti ekonomiškai pateisinamos. Priemonės gali veikti riziką 4 skirtingais būdais:

1. Mažinti rizikos tikimybę;
2. Mažinti riziką, kylančią dėl grėsmės pasireiškimo (mažinti rizikos poveikį);
3. Nustatyti iškilusią riziką (fiksavimas);
4. Švelninti rizikos padarinius.

KRA grupė turėtų parengti rekomendacijas vadovybei, kokios priemonės būtų efektyviausios ir kurios iš jų galėtų sušvelninti vienos ar kelių rūšių riziką.

Ataskaitoje paprastai nurodomas už numatytų priemonių įdiegimą atsakingas asmuo ir padalinys. Taip pat turėtų būti pateiktas priemonių diegimo grafikas.

Paskutinis rizikos analizės etapas – tai kitos rizikos analizės datos nustatymas.

Organizacija veikia dinamiškai kintančioje aplinkoje, todėl rizikos analizė turėtų būti atliekama bent kartą per 18 mėnesių arba kartą per dvejus metus.

ISRA – „30 minučių“ rizikos analizė

Metodas pagrįstas prielaida, kad nepatyrusiems ir tinkamai nepasirengusiems organizacijos darbuotojams rizikos analizės proce-

sas bus labai komplikuotas. Tad, norint atlikti Informacijos saugos rizikos analizę (ISRA), reikalinga šios srities specialisto pagalba.

Informacijos saugos rizikos analizės (ISRA) apžvalga

ISRA yra formalus metodas, taikomas sistemų kūrėjų, organizacijų vadovų arba informacijos saugos profesionalų, siekiant nustatyti saugos reikalavimus, kuriant veiksmų planus, analizuojant kaštus ir paskirstant atsakomybę.

Procedūra leidžia kuratoriui atlikti subjektyvią konkrečios sistemos, programos ar kitų organizacijos vertybių rizikos analizę. Atliekant ISRA, sistemos vartotojai įtraukiami į procesą pirmajame etape, kai jie išsako savo poreikius, ir vėliau, renkantis efektyviausias saugos priemones.

ISRA uždaviniai

ISRA metodas taikomas, siekiant identifikuoti nepageidautinus ir neleistinus įvykius, riziką ir grėsmes, įvertinus jų poveikį ne tiek informacijos saugai, kiek organizacijos veiklos procesams ir uždaviniams.

Informacijos saugos funkcija gali būti apibrėžta, nurodant tris jos uždavinius:

1. Duomenų vientisumas: duomenų sauga nuo neteisėto arba neplanuoto koregavimo arba praradimo;
2. Duomenų konfidencialumas: informacijos sauga nuo neteisėto arba neplanuoto paskelbimo;
3. Duomenų prieinamumas: duomenų sauga nuo blokavimo arba sauga nuo sistemos funkcionalumo praradimo.

Atliekant ISRA svarbu žinoti, nuo kokių veiksmų bus siekiama apsisaugoti:

- *nuo nesąmoningų veiksmų* – klaidų arba neatidumo;
- *nuo sąmoningų veiksmų* – neteisėtų veiksmų, tokių kaip sukčiavimas arba piktnaudžiavimas.

Rizikos analizės matrica

Matrica (pavyzdys – 6.3.1 lentelė) sudaroma, jungiant tris saugos uždavinius ir dvi rizikos grupes. Taikant matricą galima pradėti diskusiją apie rizikų nustatymą. Svarbu, kad saugos priemonių nustatymas nebūtų pradėtas tol, kol nebus įvardyta rizika. Taigi matrica užtikrina svarstymą tik tų saugos priemonių, kurios susijusios su konkrečiomis rizikos rūšimis.

6.3.1 lentelė

RIZIKOS ANALIZĖS MATRICA

	Vientisumas	Konfidencialumas	Prieinamumas
Nesąmoningi veiksmai			
Sąmoningi veiksmai			

Procedūra

Atlikdamas rizikos analizę, kuratorius turėtų kviestis kiekvienos analizuojamos sistemos dalies specialistus. Pavyzdžiui, analizuojant vietinio kompiuterinio tinklo (LAN) įrengimą pardavimų skyriuje, į rizikos analizės grupę turėtų būti įtraukti pardavimų skyriaus atstovai, vadovybės atstovai, LAN techninis specialistas, kompiuterinės ir programinės įrangos techninės pagalbos specialistas ir (arba) informacijos saugos skyriaus atstovas.

Kuratorius, atliekantis rizikos analizę, neturi būti nagrinėjamos sistemos ekspertas. Proceso metu jo funkcija apsiriboja klausimų bei bendrojo pobūdžio medžiagos pateikimu ir jos išdalijimu visiems proceso dalyviams. Svarbu, kad kuratorius būtų nešališkas.

Kaip ir atliekant bet kurią kitą rizikos analizę, grupės narių kompetencija labai svarbi. Rizikai nustatyti naudojamas „idėjų vėtros“ metodas.

6.3.2 lentelė

UŽPILDYTOS RIZIKOS ANALIZĖS MATRICOS PAVYZDYS

	Vientisumas	**Konfidencialumas**	**Prieinamumas**
Nesąmoningi veiksmai	• Neteisingų duomenų įvedimas • Duomenų įvedimas ne į tuos laukus • Pakartotinis duomenų įvedimas	• Baigus darbą, neišeinama iš sistemos • Duomenys nusiunčiami ne į tą spausdintuvą • Duomenys persiunčiami ne tiems asmenims	• Atsitiktinis duomenų sunaikinimas • Užliejimas vandeniu, gaisras • Ryšių sutrikimai
Sąmoningi veiksmai	• Neteisingų duomenų įvedimas, panaudojimas arba išspausdinimas • Duomenų koregavimas arba modifikavimas	• Neteisėtas prisijungimas • Nesankcionuotas publikavimas • Nesankcionuotas kopijavimas	• Duomenų sunaikinimas arba sugadinimas • Sabotažas • Paslaugų atsisakymo (DoS) ataka

Saugos priemonės, orientuotos į riziką

Nustačius riziką, grupė turėtų pasiūlyti priemones, kurios geriausiai tiktų apsisaugoti nuo rizikos (6.3.3 lentelė). Nustačius priemones, būtina atlikti kaštų-naudos analizę. Dažniausiai rizikos įvertinimas pinigine prasme nėra būtinas; užtenka įvertinti tik priemonių kaštus. Pavyzdžiui, jeigu rizika yra kompiuterio vagystė, į sąrašą gali būti įtrauktos tokios saugos priemonės: apsauginikas, didelis šuo, vaizdo kamera, durų užraktai arba tiekėjų, galinčių pasiūlyti naują kompiuterį vietoj pavogtojo, sąrašas. Dauguma grupės narių, suvokdami bendrąjį kaštų lygį, nuspręs, kad totalus sprendimas nėra tinkamas. Reikia nuspręsti, kuri iš likusių saugos priemonių geriausiai tiks organizacijai?

6.3.3 lentelė

MATRICA SU SIŪLOMAIS SPRENDIMAIS

	Vientisumas	**Konfidencialumas**	**Prieinamumas**
Nesąmoningi veiksmai	• Duomenų įvedimo kontrolė • Lentelės patikrinimas • Kontrolė ir sulyginimas	• Prieigos kontrolė • Funkcijų atskyrimas • Fizinė apsauga	• Atsarginės duomenų kopijos • Sistemos dizainas • Rezervinės duomenų linijos
Sąmoningi veiksmai	• Slaptažodžiai • Registracija, jungiantis prie sistemos	• Slaptažodžiai • Registracija, jungiantis prie sistemos • Duomenų laikmenų naikinimas • Saugos procedūros	• Atsarginių kopijų panaudojimas • Veiklos tęstinumo planavimas • Fizinė apsauga

Siekiant užkirsti kelią rizikai arba sumažinti ją iki priimtino lygio, būtina įdiegti informacijos saugos priemones. Dažnai viena saugos priemonių apsaugo nuo kelių pavojų ir atvirkščiai – vienos rizikos prevencijai gali būti panaudotos kelios saugos priemonės.

Dokumentacija

Baigus grupės darbą, turi būti parengti dokumentai, detaliai nusakantys analizės rezultatus ir siūlantys parengti veiksmų planą. Dokumentuose turi atsispindėti šie klausimai:

- *Įgyvendinamumo tyrimas*
- *Rizikos analizės procedūra:* turi būti paaiškinta specifinė rizika, kylanti organizacijos vertybei, įskaitant:
  - duomenų vientisumą;
  - duomenų konfidencialumą;
  - duomenų prieinamumą.
- *Turi būti paaiškinta, kurioms sistemos dalims reikėtų taikyti saugos priemones.*
- *Turi būti paaiškinta, kokios priemonės turėtų būti taikomos, kodėl, kur ir kada.*

Turi būti pateiktas nekontroliuojamų procesų paaiškinimas – atvejai, kai reikia prisiimti riziką, arba kai neįmanoma pritaikyti saugos priemonių.

Rizikos analizės procesas negali išspręsti visų problemų. Rizika, kurios valdyti neįmanoma, arba priemonės, kurių organizacija negali taikyti, turi būti užfiksuotos dokumentuose ir pateiktos vadovybei.

Kartais gali kilti konfliktas tarp veiklos reikmių ir saugos reikalavimų. Konfliktą ne visada pavyksta išspręsti saugos reikalavimų

naudai, tačiau vadovybė turi būti pasirengusi prisiimti potencialią riziką.

Kiekybinė rizikos analizė – tai procesas, leidžiantis organizacijai įvertinti matomus ir slaptus pavojus, kylančius jos vertybėms. Procesas užtikrina logišką ir nuoseklią rizikos bei jos poveikio vertybėms analizę ir įvertinimą.

Kuruojamas rizikos analizės procesas (KURAP)

Dauguma organizacijų bando susidoroti su tokiomis pačiomis rizikos rūšimis, kaip ir kitos organizacijos. Keičiantis veiklos kultūrai, sėkmingai veikiančioms saugos grupėms teko modifikuoti rizikos analizės procesą, siekiant įvertinti naujas grėsmes, kylančias profiliuotoje elektroninės veiklos aplinkoje.

Tačiau netgi kintant akcentams, šiandienos organizacijoms tenka saugoti savo informacinių išteklių, nuo kurių jos priklauso, vientisumą, konfidencialumą ir prieinamumą. Saugos programa turi talkinti veiklos padaliniams, padėti apsaugoti organizacijos vertybes ir užtikrinti aukštą paslaugų kokybę.

Kuruojamo rizikos analizės proceso (KURAP) apžvalga

Kuruojamas rizikos analizės procesas (KURAP) buvo sukurtas kaip efektyvus ir struktūriškas procesas, užtikrinantis, kad veiklos operacijoms kylantys pavojai, susiję su informacijos sauga, bus įvertinti ir aprašyti. Proceso metu vienu kartu analizuojama tik viena sistema, programa arba veiklos operacijų segmentas, o analizę atlieka grupė, į kurią įtraukiami veiklos vadovai, susipažinę su veiklos informacijos saugos reikmėmis, ir technikos specialistai, gerai išmanantys pažeidžiamas sistemų vietas bei atitinkamas

kontrolės priemones. Grupės posėdžiams, kurių darbotvarkė standartinė, vadovauja projektų padalinio arba informacijos saugos padalinio specialistas. Šis asmuo privalo užtikrinti, kad grupės nariai dirbtų efektyviai ir laikytųsi darbotvarkės.

Posėdžių metu rengiamos grupės „idėjų vėtros“ (angl. *brainstorming*), siekiant identifikuoti potencialias grėsmes, pažeidžiamumus ir jų sąlygojamą neigiamą poveikį duomenų vientisumui, konfidencialumui ir prieinamumui. Tuomet grupė turi išanalizuoti tokio poveikio pasekmes veiklai ir suklasifikuoti riziką pagal jos pirmumą. Paprastai grupė nesistengia konkrečiai įvertinti nei tikimybės, nei tikėtino metinio nuostolio, nebent tokiam įvertinimui jau būtų duomenų. Vietoj to grupė pasikliauja bendro pobūdžio grėsmių ir pažeidžiamumų duomenimis, gautais iš nacionalinių reagavimo į įvykius centrų, profesinių asociacijų, literatūros arba žinomais iš patirties.

Organizuojant grupę, jos narių patirtis rodydavo, kad atlikti tikslią kiekybinę rizikos analizę būtų nerentabilu, kadangi:

- Skaičiavimai užima labai daug laiko, taip pat reikia labai daug pastangų vertėms identifikuoti ir patikrinti;
- Rizikos dokumentų apimtis labai padidėja, jie tampa nepraktiški.
- Norint nustatyti saugos priemonių reikalingumą, konkrečių nuostolių apskaičiavimai paprastai nėra reikalingi.

Nustačius riziką ir suskirsčiusi ją pagal kategorijas, grupė privalo nustatyti saugos priemones, kurios turėtų būti įdiegtos rizikai sumažinti, orientuodamasi į rentabiliausias priemones. Skirtingai negu atliekant „30 minučių“ rizikos analizę, grupės pradės nuo 26 įprastinės saugos priemonių, apsaugančių nuo įvairių

rizikos rūšių. Aišku, sprendimą, kokios priemonės reikalingos, priima veiklos vadovai, atsižvelgdami į informacinių vertybių pobūdį, jų reikšmę veiklos operacijoms ir saugos priemonių kaštus.

Grupės išvados dėl rizikos rūšių, pirmumo ir konkrečių saugos priemonių reikalingumo turi būti aprašytos ir perduotos projekto vadovui bei veiklos vadovui, kad jie galėtų sudaryti galutinį veiksmų planą. Saugos profesionalai gali padėti veiklos padalinių vadovams nustatyti, kurios saugos priemonės būtų rentabiliausios ir geriausiai atitiktų jų veiklos reikmes. Parinkę saugos priemonę kiekvienai rizikos rūšiai arba priėmę grėsmę kaip natūralią veiklos riziką, svarstyme dalyvavę aukščiausieji veiklos vadovai ir techniniai specialistai turi pasirašyti galutinį dokumentą. Dokumentas ir visi su juo susiję raštai perduodami veiklos proceso valdytojui ir saugomi pagal dokumentų saugojimo tvarkos nurodytą laiką (paprastai septynerius metus).

Kiekviena rizikos analizės procedūra suskirstoma į keturias atskiras sesijas:

1. Parengtinis KURAP posėdis trunka maždaug valandą. Jame dalyvauja veiklos vadovas, projekto vadovas ir kuratorius.
2. KURAP posėdis trunka maždaug keturias valandas, jame dalyvauja nuo 7 iki 15 žmonių, nors pasitaikydavo, kai posėdyje dalyvaudavo tik 4 žmonės arba net 50 žmonių.
3. KURAP analizė ir ataskaitos parengimas paprastai trunka nuo 4 iki 6 dienų, jas galutinai apiformina kuratorius ir posėdžius protokolavęs asmuo.
4. Baigiamasis KURAP posėdis trunka maždaug valandą. Jame dalyvauja tie patys asmenys, kaip ir parengiamajame KURAP posėdyje.

Toliau šiame skyriuje bus paaiškinta, kodėl buvo sukurtas KURAP, kokie darbai atliekami kiekviename iš keturių etapų, ir kokie būna kiekvieno etapo rezultatai.

KURAP poreikis

Prieš sukuriant KURAP, rizikos analizė dažnai būdavo laikoma grandioziniu projektu, kurį norint įgyvendinti organizacijai būtina samdytis konsultantą iš šalies, ir kuris gali užtrukti labai ilgai. Dažnai rizikos analizės procesas trukdavo kelias savaites ir reikalaudavo atskiros biudžeto eilutės. Organizacija, samdydama konsultantus iš šalies, dažnai neįvertindavo savų specialistų kompetencijos, todėl gauti rezultatai dažnai būdavo nepriimtini veiklos padalinių vadovams, jie nesuprasdavo rekomenduojamų saugos priemonių, nenorėdavo jų taikyti ir tokiu būdu neretai sužlugdydavo visą diegimo procesą.

Buvo reikalingas toks rizikos analizės procesas, kurį įgyvendinti galėtų patys veiklos vadovai, kuris truktų kelias dienas, o ne savaites ir mėnesius, būtų rentabilus ir panaudotų pačios organizacijos specialistus. KURAP atitinka visus šiuos reikalavimus, be to, jį atliekantis asmuo neturi būti konkrečių sistemų arba veiklos procesų specialistas – procesui įgyvendinti reikia gerų vedėjo įgūdžių.

KURAP yra formalus metodas, sukurtas išanalizavus ankstesnius kokybinės rizikos procesus ir modifikavus juos taip, kad jie atitiktų iškeltus reikalavimus. Procesui vadovauja įmonės veiklos vadovai, ir tai užtikrina, kad pasirinktos saugos priemonės atitiks veiklos procesų reikmes ir uždavinius. Dėl tokių dalykų, kaip sauga arba audito reikalavimai, paprastai nediskutuojama. KURAP orientuojasi į veiklos reikmes ir tokiam procesui skiriamo laiko ribotumą.

KURAP įtraukia į procesą veiklos padalinius ir naudoja juos rizikai bei grėsmėms nustatyti. Kadangi išteklių valdytojai įtrau-

kiami į grėsmių nustatymo procesą, paprastai jie sutinka diegti rentabilias saugos priemones ir ieško specialistų pagalbos. KURAP leidžia veiklos padaliniams kontroliuoti savo išteklius, todėl jie gali nustatyti, kokių saugos priemonių reikia, ir kas bus atsakingas už jų įdiegimą.

KURAP rezultatas yra išsamus dokumentas, nustatantis grėsmes, grėsmių pirmumą ir saugos priemones, leidžiančias jas sušvelninti. Jis pateikia įmonei ekonomiškai rentabilų veiksmų planą, atitinkantį veiklos reikmes ir užtikrinantį įmonės išteklių saugą. Svarbiausia, kad įraukdamas į procesą veiklos vadovus, KURAP sukuria veiksmų planu tikinčių ir jį palaikančių valdytojų arba klientų grupę.

KURAP įgyvendinimas įstaigoje

Prieš pradedanti KURAP, būtina paaiškinti, kas tai per procesas ir kaip jis vykdomas. To reikės kelis pirmuosius proceso įgyvendinimo įstaigoje mėnesius. Siekiant palengvinti šį procesą, galima rengti apžvalgines KURAP sesijas. Sesijas geriausiai tiktų surengti programinės įrangos ir sistemų plėtojimo grupėms, o vėliau į procesą turėtų būti įtraukti ir veiklos padaliniai.

KURAP reikia „parduoti“ veiklos bendruomenei. Pasinaudokite jau išdėstytais argumentais, taip pat paaiškinkite, kad šis ekonomine prasme efektyvus procesas leidžia veiklos padaliniams patiems kurti savo likimą. KURAP įgyvendinamas, siekiant padėti įmonei vykdyti savo veiklos uždavinius, o rizikos analizės proceso įdiegimas – tai kaina, kurią tenka mokėti už veiklą šiandienėje aplinkoje.

Svarbu tai, kad procesu padedama nustatyti veiklos riziką. Grėsmės suklasifikuojamos į nepageidautinus arba neleistinus įvykius ne pagal jų poveikį saugos arba audito reikalavimams, bet pagal poveikį įstaigos veiklos uždavinių ir jos tikslo įgyvendinimui.

Būtina užtikrinti, kad visi darbuotojai suprastų svarbiausias KURAP procesui vartojamas sąvokas. Vėliau bus pateikta daugiau sąvokų, bet iš pradžių būtina įsitikinti, kad darbuotojai gerai supranta penkias svarbiausias:

1. Rizika – potencialus įvykis, galintis turėti neigiamą poveikį įmonės veiklos uždavinių ar jos tikslo įgyvendinimui;
2. Saugos priemone siekiama išvengti įvykio, nustatyti jį, sumažinti jo poveikį arba atsigauti po jo, saugant įmonės veiklos procesus arba jos misiją;
3. Vientisumas – pirminio pavidalo informacija, be neleistinų arba nepageidautinų pakeitimų ar pažeidimų;
4. Konfidencialumas – informacijos sauga nuo neleistino arba nepageidautino atskleidimo;
5. Prieinamumas – iškilus poreikiui, programos, sistemos ir (arba) informaciniai ištekliai turi būti prieinami.

KURAP uždavinys identifikuoti potencialius nepageidautinus arba neleistinus įvykius, kurie galėtų neigiamai paveikti įmonės veiklos uždavinių arba tikslo įgyvendinimą. Nustačius tokių įvykių riziką ir jos pirmumą, būtina nustatyti saugos priemones, kurios leistų sumažinti rizikos lygį.

Grupė turi išnagrinėti visus pavojus, kylančius tiek dėl sąmoningų, tiek dėl nesąmoningų veiksmų. Kuratorius turi padėti grupei, pateikdamas orientacinius klausimus. Pasistenkite padėti grupei įvertinti kitus rizikos šaltinius. „Ką jūs galvojate apie tai?“ arba „Kas atsitiktų, jeigu?..“

Parengtinis KURAP posėdis

Parengtinis KURAP posėdis turi lemiamos reikšmės viso proceso sėkmei. Paprastai posėdis trunka apie valandą. Posėdyje tu-

rėtų dalyvauti veiklos vadovas (atstovas), projekto vadovas ir kuratorius. Posėdžio metu turi būti apsvarstyti penki klausimai:

1. *Apimties apibrėžimas.* Projekto vadovas ir veiklos vadovas turi raštu išdėstyti analizės apimtis, t. y. suformuluoti, kas tiksliai turėtų būti nagrinėjama. Apimties apibrėžimas buvo aptartas 6.1 skyriuje. Turėtų būti orientuojamasi į jo turinį;
2. *Vizualinis modelis.* Reikalingas vizualinis modelis – dideliame popieriaus lape arba skaidrėse pateikta analizuotino proceso schema. Vizualinis modelis naudojamas KURAP posėdžių metu, kad grupė galėtų matyti, kur prasideda ir kur baigiasi procesas;
3. *KURAP grupės sukūrimas.* Paprastai KURAP grupė sudaroma iš 7–15 narių. Į ją įtraukiami atstovai iš organizacijos veiklos ir jos pagalbinių padalinių. KURAP grupės sudėtis aptariama toliau šiame skyriuje;
4. *Posėdžių tvarka.* Tai veiklos padalinių vadovų susirinkimas, todėl reikalingas asmuo, kuris parūpintų patalpas, sudarytų darbotvarkę ir gautų reikalingas priemones (projektorių, didelius popieriaus lapus, taip pat kavą ir pyragaičius);
5. *Susitarimas dėl sąvokų.* Parengtiniame KURAP posėdyje turi būti susitarta dėl sąvokų interpretavimo ir užfiksuoti analizės elementų (vientisumo, konfidencialumo, prieinamumo) apibrėžimai.

Taip pat būtina susitarti dėl tokių sąvokų kaip:

a) rizika,
b) saugos priemonė,
c) poveikis,
d) pažeidžiamumas.

Parengtinio KURAP posėdžio metu labai svarbu aptarti grėsmių pirmumo nustatymo procesą. Yra dvi šio proceso įgyvendinimo „mokyklos“.

Pirmoji siūlo KURAP grupei išnagrinėti nustatytas grėsmes, teigiant, kad nėra įdiegtų saugos priemonių. Tai leidžia sudaryti „idealių“ saugos priemonių komplektą, nes KURAP gali pamatyti spragas tarp to, kas yra, ir to, kas turi būti.

Antroji įvertina grėsmes kartu su įdiegtomis saugos priemonėmis. Šiuo atveju svarbiausia – vertybė. Išskiriamos trys informacijos saugos proceso fazės:

1. *Rizikos analizė* – įvertinama egzistuojanti aplinka, nustatomos grėsmės, jų pirmumas ir siūlomos saugos priemonės;
2. *Saugos priemonių įdiegimas* – pasirenkamos ir įdiegiamos tos saugos priemonės, kurios geriausiai atitinka veiklos reikmes;
3. *Saugos analizė* – peržiūrimos įdiegtos saugos priemonės ir įvertinamas jų efektyvumas.

KURAP grupė

Parengtinio KURAP posėdžio metu veiklos vadovas ir projekto vadovas turi nustatyti, kad dalyvaus tolesniuose KURAP posėdžiuose. Idealus dalyvių skaičius – nuo 7 iki 15. Į KURAP procesą rekomenduojama įtraukti:

- funkcijos valdytoją;
- sistemos vartotojus;
- sistemos administratorių;
- sistemos analitikus;
- sistemos programuotoją;
- taikomųjų programų kūrėją;
- duomenų bazės administratorių;
- informacijos saugos įgaliotinį;

- fizinės saugos specialistą;
- ryšių specialistą;
- tinklo administratorių;
- paslaugų tiekėją;
- auditorių (jeigu reikia);
- teisininką (jeigu reikia);
- personalo skyriaus atstovą (jeigu reikia);
- asmenį, atsakingą už darbo santykius (jeigu reikia).

Griežtų dalyvių parinkimo taisyklių nėra, bet siekiant proceso veiksmingumo, į KURAP būtina įtraukti *funkcinį veiklos vadovą* ir *sistemos vartotojus*. Kadangi bus analizuojamas būtent jų veiklos procesas, labai svarbu, kad jie dalyvautų analizėje.

„Sistemų (-ų)“ grupės atstovas taip pat yra labai svarbus KURAP grupės narys. *Sistemos administratorius* paprastai būna susipažinęs su naujomis programomis arba sistemomis, ir su problema susidūrę vartotojai kreipiasi būtent į jį.

Sistemos analitikų grupę sudaro žmonės, gerai išmanantys tiek nagrinėjamą veiklą, tiek informacines sistemas. Tai labai svarbu, siekiant užtikrinti tarpusavio supratimą KURAP posėdžių metu.

Sistemų programavimo grupę sudaro darbuotojai, užtikrinantys sistemų funkcionavimą, einamąjį darbą ir tinkamą jų konfigūraciją.

Taikomojo programavimo grupę sudaro asmenys, galintys sukurti naują programą arba pritaikyti jau įdiegtą programą, arba trečiųjų šalių programinę įrangą funkcinėms organizacijos reikmėms.

Duomenų bazės administratoriai – tai technikai, suprantantys duomenų bazės veikimą ir dažnai atsakantys už tinkamą duomenų bazės saugos mechanizmų funkcionavimą.

Informacijos saugos grupė taip pat privalo deleguoti savo atstovą į KURAP grupę. Dažnai KURAP kuruoja už informacijos

saugą atsakingas darbuotojas, vis dėlto tai gali sukelti interesų konfliktą, o kuratorius turėtų būti neutralus.

Fizinės saugos grupė (arba pastato eksploatavimo atstovas) būtinai turi būti įtrauktas į grupę. Tai leis geriau perprasti fizinių veiksnių keliamas grėsmes.

Jeigu nagrinėjama vertybė jungiama prie vietinio kompiuterių tinklo arba kitos *ryšių įrangos*, į grupę būtina įtraukti šių sričių atstovus.

Jeigu analizuojamos internetinės programos, būtinai reikės atstovo iš interneto palaikymą užtikrinančios organizacijos, taip pat tinklapio ir ugniasienės administratorių.

Likę keturi atstovai pažymėti pastaba „jei reikia". *Auditoriai* yra darbuotojai, galintys pasiūlyti gerų minčių, tačiau dažnai jie prieštarauja laisvam informacijos judėjimui. Išskyrus atvejus, kai santykiai su auditoriais yra išskirtinai geri, rekomenduojame neįtraukti jų į KURAP grupę. Auditoriai turėtų būti supažindinami su KURAP rezultatais vėliau, kad galėtų jais pasinaudoti, atlikdami išteklių auditą.

Teisininkai paprastai būna pernelyg užsiėmę, kad dalyvautų kiekviename KURAP grupės posėdyje. Tačiau jeigu aptariami ištekliai organizacijai labai reikšmingi, naudinga būtų įtraukti į grupę ir teisės skyriaus atstovą. Autorius rekomenduoja KURAP aptarti su teisininkais atskirame posėdyje ir nustatyti, kada juos reikėtų įtraukti į procesą, norint apsvarstyti specifines rizikos rūšis.

Jeigu aptariami ištekliai veikia darbo sąlygas, į KURAP grupę rekomenduotina įtraukti *Personalo skyriaus* ir *Darbo santykių* atstovą (jeigu įstaigoje veikia profesinės sąjungos).

Šis sąrašas nėra baigtinis ir nebūtinai pateikia geriausią atstovų derinį, ypač jeigu KURAP nutolsta nuo tradicinės informa-

cijos saugos rizikos analizės. Šiuo atveju svarbiausia suprasti, kad norint užtikrinti sėkmingą KURAP, jai turi atstovauti kuo daugiau padalinių.

KURAP kuratorius

KURAP kuravimas reikalauja specifinių įgūdžių. Šiuos įgūdžius galima įgyti ir ištobulinti specialiuose kursuose, taip pat dirbant praktinį darbą. Reikalingi įgūdžiai yra mokėjimas:

- *Klausytis:* reikia mokėti reaguoti į dalyvių žodžius ir gestus, perfrazuoti pasisakymus apie analizės objektą ir aiškiau pateikti atsakymus;
- *Vadovauti:* skatinti KURAP grupės darbą ir vidinę diskusiją, bet tuo pačiu neleisti grupei nukrypti nuo svarstomos temos;
- *Reflektuoti:* persakyti mintis naujais žodžiais ir sudėlioti akcentus;
- *Apibendrinti:* sugebėti sujungti į vieną atskiras temas ir mintis;
- *Gretinti:* sugebėti sugretinti skirtingas nuomones, nuoširdžiai priimti grupės pastabas, atremti aštrius komentarus ir paversti juos pozityviais pasisakymais;
- *Remti:* sukurti pasitikėjimo ir pakantumo atmosferą;
- *Įsiterpti krizės atveju:* padėti išplėsti pateiktą alternatyvų arba galimybių viziją ir imtis veiksmų konfliktams ir krizėms išspręsti;
- *Valdyti:* padėti grupės nariams priimti kitokius požiūrius ir skatinti visus drąsiai pasisakyti ir dalyvauti;
- *Spręsti problemas:* surinkti informaciją apie svarstomus klausimus ir padėti grupei efektyviai įvardyti uždavinius.
- *Keisti elgesį:* pastebėti tuos grupės narius, kuriems sunku įsitraukti į procesą, ir paskatinti juos aktyviau dalyvauti.

Norint sėkmingai atlikti KURAP, būtina laikytis esminių kuravimo taisyklių. KURAP vadovas privalo:

1. Atidžiai sekti, ką sako ir daro kiekvienas grupės narys;
2. Vertinti visas nuomones ir skatinti dalyvavimą;
3. Atkreipti dėmesį į nežodines reakcijas;
4. Niekada nepamokslauti, klausytis ir įtraukti dalyvius į diskusiją;
5. Niekada nenukrypti nuo tiesioginio tikslo;
6. Išlikti neutralus (arba visada atrodyti neutralus);
7. Išmokti pakęsti priešiškumą, pačiam netampant priešišku;
8. Vengti būti „ekspertu“. Kuratoriaus vaidmuo apsiriboja klausymusi, klausimų pateikimu, proceso skatinimu ir alternatyvų siūlymu;
9. Laikytis reglamento ir būti punktualus;
10. Naudoti pertraukas diskusijai palengvinti;
11. Būti pasirengęs padėti KURAP grupei;
12. Sustabdyti KURAP susitikimą, jeigu grupė yra vangi arba sunkiai kontroliuojama.

KURAP kuratorius privalo turėti nuosavą KURAP priemonių komplektą. Jame turi būti:

- dideli popieriaus lapai;
- žymėjimo juostelė ir smeigtukai;
- žymekliai/flomasteriai;
- kortelės;
- sesijos taisyklės.

Sesijos tvarka buvo sukurta prieš keliolika metų, ir vienas iš metodo autoriaus vadovaujamos grupės narių jas įrėmino ir pakabino KURAP posėdžių kambaryje. Taisyklės tokios:

- ✔ *Dalyvauja visi:* kas nors stebės, kaip ši taisyklė vykdoma KURAP proceso metu;

- *Kiekvienas dirba savo darbą:* kuratorius kuruoja, sekretorius protokoluoja, visi kiti – dalyvauja.
- *Visi laikosi darbotvarkės/nustatytos temos:* analizės apimtis ir jos vizualinis atvaizdavimas turi būti atspausdintas ir išdalytas visiems dalyviams.
- *Visos idėjos yra vienodai vertingos:* nors George Orwell sakė „visi gyvuliai lygūs, bet kai kurie lygesni už kitus“, šiuo atveju turi būti užtikrinta tikra lygybė.
- *Kiekvienas privalo išklausyti kito nuomonę:* priverskite grupę klausytis kiekvieno pasisakančiojo, ne tik laukti savo eilės.
- *Jokių „plumpsėjimų“ (nereikalingų garsų), viskas užrašinėjama*: šį terminą pasiūlė Jack Durner iš Mendon grupės, pastebėjęs, kad ant grindų vis kas nors numetama.
- *Nukrypimai nuo temos užrašinėjami:* jeigu pasisakymas nukrypsta nuo svarstomos temos, jis įtraukiamas į nukrypimų sąrašą, ir skiriamas asmuo klausimui išsiaiškinti.
- *Užrašykite idėją, prieš pradėdami jos svarstymą:* užrašykite ją ant didelio popieriaus lapo.
- *Padėkite sekretoriui užprotokoluoti visus klausimus:* priminkite sekretoriui, kad įtrauktų į protokolą tai, kas užrašyta dideliuose popieriaus lapuose.
- *Vienu metu šneka tik vienas:* čia bus patikrinti kuratoriaus įgūdžiai.
- *Vienu metu pykti gali tik vienas:* autorius dažniausiai būna savanoris.
- *Taikoma 3–5 minučių taisyklė:* visos diskusijos turi vykti pagal nustatytą reglamentą.

- *Kiekvienas turi būti*:
  - operatyvus,
  - sąžiningas,
  - malonus,
  - kūrybingas.
- Mėgautis procesu.

KURAP posėdis

KURAP posėdis paprastai planuojamas keturioms valandoms. Kai kurios organizacijos pratęsdavo posėdį iki trijų dienų, bet paprastai, atsižvelgiant į darbuotojų užimtumą ir siekiant užtikrinti KURAP efektyvumą, nustatomas keturių valandų limitas. KURAP posėdį galima suskirstyti į tris atskirus posėdžius pagal devynis elementus ir tris rezultatų grupes.

Pradžioje KURAP grupės dalyviai prisistato vieni kitiems, nurodydami savo vardą, pavardę, pareigas, skyrių ir telefono numerį (sekretorius tai turi užprotokoluoti). Turi būti nustatyti ir aptarti dalyvių vaidmenys KURAP grupėje. Paprastai būna penketas vaidmenų:

1. Valdytojas,
2. Projekto vadovas,
3. Kuratorius,
4. Sekretorius,
5. Grupės narys (nariai).

Po to KURAP grupės nariams pateikiama proceso, kuriame jie dalyvaus, apžvalga. Jiems taip pat pristatomas dokumentas dėl proceso apimties, o po to kuris nors iš techninės grupės pateikia penkių minučių trukmės nagrinėjamo proceso apžvalgą (vizualinį modelį). Galiausiai turi būti pristatytos sąvokos; jų egzempliorius turi būti įteiktas kiekvienam grupės nariui.

Po įvadinės dalies reikia surengti KURAP grupės „idėjų vėtrą“ (žr. 6.5.1 pav.). Tai antrasis proceso etapas, kuriame turi būti apsvarstyti visi analizės elementai (vientisumas, konfidencialumas ir prieinamumas), taip pat nustatyta su kiekvienu elementu susijusi rizika, grėsmės, problemos ir kiti klausimai.

„Idėjų vėtros“ proceso metu kuratorius turi pateikti rizikos apibrėžimą ir keletą praktinių pavyzdžių. Tuomet grupei duodamos trys minutės užrašyti jiems rūpimas grėsmes. Kuratorius turi apeiti posėdžių kambarį ir surinkti po vieną grėsmės aprašymą iš kiekvieno grupės nario. Dauguma bus užrašę daugiau nei vieną grėsmę, tačiau reikia paimti tik vieną ir eiti prie kito žmogaus. Tokiu būdu užtikrinamas kiekvieno nario dalyvavimas. Procesas tęsiamas tol, kol grupė daugiau nebegalės sugalvoti naujų grėsmių.

Grėsmių pavyzdžiai (sąrašas nėra baigtinis)

Grėsmės konfidencialumui

– neleistinas prisijungimas,
– neleistinas atskleidimas,
– sandorių sekimas arba stebėsena,
– kopijavimas, neturint tam leidimo,
– paketų perėmimas tinkle,
– konfidenciali informacija tapo prieinama rangovui.

Apibrėžimas:

Konfidencialumas – informacijos apsauga nuo neleistino arba nepageidautino atskleidimo.

6.5.1 pav. Apibrėžimas „idėjų vėtros“ sesijai ir grėsmių pavyzdžiai.

„Idėjų vėtros“ sesija tęsiama tol, kol bus baigta visų elementų apžvalga. Baigus šį procesą, rekomenduojama grupei surengti kavos pertraukėlę. Kai grupės nariai grįš atgal į posėdžių kambarį, pateikite jiems grėsmių apžvalgą, o lapus, kuriuose surašytos grėsmės, pakabinkite ant sienos. Tuomet nuimkite besidubliuojančias grėsmes ir, jeigu reikia, paredaguokite likusias.

Baigus šį procesą (skirkite jam 10–15 minučių), grupė turi susikoncentruoti ir nustatyti grėsmių pirmumą. Tai atliekama, nustatant galimą žalą organizacijai, jos tikimybę ir įtaką. Apibrėžimai, suderinti parengtinio KURAP posėdžio metu, pateikiami grupei iš pradžių. Įprastinis apibrėžimų sąrašas gali atrodyti taip:

- *Didelis pažeidžiamumas:* egzistuoja esminis sistemos arba operacinių procedūrų pažeidžiamumas. Jeigu jo poveikio veiklai potencialas yra didelis arba esmingai reikšmingas, būtina įdiegti saugos priemones.
- *Vidutinis pažeidžiamumas:* yra tam tikrų trūkumų. Jeigu jų poveikio veiklai potencialas yra didelis arba esmingai reikšmingas, saugos priemonės turi būti patobulintos.
- *Mažas pažeidžiamumas:* sistema sukonstruota gerai ir veikia tinkamai. Papildomos saugos priemonės rizikai sumažinti nereikalingos.
- *Esminis poveikis (didelis):* gali sužlugdyti įmonės veiklą arba rimtai pakenkti jos veiklos perspektyvoms ir plėtrai.
- *Rimtas poveikis (vidutinis):* sąlygoja didelę žalą ir išlaidas, bet neturi esminės reikšmės įmonės egzistavimui.
- *Nedidelis poveikis (mažas):* einamasis poveikis, kuris yra tikėtinas, pašalinamas įprastinės veiklos metu.

Grupė gali naudotis prioritetų modeliu, pateiktu 6.5.2 pav.

Pasirinktas laukelis atitinka raide įvertintą rizikos pirmumą. KURAP grupė turi suskirstyti grėsmes tokia tvarka:

- A – korekciniai veiksmai būtini,
- B – korekciniai veiksmai pageidautini,
- C – būtina stebėsena,
- D – nereikia imtis jokių veiksmų.

Yra keletas būdų, kuriuos pasitelkusi grupė gali nustatyti rizikos pirmumą. Trys populiariausi yra šie:

1. Kuratorius pristato grėsmes vieną po kitos, o grupė aptaria kiekvieną iš jų ir bendru susitarimu nustato pirmumą.
2. Kuratorius pristato pirmąsias tris keturias grėsmes, įsitikina, kad grupė suprato, kaip veikia procesas, o tada duoda kiekvienam grupės nariui spalvotą žymeklį ir paprašo pažymėti pirmumą. Jeigu grėsmė jau įvertinta, jie turi pereiti prie kitos grėsmės. Grupei baigus darbą, kuratorius jį apibendrina, o jeigu kyla nesutarimų – pradeda diskusiją. Pvz., KURAP grupėje yra 15 narių, 10 iš jų įvertina grėsmę „C“ raide, o 5 – „A“ arba „B“. Kuratorius turi pradėti aptarimą ir įsitikinti, kad „C“ tikrai yra tinkamiausias įvertinimas.
3. Trečiasis galimas metodas yra toks: kuratorius duoda kiekvienam grupės nariui dešimt lipnių žymeklių. Kiekvienas grupės narys gali pažymėti dešimt svarbiausių grėsmių. Žymekliais pažymėtoms grėsmėms bus taikomos saugos priemonės, o nepažymėtos grėsmės bus laikomos nereikšmingomis.

		Poveikis veiklai		
		Didelis	Vidutinis	Mažas
Pažeidžiamumas	Didelis	A	B	C
	Vidutinis	B	B	C
	Mažas	C	C	D

6.5.2 pav. Prioritetų matricos pavyzdys.

KURAP posėdžio metu parengiama:

- rizikos identifikacija;
- rizikos prioritetai;
- siūlomos saugos priemonės nuo didžiausių arba prioritetinių grėsmių.

6.5.1 lentelėje dviguba linija apibrėžtuose laukuose buvo pateikta apie 120 grėsmių, nustatytų KURAP metu. Svarbiausios 6.5.1 lentelės sąvokos tokios:

Grėsmė = faktinė grėsmė, kurią pažymėjo KURAP grupės nariai (paryškintame laukelyje);

Tipas = grėsmė vientisumui, konfidencialumui arba prieinamumui;

Prioritetas = pirmumo lygis A, B, C arba D (paryškinta);

Saugos priemonės = saugos priemonės, padedančios sušvelninti riziką.

6.5.1 lentelė

KURAP POSĖDŽIO REZULTATAI

Grėsmės Nr.	Grėsmė	Tipas	Prioritetas	Saugos priemonės
1	Personalas, kuriam nenumatytos prieigos prie informacijos, bet ją gauna	INT	B	3, 5, 6, 11, 12,16
2	Neaiškios arba neegzistuojančios informacijos versijos	INT	B	9, 13, 26
3	Duomenų bazė gali būti sugadinta dėl technikos gedimo arba netinkamos ar nekokybiškos programinės įrangos	INT	D	
4	Duomenys gali būti sugadinti nevisiško perdavimo atveju	INT	C	
5	Galimybė pakeisti duomenis tranzito metu, o po to panaikinti pakeitimą jį nuslepiant	INT	C	
6	Nepranešama apie vientisumo pažeidimus	INT	A	7, 11, 12, 13, 20, 21
7	Netinkamai atlikta arba neatlikta procedūra gali sugadinti duomenis	INT	B	1, 2, 12, 13, 14, 15, 18, 20, 21, 25
8	Vidaus procedūrų, reglamentuojančių duomenų kūrimą, kontrolę, valdymą ir apsikeitimą tarp padalinių, trūkumas	INT	A	7, 13, 17, 20, 23, 25
9	Nepranešama apie vientisumo problemas	INT	A	7, 13, 26
10	Netinkamas informacijos panaudojimas	INT	B	11,12,19
11	Trečiosios šalies informacija gali turėti vientisumo problemų	INT	B	7, 13, 26
12	Trečioji šalis gauna prieigą prie informacijos	INT	A	3,4,5

Paskutinis KURAP posėdžio etapas yra saugos priemonių, taikytinų grėsmėms, kurioms jos būtinos, nustatymas. Siųsdamas kvietimą į KURAP posėdį, veiklos vadovas pridėjo 26-ių saugos priemonių, kurias buvo numatyta svarstyti posėdyje, sąrašą, pateiktą 6.5.2 lentelėje. Saugos priemonių sąrašas yra įtrauktas į KURAP medžiagą kaip „Excel“ išklotinės dalis. 26-ių saugos priemonių sąrašas buvo parengtas remiantis įvairių KURAP kuratorių per pastaruosius keletą metų surinktais saugos priemonių pavyzdžiais. Saugos priemonių sąrašas KURAP grupei yra tik pavyzdys, todėl, jei grupė pageidauja, jį galima modifikuoti ir papildyti. Jeigu posėdžio metu nusprendžiama sąrašą keisti, pakeitimai turi būti atlikti „Excel“ lentelėje „Saugos priemonės“.

6.5.2 lentelė

KURAP SAUGOS PRIEMONIŲ SĄRAŠAS

Priemonės numeris	Klasė	Saugos priemonės apibūdinimas
1	Atsarginė kopija	Atsarginių kopijų kūrimo reikalavimai bus nustatyti ir pateikti paslaugų tiekėjui, įskaitant reikalavimą atsiųsti elektroninį pranešimą sis-sistemos administratoriui, kad atsarginė duomenų kopija buvo padaryta. Paslaugų tiekėjas turės patikrinti atsarginio kopijavimo procedūras.
2	Atkūrimo planas	Sukurti, aprašyti ir patikrinti atkūrimo procedūras, užtikrinančias, kad praradimo atveju programinę įrangą ir informaciją bus galima atkurti, pasinaudojus atsarginėmis kopijomis.
3	Prieigos kontrolė	Įdiegti prieigos kontrolės mechanizmą, užkertantį kelią neteisėtam priėjimui prie informacijos. Šis mechanizmas turi apimti ir bandymų pralaužti informacijos saugą, nustatymą, registravimą ir ataskaitos apie juos pateikimą.

4	Prieigos kontrolė	Prieigos ribojimas: įdiegti mechanizmą, apribojantį prieigą prie konfidencialios informacijos logine ir fizine prasme.
5	Prieigos kontrolė	Įdiegti vartotojų autorizacijos mechanizmus (ugniasienes, prisijungimo telefono linija kontrolę, saugius ID), užtikrinant prieigą tik įgaliotam personalui.
6	Prieigos kontrolė	Įdiegti kodavimo mechanizmą (duomenų, galinio ryšio), užkertantį kelią neteisėtam duomenų perėmimui ir saugantį informacijos vientisumą ir konfidencialumą.
7	Programų kontrolė	Įdiegti programinės įrangos kontrolę (duomenų įvedimo patikra, laukeliai, kuriems reikalingas patvirtinimas, aliarmo indikatoriai, slaptažodžių galiojimo laikas, patikrų ataskaitos), užtikrinančią programinės įrangos duomenų vientisumą, konfidencialumą ir prieinamumą.
8	Testavimas priimant	Sukurti testavimo procedūras, kuriomis bus vadovaujamasi kuriant naujas arba keičiant jau egzistuojančias programas. Testavimo procedūrose turi būti numatytas vartotojų dalyvavimas, priimant programą.
9	Pokyčių valdymas	Taikyti pokyčių procesams sistemingą modifikacijų įvertinimo procedūrą, užtikrinančią, kad būtų laikomasi atitinkamų etapų ir atsargumo priemonių. Į šią procedūrą turi būtį įtrauktos ir modifikacijos, atliekamos skubos tvarka.
10	Antivirusinės priemonės	1) Pasirūpinti, kad kompiuterių tinklo administratorius visuose kompiuteriuose įdiegtų bendrovės standartus atitinkančias antivirusines programas. 2) Į organizacijos IP programą įtraukti švietimą ir supažindinimą su virusų prevencijos technologijomis.
11	Politika	Sukurti politiką ir procedūras, ribojančias prieigą ir suteikiančias teises tik tiems darbuotojams, kuriems reikia jų veiklai.

12	Mokymai	Vartototojų mokymų metu bus pateiktos aprašytos instrukcijos, kaip teisingai naudotis programa. Bus akcentuojama vartotojų registracijos ir slaptažodžių konfidencialumo, taip pat informacijos konfidencialumo svarba.
13	Auditas/ stebėsena	Įdiegti mechanizmus, užtikrinančius veiksmų, reikalaujančių nepriklausomo įvertinimo, stebėseną, pranešimą apie juos ir jų auditą, įskaitant periodišką vartotojų ID patikrinimą, siekiant užtikrinti ir įvertinti veiklos poreikius.
14	Atsarginės kopijos	Operacijų valdymas: bus rengiami sistemos administratorių mokymai, jų pareigos bus perskirstomos rotacine tvarka, tokiu būdu tikrinant mokymų programos adekvatumą.
15	Mokymai	Operacijų valdymas: programų kūrėjai turi pateikti dokumentaciją, instrukcijas ir suteikti pagalbą programų operatoriams (paslaugų tiekėjui), diegiant mechanizmus, užtikrinančius iš vienos programos į kitą persiunčiamų duomenų saugą.
16	Prieigos kontrolė	Operacijų valdymas: turi būti sukurti ir įdiegti mechanizmai, užkertantys kelią neteisėtiems prisijungimams prie duomenų bazės ir neleidžiantys modifikuoti joje esančių duomenų.
17	Sąsajų tarpusavio priklausomybė	Operacijų valdymas: bus identifikuota fiderinė sistema, ir apie ją bus pranešta paslaugų tiekėjui, akcentuojant, kokį poveikį funkcionavimui turėtų fiderinių programų veikimo sutrikimai.
18	Techninė priežiūra	Operacijų valdymas: bus nustatytas techninei profilaktikai reikalingas laikas ir pareikalauta, kad vadovybė jį suderintų, jeigu turima pakankamai patirties.
19	Mokymai	Vartotojų valdymas: įdiegti vartotojų programą (jų veiksmų įvertinimo programą), skatinančią laikytis nustatytos politikos bei procedūrų ir užtikrinančią tinkamą programinės įrangos naudojimą.

20	Paslaugų lygio sutartys	Sudaryti paslaugų lygio sutartis, reglamentuojančias vartotojų lūkesčių lygį ir paslaugų tiekėjų garantijas.
21	Techninė priežiūra	Sudaryti techninės priežiūros ir tiekėjo paslaugų sutartis, užtikrinančias nuolatinį programinės įrangos funkcionavimą.
22	Fizinė sauga	Kartu su infrastruktūros vadybininkais pasirūpinti, kad būtų įdiegtos fizinės saugos priemonės, garantuojančios sistemai reikalingos informacijos, programinės įrangos ir kompiuterinės technikos saugą.
23	Vadovybės parama	Pareikalauti vadovybės paramos, organizuojant tam tikrų veiklos padalinių bendradarbiavimą ir jų veiklos koordinavimą, kad būtų galima užtikrinti sklandų programinės įrangos diegimą.
24	Nuosavybės teisės	Nuosavybės teisių kontrolė
25	Koregavimo strategija	Strategijos grupė turi sukurti koregavimo strategijas, tokias kaip procesų atnaujinimas, programinės įrangos peržiūra ir t. t.
26	Pokyčių valdymas	Produktų šalinimo kontrolė, įskaitant programų paieškos ir šalinimo procedūras, užtikrinančias duomenų saugojimo laikmenų išvalymą.

Yra du pagrindiniai saugos priemonių nustatymo būdai:

- Kuratorius gali atskirai apsistoti ties kiekviena prioritetine grėsme ir paprašyti grupės išvardyti saugos priemones, kurios padėtų apsisaugoti nuo minėtosios grėsmės.
- Kuratorius gali išanalizuoti tris ar keturias pirmąsias prioritetines grėsmes, o po to leisti grupės nariams patiems pasirinkti riziką ir užrašyti jai taikytinas saugos priemones. Jeigu pasirinkta grėsmė jau aptarta, prie jos grįžti nereikia.

Grupė privalo suprasti, kad jos nurodytos saugos priemonės nebūtinai bus diegiamos. Pavyzdžiui, 6.5.1 lentelės septintojoje eilutėje buvo nurodytos devynios galimos saugos priemonės. Baigiamojo KURAP posėdžio metu veiklos vadovas, projekto vadovas ir kuratorius galės iš jų išrinkti vieną ar dvi labiausiai tinkančias.

KURAP grupė turi suprasti, kad renkantis saugos priemones būtina atsižvelgti į veiklos uždavinius. Bet kokia saugos ar kontrolės priemonė vienu ar kitu būdu daro įtaką veiklos procesams, kadangi priemonės diegimui panaudojami organizacijos ištekliai. Avarijos, klaidos ir praleidimai dažnai padaro daug daugiau žalos, negu sąmoningi veiksmai. Nė viena saugos priemonė negali garantuoti šimtaprocentinio saugumo. Svarbiausias tikslas užtikrinti priimtiną saugos lygį.

KURAP negali eliminuoti visų grėsmių. Vadovybės pareiga yra nustatyti, kokioms grėsmėms bus taikomos saugos priemonės, ir kokia rizika bus priimama. KURAP grupė tik padeda vadovybei priimti pagrįstus veiklos sprendimus.

KURAP posėdis baigiamas, parengus:

1 – grėsmių nustatymą;

2 – grėsmių prioritetus;

3 – saugos priemonių identifikaciją.

Baigiamasis KURAP posėdis

30 minučių rizikos analizė būtų netinkama, todėl KURAP koncepcijoje jai skiriamos keturios valandos. Kaip pastebėta, parengtinis KURAP posėdis paprastai trunka valandą, o pagrindinis – apie keturias. Šių dviejų posėdžių metu surenkama rizikos analizės procesui reikalinga informacija. Kad būtų galima parengti galutinę ataskaitą, veiklos vadovas, proceso vadovas ir kuratorius

dar turi užbaigti veiksmų planą. Baigiamajame KURAP proceso etape parengiami penki dokumentai:

1. Kryžminių nuorodų lentelė;
2. Egzistuojančių saugos priemonių nustatymas;
3. Atvirų grėsmių aptarimas su valdytoju;
4. Saugos priemonių, taikytinų atviroms grėsmėms, nustatymas;
5. Galutinė ataskaita.

Atsižvelgiant į šiandieninį techninės pažangos lygį, daugiausia laiko kuratoriui ir sekretoriui užima kryžminių nuorodų lentelės sudarymas. Šiame dokumente prie kiekvienos saugos priemonės turi būti nurodytos grėsmės, kurių būtų galima išvengti.

Pavyzdžiui, 6.5.1 lentelės antrojoje eilutėje KURAP grupė nurodė tris saugos priemones (9, 13, 26), kuriomis būtų galima sušvelninti atitinkamą grėsmę. Kryžminių nuorodų lentelėje saugos priemonės Nr. 9 nuorodų laukelis atrodytų panašiai, kaip 6.5.3 lentelėje.

Kaip parodyta šiame pavyzdyje, saugos priemonė Nr. 9 leis sušvelninti 11 skirtingų grėsmių. Kryžminių nuorodų lentelė padeda veiklos vadovams apsispręsti, kaip geriausiai panaudoti turimus ribotus išteklius.

6.5.3 lentelė

KRYŽMINIŲ NUORODŲ LENTELĖS PAVYZDYS

Saugos priemonė	Saugos priemonės apibūdinimas	Grėsmės Nr.	Grėsmė	Tipas	Pirmumas
9	Taikyti sistemingą keitimų valdymą, kuris vykdomas etapais ir laikomasi atsargumo priemonių. Avariniai pakeitimai turėtų būti šio proceso dalis.	2	Neaiškus arba neegzistuojantis informacijos versijų nustatymas	**INT**	**B**
		16	Neteisingos informacijos panaudojimo poveikis veiklai	**INT**	**B**
		23	Nereagavimas laiku į reikalavimus	**INT**	**A**
		25	E-veiklos vientisumo politikos ir egzistuojančios bendrovės politikos tarpusavio neatitikimas	**INT**	**A**
		29	Neteisingų duomenų arba dokumentų paskelbimas	**INT**	**A**
		35	Netinkamas programinės įrangos modifikavimo procedūrų taikymas, tobulinant programinę įrangą (kodų keitimas, neatlikus patikrinimo)	**INT**	**B**
		40	Personalo duomenų paskelbimas internete, neturint tam leidimo	**CON**	**A**
		44	Naujų technologijų atsiradimas, sąlygojantis konfidencialumo pažeidimą	**CON**	**A**
		47	Pardavimų nuostoliai ir konkurencinį pranašumą teikiančios informacijos žinios	**CON**	**B**
		50	Bendrovės informacijos elektroninis perėmimas (pasiklausymas)	**CON**	**B**
		9	Netinkamai atlikti programinės įrangos arba kompiuterinės technikos pakeitimai	**AVA**	**B**

Sudarius kryžminių nuorodų lentelę (tam turėtų užtekti dviejų darbo dienų), veiksmų planas ir kryžminių nuorodų lentelė turėtų būti perduota veiklos vadovui.

KURAP ataskaita turėtų būti parengta taip, kaip parodyta 6.5.4 lentelėje. Turėdami veiksmų planą ir kryžminių nuorodų lentelę, kuratorius ir projekto vadovas paprastai nustato, kokios saugos priemonės jau yra įdiegtos. Baigę šį darbą, jie susitinka su veiklos vadovu, kartu su juo peržiūri dokumentus ir rekomenduoja saugos priemones, kurios galėtų sušvelninti atviras grėsmes.

6.5.4 lentelė

VEIKSMŲ PLANUI PASIRINKTOS SAUGOS PRIEMONĖS

Veiksmai	**Kas**	**Kada**	**Papildomos pastabos**
PKF 2 jau yra įdiegta, o prieigos kontrolės sąrašas bus peržiūrėtas, siekiant identifikuoti įgaliotus vartotojus	Valdytojas ir IP	2005-05-02	
Pokyčių valdymo procedūros jau įdiegtos	Operatoriai	Baigta	
Darbuotojų mokymo grafikas sudarytas	Personalo skyrius		
Atsarginio kopijavimo paslaugų lygio sutartis, peržiūrėta kartu su vykdytojais	Valdytojas ir vykdytojai	2005-07-01	
Paslaugų lygio sutartis bus įgyvendinta kartu su paslaugų tiekėju	Valdytojas	2005-08-20	

6.5.4 lentelėje pažymėti klausimai jau baigti, t. y. saugos priemonės jau įdiegtos. Dažniausiai pasiekusi šį rizikos analizės proceso etapą, grupė pastebi, kad maždaug 80 procentų grėsmių jau taikomos kokios nors saugos priemonės.

Tačiau atviroms grėsmėms kuratorius, projekto ir veiklos vadovai turi parinkti efektyviausias ir ekonomine prasme rentabiliausias saugos priemones, taip pat nustatyti, kas bus atsakingas už jų įdiegimą ir iki kurios dienos jos turės būti įdiegtos. Jeigu saugos priemonei įdiegti reikalinga trečiosios šalies pagalba, įdiegimo terminus būtina suderinti su ja.

Kai kiekvienai rizikai bus paskirta saugos priemonė, arba valdytojas posėdžio metu bus jas pripažinęs priimtinomis, galima pradėti rengti galutinę ataskaitą. Jos pavyzdys pateiktas 6.5.5 lentelėje.

Išvada

Kuruojamos rizikos analizės procesas (KURAP) šiandien yra plačiausiai taikomas kiekybinės rizikos analizės metodas. KURAP sudaro trys pagrindinės dalys:

1. Parengtinis KURAP posėdis, trunkantis apie valandą, kurio metu parengiama:
   1. 1. Apimties apibrėžimas;
   1. 2. Vizualinė schema;
   1. 3. Grupės narių sąrašas;
   1. 4. Susirinkimo tvarka;
   1. 5. Sąvokos:
   - rizika,
   - saugos priemonė,
   - analizės elementai (vientisumas, konfidencialumas, prieinamumas),
   - pažeidžiamumo poveikis.

6.5.5 lentelė

GALUTINĖS ATASKAITOS PAVYZDYS

Data: (įrašykite datą)
Kam: Pareigos
Vardas, pavardė

Nuo: Vardas, pavardė
Pareigos

Dėl: Kuruojamos rizikos analizės

Informacijos saugos grupė atliko toliau nurodytų funkcijų kuruojamą rizikos analizę. Rizikos analizės dalyviai identifikavo rizikos ir saugos priemones, kurios pateikiamos pridedamame veiksmų plane. Siekiant užtikrinti, kad jūsų organizacijos reikmės būtų tinkamai įvertintos, į procesą buvote įtraukti ir jūs arba jūsų atstovas. Veiksmų plane nurodyta, kurios rizikos analizės metu identifikuotos saugos priemonės yra įdiegtos arba bus diegiamos. Jūs priėmėte sprendimus dėl diegiamų priemonių ir jų diegimo grafiko.

KURAP data: 2005-08-05

Sistema/programa: IS elektroninės komercijos funkcija

Valdytojas: Vardas, pavardė

Kuratorius: Vardas, pavardė

Prašome susipažinti su toliau pateiktu įsipareigojimų pareiškimu, pasirašyti jį ir grąžinti man.

Įsipareigojimo pareiškimas: aš, valdytojas, suprantu, kad rizikos, nurodytos Rizikos analizės veiksmų plane, gali neigiamai paveikti šios sistemos/programos informacijos vientisumą, konfidencialumą ir prieinamumą. Nusprendžiau įdiegti saugos priemones, laikydamasis grafiko, nurodyto pridedamame Rizikos analizės veiksmų plane. Suprantu, kad nekontroliuojama grėsmė gali neigiamai paveikti įstaigos informaciją ir jos veiklą.

Aš žinau, kad Rizikos analizės veiksmų plano kopija bus perduota audito organizacijai.

_____ _____

Direktorius, direktoriaus pav. (Vardas, pavardė) Data

Įstaigos pavadinimas

_____ _____

Kuratorius (Vardas, pavardė) Data

2. KURAP sesija, trunkanti apie keturias valandas, kurios metu parengiami šie dokumentai:
   2. 1. Rizikos nustatymas;
   2. 2. Suskirstytos rizikos pagal svarbą;
   2. 3. Siūlomos saugos priemonės.
3. Baigiamasis KURAP etapas trunka apie dešimt dienų, jį sudaro trys elementai:
   3. 1. Kryžminių nuorodų lentelės sudarymas;
   3. 2. Egzistuojančių saugos priemonių nustatymas;
   3. 3. Saugos priemonių parinkimas nustatytoms rizikoms arba rizikos prisiėmimas.

Dauguma organizacijų sutinka, kad rizikos ir su jomis susijusių priemonių kaštų-naudos įvertinimas yra pagrindinė saugos programų efektyvumo prielaida. Sauga negali būti savitikslė – tai programų ir procedūrų visuma, kuriama veiklos operacijoms palaikyti. Jeigu, įgyvendinant rizikos analizės programą, bus atsižvelgta į veiklos procesų palaikymą, saugos priemonėmis bus labiau pasitikima.

Informacija ir duomenų apdorojimo sistemos yra labai svarbios vertybės, užtikrinančios bet kokios įmonės veiklą ir jos tikslų įgyvendinimą, todėl jos turi būti tinkamai saugomos. Efektyvi rizikos analizė užtikrina šių veiklos poreikių tenkinimą.

6.4 Rizikos vertinimo procesas

Rizikos vertinimas priklauso nuo šių veiksnių:

- Vertybių nustatymas ir įvertinimas (žr. 6.4.1 ir 6.4.2);
- Saugos reikalavimų nustatymas, pvz., nustatant grėsmes ir pažeidžiamumą, teisinius ir veiklos reikalavimus (žr. 6.4.3);

- Galimų grėsmių ir pažeidžiamumo tikimybės, teisinių reikalavimų ir veiklos reikmių įvertinimas (žr. 6.4.4);
- Rizikų apskaičiavimas (žr. 6.4.5);
- Tinkamų rizikos valdymo priemonių pasirinkimas (žr. 6.4.6);
- Rizikos kontrolės procedūros, mažinančios riziką iki priimtino lygio, pasirinkimas (žr. 6.4.7).

6.4.1 Vertybių nustatymas

Vertybė (turtas) šiuo atveju reiškia vertingą turtą arba priemones, būtinas organizacijai, užtikrinti jos veiklą arba veiklos tęstinumą. Taigi vertybėms reikalinga apsauga, leidžianti normaliai vykdyti veiklos operacijas ir jas tęsti. Tinkamas vertybių valdymas ir apskaita[1] yra labai svarbūs, siekiant užtikrinti tinkamą organizacijos turto apsaugą. Šie du aspektai turėtų būti pagrindinė visų lygių vadovų atsakomybė[2]. Labai svarbu, kad į vertybes būtų įtrauktas pagrindinis turtas. Siekiant užtikrinti, kad nė viena turto dalis nebūtų užmiršta arba praleista, Informacijos saugos valdymo sistemos (ISVS) apimtis būtina nustatyti, įvertinant veiklos ypatumus, organizaciją, jos veiklos vietą, turtą ir taikomas technologijas.

Kiekvienas turto elementas privalo būti tiksliai įvardytas ir tinkamai įvertintas (žr. toliau 6.4.2 skyrių), jo nuosavybė ir saugos

[1] ISO/IEC 17799 3 skyrius nurodo du specifinius uždavinius, susijusius su turtu: (I) 3.1 Atsakomybė už turtą ir ii), 3.2 Informacijos klasifikacija.

[2] Atsakomybė už turtą leidžia užtikrinti adekvačią informacijos apsaugą. Turi būti nurodyti pagrindinio turto valdytojai, ir jie turi būti atsakingi už tinkamų saugos priemonių palaikymą. Atsakomybė už saugos priemonių įgyvendinimą gali būti perduota kitiems, tačiau atsiskaito turto valdytojai.

klasė privalo būti tiksliai nustatyta ir aprašyta (žr. ISO/IEC 17799 [1] 5 ir [8]/[9] skyrius). Vertybių (turto) pavyzdžiai tokie:

- **Informacinis turtas***:* duomenų bazės ir duomenų bylos, sistemų dokumentacija, vartotojo instrukcijos, mokomoji medžiaga, operacinės arba priežiūros procedūros, tęstinumo planai, atsarginės priemonės;
- **Popierinė dokumentacija:** sutartys, rekomendacijos, bendrovės dokumentacija, svarbių veiklos rezultatų dokumentai;
- **Programinė įranga:** taikomosios programos, sistemos programinė įranga, programavimo priemonės;
- **Fizinis turtas:** kompiuteriai ir ryšių įranga, laikmenos (juostos ir diskai), kita techninė įranga (maitinimo įranga, oro kondicionieriai), baldai, patalpos;
- **Žmonės:** personalas, klientai, abonentai;
- Organizacijos įvaizdis ir reputacija;
- **Paslaugos**: kompiuterinės ir ryšių paslaugos, kitos techninės paslaugos (šildymas, apšvietimas, elektros energijos tiekimas, oro kondicionavimas).

6.4.1 žingsnio rezultatas:
Šio žingsnio rezultatas turėtų būti turto (vertybių) sąrašas, į kurį būtų įtrauktas visas pagrindinis turtas ISVS ribose, nurodant kiekvieno elemento vietą ir jo turėtoją. (Žr. 6.4.1 lentelę).

6.4.2 Turto įvertinimas

Turto nustatymas ir įvertinimas, remiantis organizacijos veiklos reikmėmis, yra svarbiausias rizikos vertinimo veiksnys. Siekiant nustatyti tinkamiausią turto saugą, būtina įvertinti jo vertę

pagal turto reikalingumą arba jo potencialią vertę organizacijos veiklai. Šios vertės paprastai išreiškiamos atsižvelgiant į tai, kokį tikėtiną poveikį veiklai gali turėti nepageidautini įvykiai, tokie kaip informacijos atskleidimas, modifikacija, neprieinamumas ir (arba) turto sunaikinimas. Šie įvykiai gali sukelti finansinius nuostolius, dėl jų gali būti prarastos pajamos, rinkos dalis arba jie gali pakenkti įstaigos įvaizdžiui.

Informaciją, reikalingą turto vertei nustatyti, privalo pateikti turto valdytojai ir vartotojai, galintys autoritetingai pasisakyti apie turto svarbą ir ypač pateikti informaciją apie organizaciją ir jos veiklą.

Vertinamas turtas turėtų būti susietas su jo įsigijimo ir priežiūros kaštais, neigiamu poveikiu, kurį organizacijai arba jos veiklai gali turėti informacijos atskleidimas, jos vientisumo pažeidimas arba neprieinamumas. Norint užtikrinti turto įvertinimo visapusiškumą ir tinkamai jį įvertinus, būtina taikyti turto vertinimo skalę.

Kiekvieno turto elemento vertė turi būti nustatyta, atsižvelgiant į tai, kokį neigiamą poveikį organizacijai arba jos veiklai gali turėti informacijos konfidencialumo, vientisumo arba prieinamumo pažeidimas arba kito turto sunaikinimas[3]. Vertinimo skalės pavyzdys galėtų būti:

- Didelė, vidutinė ir maža vertė;
- Detaliau: nereikšminga – maža – vidutinė – didelė – labai didelė.

[3] Kartais „konfidencialumo“, „vientisumo“ arba „prieinamumo“ kriterijų nepakanka, norint išreikšti turto svarbą, pvz., kalbant apie informaciją, kuriai taikoma intelektinės nuosavybės teisių apsauga. Tokiais atvejais turėtų būti įvesti papildomi kriterijai, atspindintys šiuos reikalavimus.

Organizacija turėtų pati nustatyti turto vertinimo skalės ribas. Spręsti, kas būtų vertintina kaip „mažas“ arba „didelis“ nuostolis, yra pačios organizacijos kompetencija, nes nuostolis, kuris gali būti lemtingas nedidelei organizacijai, didelei organizacijai gali būti mažas arba netgi nereikšmingas.

Teisingas verčių skalės sąvokos pateikimas turi būti aiškiai suvokiamas organizacijai. Šių sąvokų aiškumas labai svarbus. Tai ypač svarbu bendraujant su turto valdytojais ir vartotojais, siekiant gauti informaciją, reikalingą turtui įvertinti.

6.4.2 žingsnio rezultatas:

Šio žingsnio rezultatas turėtų būti turto sąrašas, apimant kiekvieno iš nustatytų turto vienetų vertę pagal kiekvieną kriterijų, pvz., konfidencialumą, vientisumą ir prieinamumą, jei reikia, taip pat ir pagal kitus kriterijus. (Žr. 6.4.2 lentelę).

6.4.3 Saugos reikalavimų nustatymas

6.4.3.1 Reikalavimų šaltiniai

Kiekvienoje – nesvarbu, didelėje ar mažoje – organizacijoje taikomi saugos reikalavimai kyla iš trijų pagrindinių šaltinių, juos būtina aprašyti ISVS:

- Specifinio pažeidžiamumo ir grėsmių, galinčių lemti rimtus veiklos nuostolius;
- Įstatyminių ir sutartinių reikalavimų, kuriuos privalo tenkinti organizacija, jos veiklos partneriai, rangovai ir paslaugų tiekėjai;
- Organizacijos savitų principų, tikslų ir informacijos valdymo reikalavimų visuma.

Nustačius saugos reikalavimus, juos būtina apibrėžti pagal konfidencialumo, vientisumo ir prieinamumo reikalavimus.

Kažkuriuo momentu arba prieš pradedant rizikos vertinimą, arba prieš pradedant šio žingsnio procedūras, būtina nustatyti jau įdiegtas saugos priemones. To reikia, kad būtų galima užbaigti identifikaciją ir realiai įvertinti grėsmes ir pažeidžiamumus. Tai taip pat svarbu, norint tinkamai pasirinkti papildomas saugos priemones (žr. 6.4.6 žingsnį) ir užtikrinti jų suderinamumą su jau esamomis saugos priemonėmis.

6.4.3.2 Grėsmių ir pažeidžiamumo nustatymas

Turtui (vertybėms) gali grėsti labai įvairūs pavojai. Grėsmė reiškia potencialų nepageidaujamą įvykį, galintį pakenkti organizacijos sistemoms arba jos turtui. Pvz., žalą gali sukelti tiesioginė arba netiesioginė ataka į organizacijos duomenis (neteisėtas duomenų sunaikinimas, atskleidimas, keitimas, sugadinimas, nepasiekiamumas arba praradimas). Grėsmės kyla tiek dėl sąmoningų, tiek dėl nesąmoningų veiksmų arba atsitiktinių įvykių. Kad grėsmė būtų realizuota, pakenkiant organizacijos turtui, turi būti išnaudoti pažeidžiamumai, esantys organizacijos IT sistemose, programinėje įrangoje arba paslaugose. Publikacijoje „Apie veiklos informacijos apsaugą“ (žr. 8 ir 9) pateikta papildoma informacija apie grėsmes.

Pažeidžiamumai – tai organizacijos turto silpnosios vietos. Šios silpnosios vietos gali būti panaudotos, įgyvendinant grėsmes ir sukeliant nepageidautinus įvykius, galinčius padaryti nuostolių arba žalą minėtam turtui. Pažeidžiamumas pats savaime nesukelia žalos, tai greičiau sąlyga arba sąlygų visuma, leidžianti įgyvendinti grėsmes ir padaryti žalą turtui. Pažeidžiamumų nustatymo metu turi būti išaiškintos silpnosios vietos, susijusios su:

- Turto fizine aplinka,
- Personalu, valdymo ir administracinėmis procedūromis bei kontrolės priemonėmis,
- Technine, programine bei ryšių įranga ir infrastruktūra.

Pastaba. Priklausomai nuo taikomos rizikos vertinimo metodikos, grėsmės ir pažeidžiamumai gali būti vertinami kartu arba atskirai. Galimi abu variantai, todėl dėl metodikos būtina apsispręsti, renkantis bendrą rizikos vertinimo procedūrą.

6.4.3.3 Teisiniai, norminiai ir sutartiniai reikalavimai

Saugos reikalavimai, kylantys iš teisinių, norminių ir sutartinių reikalavimų, kuriuos privalo tenkinti organizacija, jos veiklos partneriai, rangovai ir paslaugų tiekėjai, turi būti aprašyti ISVS. Tai svarbu, norint užtikrinti, pvz., programinės įrangos ar duomenų kopijavimo kontrolę, apsaugoti organizacijos duomenis, užtikrinti, kad ISVS atitiktų jau nurodytus reikalavimus arba kad saugos priemonių taikymas arba netaikymas kiekvienai informacinei sistemai neprieštarautų jokiems teisiniams reikalavimams, civiliniams įsipareigojimams arba komercinių sutarčių nuostatoms. Taigi būtina nustatyti teisinius, norminius ir sutartinius reikalavimus, susijusius su kiekvienu turto vienetu.

6.4.3.4 Organizaciniai principai, tikslai ir veiklos reikalavimai

Saugos reikalavimai, susiję su bendraisiais organizacijos principais, tikslais ir reikalavimais, taikomais informacijos apdorojimui, palaikant organizacijos veiklos operacijas, taip pat turi būti aprašyti ISVS. Konkurencine, piniginių srautų ir (arba) pelningumo prasme labai svarbu, kad ISVS atitiktų šiuos reikalavimus. Taip pat labai svarbu, kad saugos priemonių taikymas arba ne-

taikymas kiekvienai informacinei sistemai nepakenktų įprastinės veiklos efektyvumui. Vertinant kiekvieną turto vienetą, turi būti nustatyti su juo susiję veiklos tikslai ir reikalavimai.

6.4.3 žingsnio rezultatas:

6.4.3 žingsnio rezultatas turi būti nustatytų grėsmių ir pažeidžiamumų sąrašas, taip pat teisiniai/ sutartiniai ir veiklos reikalavimai, taikytini kiekvienam 6.4.1 žingsnio metu nustatytam turto vienetui. (Žr. 6.4.3 lentelę).

6.4.4 Saugos reikalavimų įvertinimas

Taip pat, kaip ir vertinant turtą, nustatant saugos reikalavimus, būtina vertinimo skalė. Daugeliu atveju tiks paprasta trijų lygių skalė:

- Žemas,
- Vidutinis,
- Aukštas.

Tokiu būdu procesas nebus pernelyg komplikuotas.

6.4.4.1 Grėsmių ir pažeidžiamumų įvertinimas

Identifikavus pažeidžiamumus ir grėsmes, būtina įvertinti grėsmių ir pažeidžiamumų kombinacijos iškilimo tikimybę. Būtina atkreipti dėmesį į tai, ar grėsmės ir pažeidžiamumai vertinami kartu, ar atskirai. Priklausomai nuo to atitinkamas ir pažeidžiamumo įvertinimas.

Grėsmių tikimybės įvertinimas turi būti atliekamas atsižvelgiant į:

- Tyčines grėsmes: motyvacijos, kompiuterio įsilaužėlio sugebėjimus ir numanomos atakos patrauklumo;

- Atsitiktines grėsmes: kaip dažnai jos gali iškilti (remiantis patirtimi, statistika ir t.t.); geografiniai veiksniai (pvz., cheminių arba naftos perdirbimo gamyklų artumas, zonos, kuriose visuomet gali susidaryti ekstremalios oro sąlygos) ir veiksnius, kurie gali sąlygoti personalo klaidas arba įrangos darbo sutrikimus.

Bendroji įvykio tikimybė taip pat priklauso nuo turto pažeidžiamumų, pvz., kaip lengvai juos būtų galima panaudoti saugos įvykiui sukelti. Atitinkamai ir pažeidžiamumai turėtų būti įvertinti pagal tam tikrą skalę, pvz.:

- Labai tikėtina arba tikėtina – pažeidžiamumą lengva panaudoti saugos įvykiui sukelti, turtas tinkamai neapsaugotas;
- Galima – pažeidžiamumą galima išnaudoti, bet yra įdiegtos tam tikros saugos priemonės;
- Mažai tikėtina arba neįmanoma – pažeidžiamumą išnaudoti sunku, įdiegtos tinkamos saugos priemonės.

Informaciją, reikalingą grėsmėms ir pažeidžiamumams įvertinti, galima gauti iš darbuotojų, susijusių su ISVS ir kitais atitinkamais veiklos procesais. Pavyzdžiui, tai gali būti personalo skyriaus darbuotojai, pastatų priežiūros darbuotojai, IT specialistai, taip pat darbuotojai, atsakingi už organizacijos saugą.

6.4.4.2 Teisinių ir veiklos reikalavimų įvertinimas

Taip pat, kaip ir vertinant grėsmes ir pažeidžiamumus, būtina nustatyti teisinius ir sutartinius reikalavimus (žr. 6.4.3.3 ir 6.4.3.4). Tai būtina siekiant apskaičiuoti riziką, susijusią su šiais reikalavimais.

Norint nustatyti konkrečias vertes teisiniams arba veiklos reikalavimams, būtina:

- įvertinti pasekmes veiklai, jeigu teisiniai ir sutartiniai ar veiklos reikalavimai nebūtų įvykdyti;
- įvertinti pasekmes nagrinėjamam turtui ir visai ISVS;
- įvertinti paties įvykio tikimybę.

Šių svarstymų rezultatai turėtų būti panaudoti, siekiant nustatyti su kiekvienu turto elementu susijusių teisinių ir sutartinių bei veiklos reikalavimų vertę pagal saugos reikalavimų vertinimo skalę.

6.4.4 žingsnio rezultatas:
Šio žingsnio rezultatas – kiekvienam saugos reikalavimui turėtų būti priskirta konkreti vertė (žr. 6.4.3 žingsnį).

6.4.5 Saugos rizikų apskaičiavimas

Rizikos įvertinimo tikslas yra nustatyti ir įvertinti riziką, remiantis 6.4.1-6.4.4 žingsnių rezultatais. Rizika apskaičiuojama remiantis turto vienetų vertėmis ir įvertintais tarpusavyje susijusių saugos reikalavimų lygiais.

Šie veiksniai gali būti susieti skirtingais būdais. Pavyzdžiui, rizikos reikšmės apskaičiuojamos pagal turto vienetams, pažeidžiamumams ir grėsmėms bei teisiniams ir veiklos reikalavimams priskirtų verčių sumą.

Svarbu pastebėti, kad nėra „teisingų“ ir „neteisingų“ rizikos apskaičiavimo būdų, jeigu ankstesniuose skyriuose aptartos koncepcijos racionaliai derinamos tarpusavyje. Taigi organizacija gali pasirinkti tą rizikos įvertinimo metodiką, kuri geriausiai atitinka jos veiklos ir jos saugos reikalavimus.

6.4.5. žingsnio rezultatas:

Šio žingsnio rezultatas turėtų būti apskaičiuotų rizikų sąrašas, susijęs su kiekvienu informacijos atskleidimo, modifikacijos arba neprieinamumo atveju arba turto vieneto sunaikinimu, neperžengiant ISVS ribų. (Žr. 6.4.5 lentelę).

6.4.6 Rizikos valdymo priemonių pasirinkimas

Atlikus rizikos nustatymą ir įvertinimą, kitas organizacijos uždavinys yra nustatyti ir įvertinti tinkamiausias rizikos valdymo priemones. Šios priemonės turėtų būti pasirenkamos atsižvelgiant į konkrečius turto vienetus ir su jais susijusios rizikos poveikį verslui. Kitas svarbus veiksnys priimant sprendimą yra priimtinas rizikos lygis, kuris nustatomas pasirinkus tinkamiausią rizikos vertinimo metodiką.

Nustatytai ir įvertintai rizikai (6.4.1 – 6.4.5 žingsnių rezultatas) organizacija gali pasirinkti vieną iš keturių veiksmų:

- Sumažinti riziką, įdiegdama atitinkamas kontrolės priemones (žr. toliau 6.4.7 skyrių);
- Sąmoningai ir objektyviai priimti riziką, numatant, jeigu tai atitinka organizacijos politiką ir rizikos priimtinumo kriterijus (žr. 4 skyrių);
- Vengti rizikos (žr. toliau 6.4.6.1);
- Su veikla susijusią riziką perkelti kitoms šalims (žr. toliau 6.4.6.2).

Kiekvienos konkrečios rizikos atveju būtina įvertinti visas galimybes, kad būtų galima pasirinkti tinkamiausią. Šių veiksmų rezultatai turėtų būti aprašyti ir vėliau panaudoti rizikos valdymo plano rengimo procese.

6.4.6.1 Rizikos vengimas

Rizikos vengimas apibūdina bet kokį atvejį, kai turtas iškeliamas iš rizikos zonų (pvz., iš fizinių zonų arba iš veiklos procesų). Tai galima pasiekti, pvz., tokiais būdais:

- Nevykdant tam tikrų veiklos operacijų (t.y., nenaudojant elektroninės komercijos priemonių arba nenaudojant interneto tam tikroms veiklos operacijoms);
- Iškeliant turtą iš rizikos zonų (t.y., nekaupiant konfidencialių bylų organizacijos vidaus tinkle arba iškeliant vertybes iš tų zonų, kurios neturi tinkamos fizinės apsaugos);
- Nusprendžiant neperduoti konfidencialios informacijos, pvz., trečiosioms šalims, jeigu jos neužtikrina tinkamos saugos.

Svarstant rizikos išvengimo galimybę būtina subalansuoti veiklos ir finansinius poreikius. Pavyzdžiui, internetas arba elektroninė komercija gali būti būtina organizacijai dėl jos veiklos pobūdžio, nepaisant kompiuterių įsilaužėlių keliamos grėsmės. Taigi veiklos požiūriu perkelti vertybes į saugią aplinką gali būti neįmanoma. Tokiu atveju būtina apsvarstyti kitas alternatyvas, pvz., rizikos perdavimą partneriams arba rizikos mažinimą.

6.4.6.2 Rizikos perdavimas

Rizikos perdavimas gali būti geriausia alternatyva, jeigu tai leidžia išvengti rizikos arba rizikos mažinimo priemonės yra labai sudėtingos ar pernelyg brangios. Pavyzdžiui, rizikos perdavimą galima organizuoti apdraudus proporcingai turto vertę ir su tuo turtu susijusią riziką, taip pat atsižvelgiant į turto reikšmę organizacijos veiklos procesams.

Kita galimybė – pavesti trečiosioms šalims arba išorės partneriams tvarkyti gyvybiškai svarbų veiklos turtą arba procesus, jei-

gu šios šalys arba partneriai turi tam tinkamas priemones. Šiuo atveju būtina pasirūpinti, kad į atitinkamas sutartis būtų įtraukti visi saugos reikalavimai, kontrolės uždaviniai ir priemonės ir tokiu būdu būtų užtikrinta tinkama sauga. Būtina turėti minty-je, kad daugeliu atveju atsakomybė už išorinės informacijos saugą ir informacijos apdorojimo priemones nepersikelia ir lieka pačiai organizacijai.

Kitas rizikos perdavimo pavyzdys galėtų būti rizikingo turto iškėlimas už ISVS ribų. Tai gali palengvinti ypač slaptos informacijos apsaugą ir padaryti ją pigesnę, bet būtina pasirūpinti, kad visas veiklai reikalingas inventorius būtų integruotas į ISVS per sietuvus ir sąsajas.

6.4.6 žingsnio rezultatas:

Šio žingsnio rezultatas – tinkamiausių kiekvieno rizikos tipo, nustatyto 6.4.1–6.4.5 žingsnių proceso metu, valdymo priemonių nustatymas ir aprašymas. (Žr. 6.4.6 lentelę).

6.4.7 Saugos kontrolės priemonių pasirinkimas

6.4.7.1 Dėl saugos kontrolės priemonių pasirinkimo

Siekiant sumažinti nustatytą riziką per aptariamąją ISVS, būtina nustatyti ir pasirinkti tinkamas ir pateisinamas saugos kontrolės priemones. Kontrolės priemones reikia pasirinkti iš ISO/IEC 17799 arba BS 7799 2 dalies A priedo, o prireikus – iš kitų šaltinių. Kontrolės priemonių pasirinkimo tikslas – sumažinti riziką iki organizacijai priimtino lygio. Pasirinkimą reikėtų pagrįsti rizikos vertinimo rezultatais, pavyzdžiui, pažeidžiamumai ir su jais susijusios grėsmės parodo, kur ir kokio pobūdžio saugos prie-

mones reikėtų įdiegti. Sertifikavimo reikmėms būtina aprašyti kontrolės priemonių pasirinkimo (ar kito sprendimo) pagrįstumą.

Jau įdiegtos kontrolės priemonės turi būti įvertintos lyginant jų kainą, įskaitant eksploatavimą. Turi būti numatyta galimybė pakeisti kontrolės priemones arba pagerinti jas, jeigu jos nėra pakankamai efektyvios. Reikėtų pastebėti, kad kartais pakeisti netinkamas kontrolės priemones gali būti brangiau, negu palikti jas, galbūt papildant naujomis kontrolės priemonėmis. Šis procesas turi apimti PDCA modelio (vadinamojo Demingo ciklu) „Patikros" rezultatus, jeigu buvo atliktas išankstinis rizikos įvertinimas.

Renkantis diegtinas kontrolės priemones, būtina įvertinti daugelį veiksnių, tarp jų:

- Naudojimo ir valdymo paprastumą,
- Skaidrumą vartotojui,
- Vartotojui teikiamą pagalbą, palengvinant funkcijų atlikimą,
- Santykinį kontrolės priemonių efektyvumą,
- Atliekamų funkcijų pobūdį – prevencija, sulaikymas, nustatymas, atkūrimas, taisymas, priežiūra ir informavimas.

Paprastai viena kontrolės priemonė atlieka keletą funkcijų, ir kuo daugiau, tuo geriau. Vertinant bendrą saugą arba visumą kontrolės priemonių, kurias rengiamasi įdiegti, būtina, jei tai įmanoma, suderinti įvairaus pobūdžio funkcijas. Tai padeda užtikrinti bendrą saugos efektyvumą ir veiksmingumą. Kontrolės priemonių pasirinkimas turi papildyti viena kitą ir operacines (netechnines) bei technines kontrolės priemones. Operacinės kontrolės priemonės yra fizinės, personalo ir administracines saugos priemonės.

Be itin svarbaus rizikos sumažinimo veiksnio (žr. toliau 6.4.7.2 skyrių), renkantis kontrolės priemones taip pat būtina įvertinti

ir kaštus. Nederėtų rinktis tokių kontrolės priemonių, kurių įrengimo ir eksploatavimo kaina viršija iš anksto nustatytą saugos biudžetą. Tokiais atvejais reikia ieškoti pigesnių priemonių. Tačiau būtina itin atidžiai pasirūpinti, kad dėl biudžeto apribojimų nebūtų sumažintas diegiamų kontrolės priemonių skaičius ir nenukentėtų jų kokybė, nes tai gali sukelti papildomą riziką. Kontrolės priemonėms skirtas biudžetas neturėtų būti vertinamas kaip griežtas apribojimas, jį mažinti reikia itin atsargiai.

6.4.7.2 Rizikos mažinimas ir jos priimtinumas

Kai pagal 6.4.6 skyrių pasirenkamas „rizikos mažinimo“ variantas, reikia pasirinkti tinkamas priemones, kurios sumažintų riziką iki nustatyto priimtino lygio. Norint nustatyti tinkamiausias kontrolės priemones, būtų naudinga įvertinti su konkrečia rizika susijusius saugos reikalavimus (pvz., grėsmes ir pažeidžiamumus, teisinius ir sutartinius reikalavimus), taip pat kitus rizikos vertinimo rezultatus. Kontrolės priemonės gali mažinti riziką įvairiais būdais, pavyzdžiui:

- Sumažinti grėsmės tikimybę arba riziką sukeliantį pažeidžiamumą;
- Užtikrinti teisinių arba sutartinių reikalavimų laikymąsi;
- Sumažinti galimą iškilusios rizikos poveikį;
- Aptikti nepageidautinus įvykius, reaguoti į juos ir pašalinti jų pasekmes.

Būdas (ar jų kombinacija), kurį pasirinks organizacija, siekdama apsaugoti savo turtą, esantį ISVS, yra sprendimas, kuris priklauso nuo veiklos aplinkos, kurioje dirba organizacija. Svarbu, kad kontrolės priemonės atitiktų specifinius organizacijos poreikius, taip pat svarbu, kad jų pasirinkimas būtų pagrįstas.

Nustačius kontrolės priemones, kurios leistų sumažinti riziką iki priimtino lygio, būtina įvertinti, kiek minėtų priemonių įdiegimas sumažintų riziką – sumažinta rizika vadinama *likutine rizika*. Įvertinti *likutinę riziką* visuomet sunku, bet būtina įvertinti bent tai, kiek kontrolės priemonės sumažina rizikos vertę.

Jeigu paaiškėja, kad *likutinė rizika* tebėra nepriimtina, būtinas sprendimas, kaip ją kontroliuoti. Viena galimybė yra įdiegti papildomas kontrolės priemones, kurios galutinai sumažintų riziką iki priimtino lygio. Nors iš esmės atsisakymas toleruoti nepriimtiną riziką yra gera praktika, kartais sumažinti riziką iki priimtino lygio būna neįmanoma arba finansiškai nepriimtina.

Netgi įdiegus pasirinktas kontrolės priemones, tam tikra rizika visuomet lieka. Taip yra todėl, kad organizacijos informacinių sistemų neįmanoma visiškai apsaugoti. Dėl šios priežasties būtina įvertinti kontrolės priemonių diegimo rezultatus (pvz., pagal saugos įvykių ataskaitas arba registracijos bylas), kad būtų galima nustatyti, ar įdiegtos kontrolės priemonės pasiteisina. Šie veiksmai yra PDCA modelio „Patikros“ fazės dalis, o reikalingi pagerinimai turėtų būti įdiegti „Veiksmų“ fazėje, užtikrinant efektyvesnę saugą.

6.4.7 žingsnio rezultatas:

Šio žingsnio rezultatas – turėtų būti pasirinktos kontrolės priemonės, mažinančios riziką būdais, pasirinktais 6.4.6 žingsnio metu. Be to, būtina aprašyti sąsają su rizikos vertinimo rezultatais, ir tai turi užtikrinti, kad visų tipų rizika bus sumažinta, kiek tai įmanoma.

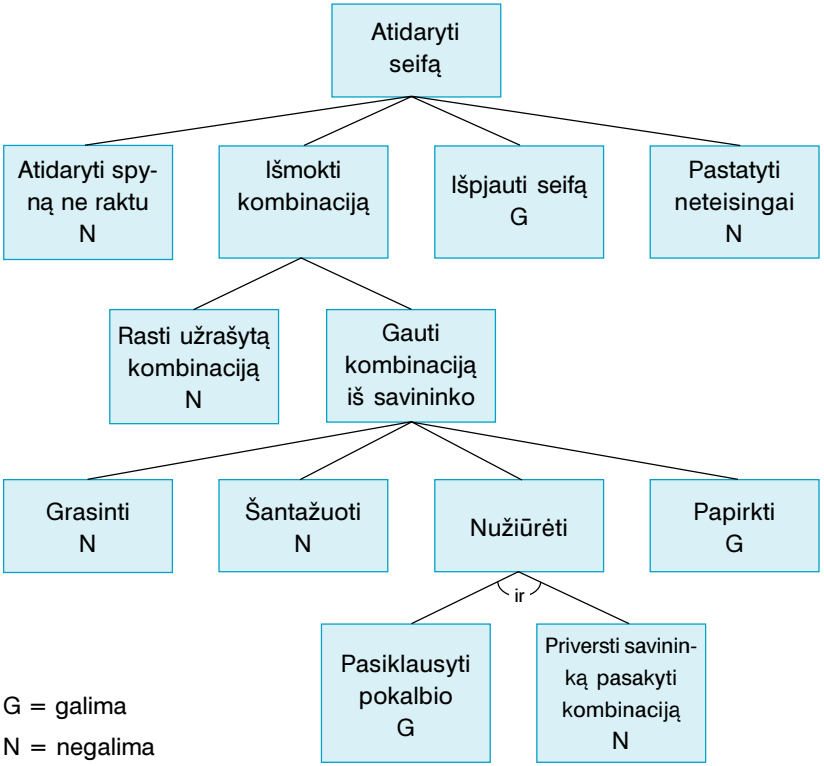
7. Grėsmių analizė, naudojant atakų medžio modelį

B. Shneer [2] pasiūlė šį kompiuterių sistemoms kylančių grėsmių analizės modelį. Jeigu galėtume nustatyti visus būdus, kuriais sistema gali būti atakuojama, galėtume sukurti kontrpriemones, leidžiančias atremti atakas. Ir jeigu galėtume nustatyti, kas yra potencialūs atakuotojai – nekalbant apie jų įgūdžius, motyvus ir tikslus – galbūt galėtume įdiegti tinkamas kontrpriemones, užkertančias kelią realioms grėsmėms.

Atakų medžio sudarymas

Atakų medžio sudarymas – tai formalus, metodiškas sistemų saugos nuo įvairių atakų aprašymas. Paprastai atakos yra pateikiamos medžio struktūros forma, kur tikslas atsispindi šaknies mazge, o išsišakojimai parodo įvairius tikslų siekimo kelius.

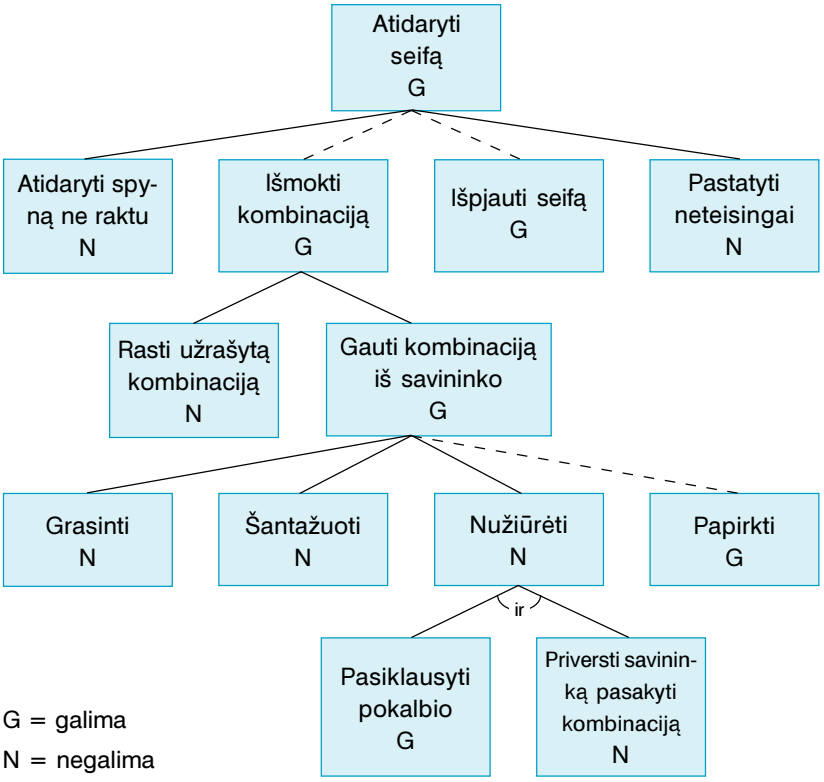
Pavyzdžiui, 7.1.1 pav. pavaizduotas paprastas atakų prieš fizinę saugą medis. Tikslas – atidaryti seifą. Norint atidaryti seifą, galima pasirinkti užraktą ir sužinoti kodo kombinaciją, išlaužti patį seifą arba blogai jį įrengti, kad vėliau būtų galima lengvai atidaryti. Norint sužinoti kodo kombinaciją, reikia arba rasti užrašytą kodą, arba gauti jį iš seifo valdytojo ir t. t. Kiekviena galimybė tampa tarpiniu tikslu, iš kurio seka tolesnės tikslo įgyvendinimo alternatyvos. (Aišku, tai tik paprastas atakų medžio pavyzdys. Kiek dar potencialių atakų, kurios leistų pasiekti tikslą, galėtumėte sugalvoti?)



7.1.1 pav. Atakų galimybės.

Atkreipkite dėmesį, kad yra „ir“ galimybės ir „arba“ galimybės (schemoje viskas, kas nėra „ir“, yra „arba“). „Arba“ žymi alternatyvas – pavyzdžiui, yra keturi būdai atidaryti seifą. „Ir“ galimybės reiškia skirtingus žingsnius į tą patį tikslą. Norint išgirsti kodo kombinaciją, reikia pasiklausyti pokalbių IR paskatinti seifo valdytoją pasakyti kodo kombinaciją. Nepatenkinus šių dviejų sąlygų, tikslo pasiekti neįmanoma.

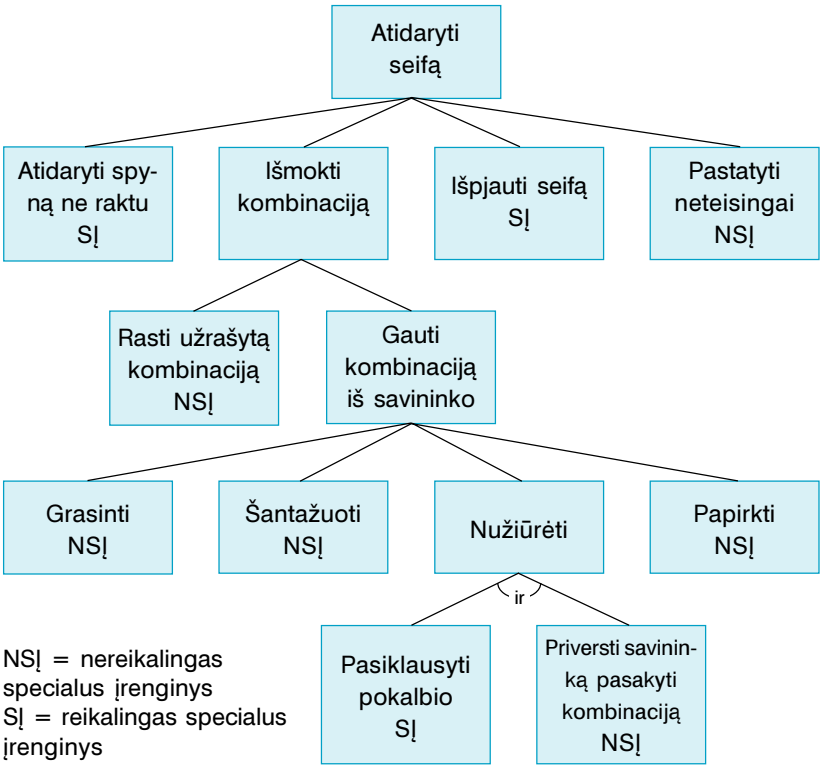
Tai pagrindinis atakų medžio principas. Jį baigus, atskiroms 7.1.1 lentelėje pavaizduotoms galimybėms reikia priskirti vertes – N (neįmanoma) ir Į (įmanoma) – ir atlikti skaičiavimus. (Vėlgi, tai tik iliustracinio pobūdžio pavyzdys, todėl pagal jį nereikėtų vertinti konkretaus seifo saugumo.) Priskyrus vertes – paprastai vertės priskiriamos nuodugniai išanalizavus patį seifą – galima apskaičiuoti tikslui taikytiną saugumą. Galimybė „arba“ gali būti įmanoma tik tuo atveju, jeigu įmanoma bent viena iš jos prielaidų.



7.1.2 pav. Atakų galimybės.

Jeigu prielaidos neįmanomos, pati galimybė taip pat neįmanoma. Galimybė „ir“ gali būti įmanoma tik tuo atveju, jeigu įmanoma bent viena iš jos prielaidų, priešingu atveju – ne. Žr. 7.1.2 pav.

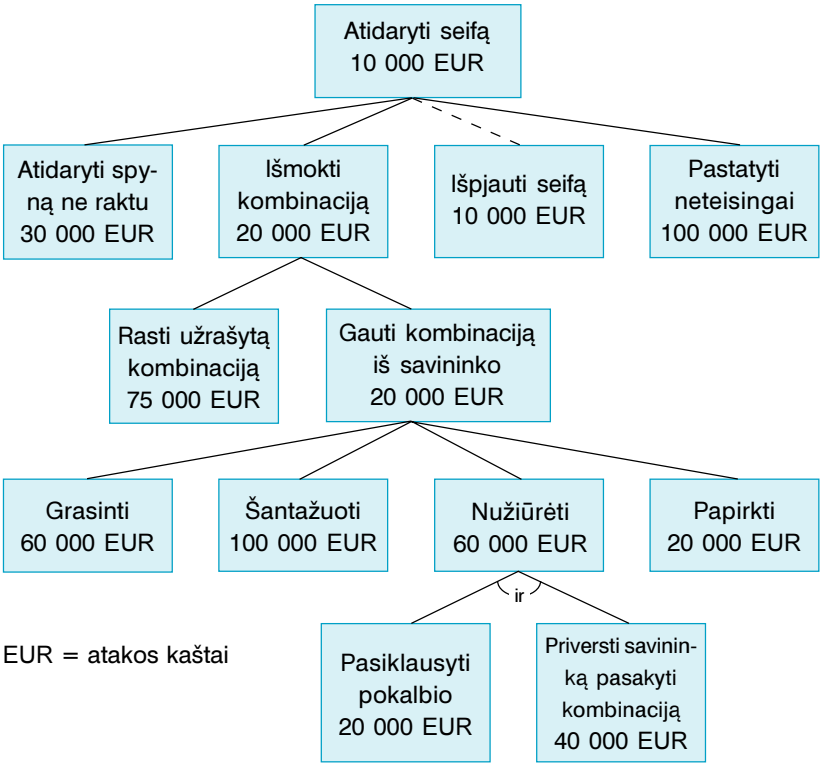
Punktyrinės linijos 7.1.2 pav. žymi visas galimas atakas – ir galimybių hierarchiją nuo pradinės prielaidos iki tikslo įgyvendinimo. Šiame pavyzdyje numatytos dvi galimos atakos: seifo išlaužimas arba spynos kodo kombinacijos sužinojimas, papirkus seifo valdytoją. Turėdami šias žinias, jūs tiksliai žinosite, kaip saugoti sistemą nuo galimų atakų.



7.1.3 pav. Specialios įrangos poreikis.

Galimybių įvertinimas pagal principą „įmanoma-neįmanoma“ yra tik vienas atakų medžio analizės būdas. Galimybėms gali būti priskirta bet kurios kitos alternatyvios loginės vertės: sudėtinga-paprasta, brangu-pigu, teisėta-neteisėta, reikalinga-nereikalinga speciali įranga ir t. t. Tuomet medžio struktūra bus analizuojama pagal ją. 7.1.3 pav. parodyta to paties atakų medžio analizė, pasitelkus kitas alternatyvias logines vertes.

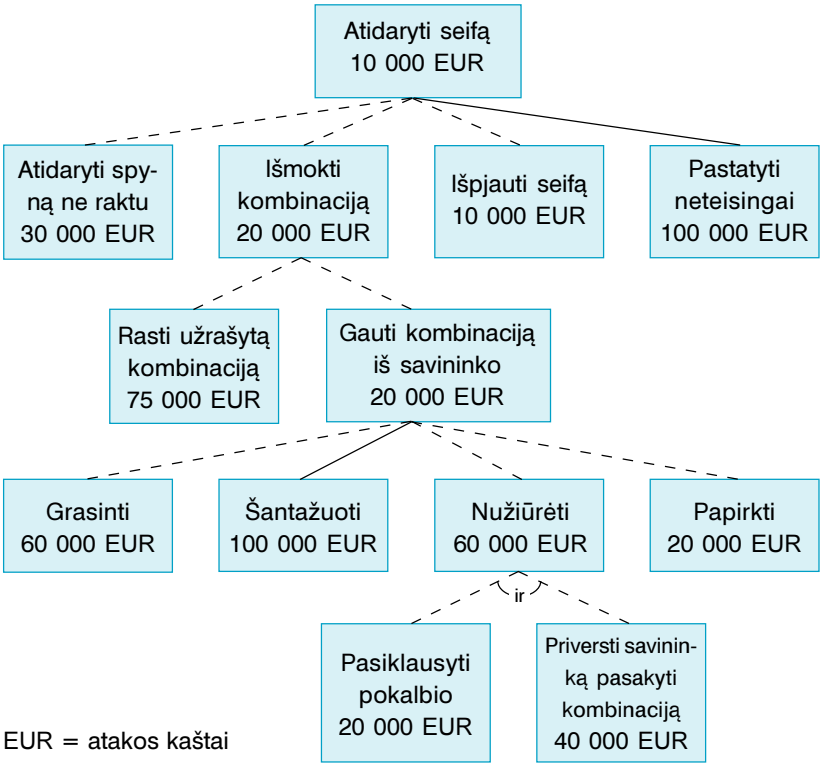
Reikšmių „brangu-pigu“ vartojimas gali būti naudingas, bet būtų geriau tiksliai žinoti, ką reiškia „brangu“. Medžio mazgams



7.1.4 pav. Atakos kaštai.

galima priskirti ir skaitines reikšmes. 7.1.4 pav. parodytas atakų medis su mazgams skirtais kaštais. Jos, kaip ir loginės reikšmės, gali būti perduodamos iš vieno lygio į kitą. Mazgai „arba“ verti tiek, kiek jų pigiausia prielaida. Mazgų „ir“ vertė lygi jų prielaidų reikšmių sumai. 7.1.4 pav. atakų medis buvo analizuojamas pasitelkus kaštus, ir tokiu būdu buvo nustatyta pigiausia galima ataka.

Atakų medis gali būti naudojamas ir sistemos pažeidžiamumui nustatyti. 7.1.5 pav. parodomos visos atakos, kurių kaštai



7.1.5 pav. Atakos, kurių vertė neviršija 100 000 EUR.

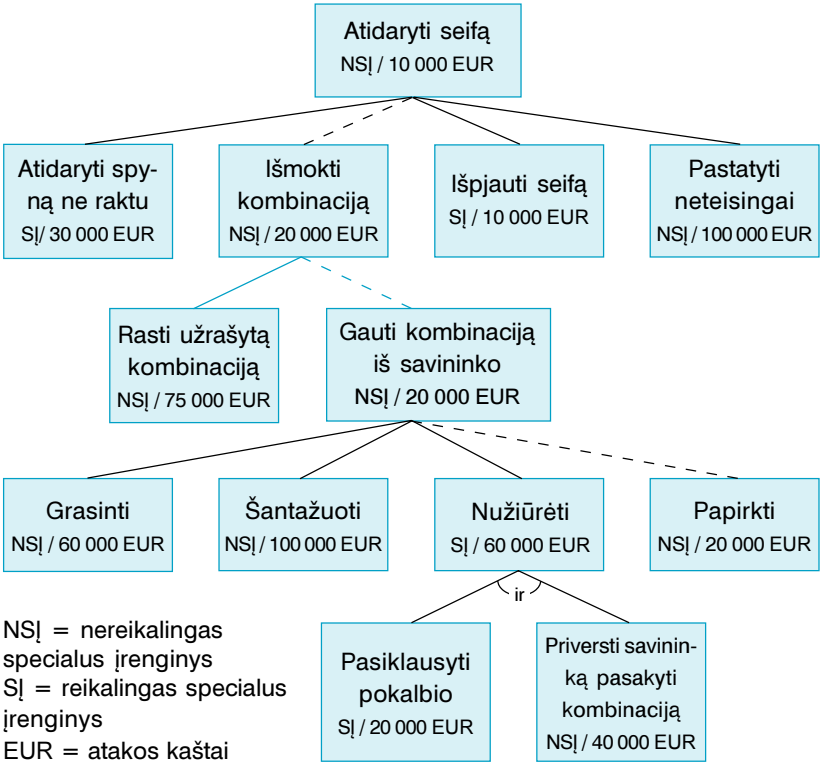
nesiekia 100 000 EUR. Jeigu jus domina tik mažesnės reikšmės (pvz., seifo turinio vertė yra tik 100 000 EUR), tada nereikia rūpintis dėl didesnės vertės atakų.

Yra daug kitų skaitinių reikšmių, kurios gali būti panaudotos atakų medžio analizei, pvz., konkrečios atakos sėkmės tikimybė, tikimybė, kad bus išbandyta konkreti atakos forma ir t. t.

Mazgai ir jų vertės

Sudarius realių atakų medį, mazgams bus galima priskirti daug skirtingų kintamųjų (tiek loginių, tiek skaitinių), tenkinančių įvairias realijas. Skirtingas mazgų vertes galima derinti tarpusavyje, tokiu būdu išsamiau įvertinant sistemos pažeidžiamumus. Pavyzdžiui, 7.2.1 pav. nustatyta pigiausia ataka, kuriai atlikti nereikia jokios specialios įrangos. Taip pat galima nustatyti pigiausią ataką, nekeliančią didelės grėsmės, labiausiai tikėtiną specifinių įgūdžių nereikalaujančią ataką, pigiausią ataką, kurios sėkmė labiausiai tikėtina, labiausiai tikėtiną teisėtą ataką ir t. t. Kaskart nagrinėjant naujas atakų charakteristikas daugiau sužinosite apie jūsų sistemos saugą.

Kad analizė būtų sėkminga, būtina susieti atakų medį su jūsų žiniomis apie potencialius užpuolikus. Skirtingi užpuolikai turi skirtingo lygio įgūdžius, priėjimą, pinigų ir t. t. Jeigu baiminatės organizuoto nusikalstamumo, turėsite analizuoti brangiai kainuojančias atakas ir įvertinti, kad užpuolikai bus pasirengę pakliūti į kalėjimą. Jeigu baiminatės teroristų išpuolio, jums taip pat teks atsižvelgti į tai, kad potencialūs užpuolikai dėl savo tikslų nebijos net mirti. Tačiau jeigu galvojate apie nuobodžiaujančius studentus, iš neturėjimo ką veikti nusprendusius patikrinti jūsų sistemų saugą, nereikės svarstyti neteisėtų atakų, kyšininkavimo



7.2.1 pav. Pigiausia ataka, nereikalaujanti specialios įrangos.

arba šantažo galimybių. Atakuojančiojo charakteristika lemia, kokias atakų medžio šakas reikės analizuoti.

Atakų medis taip pat leidžia jums žaisti žaidimą „kas, jeigu..?“, įvertinant galimas kontrpriemones. Pavyzdžiui, 7.2.1 pav. tikslo vertė yra 20 000 EUR, kadangi pigiausia ataka, nereikalaujanti specifinių įgūdžių, yra papirkti kodo kombinaciją žinantį asmenį. Kas bus, jeigu įdiegsite kontrpriemonę – mokėsite tam asmeniui daugiau, kad jis nesusigundytų paimti kyšio? Jeigu po kontrprie-

monės įdiegimo papirkimo kaina pasieks 80 000 EUR (vėlgi, tai tik pavyzdys; tikrovėje jums reikės tiksliai įvertinti kontrpriemonės poveikį mazgo vertei), ataka pabrangs iki 60 000 EUR (pvz., už tiek galima pasamdyti banditus, kurie išgautų kodo kombinaciją grasinimais).

PGP pavyzdys

7.3.1 pav. pateikiamas atakų prieš populiarią elektroninio pašto saugos programą PGP medis. Kadangi PGP yra sudėtinga programa, atakų medis taip pat yra sudėtingas, todėl aprašyti jį lengviau, negu pavaizduoti grafiškai. PGP turi keletą saugos funkcijų, taigi čia pateikiamas atakų prieš PGP medis yra tik vienas iš kelių galimų. Šis atakų medis yra orientuotas į tikslą „perskaityti pranešimą, užkoduotą per PGP“. Kiti tikslai gali būti: „pridėti prie pranešimo svetimą parašą“, „pakeisti parašą“, „nepastebimai pakeisti per PGP pasirašytus arba užkoduotus pranešimus“ ir t.t.

Tikslas: Perskaityti pranešimą, užkoduotą PGP
1. Atkoduoti patį pranešimą (ARBA)
1.1. Sulaužyti asimetrinį šifrą (ARBA)
1.1.1. Sulaužyti asimetrinį šifrą jėga (ARBA)
1.1.2. Sulaužyti asimetrinį šifrą matematiškai (ARBA)
1.1.2.1. Sulaužyti RSA (ARBA)
1.1.2.2. Suskaidyti RSA į modulius/apskaičiuoti ElGamal slaptą šifrą.
1.1.3. Iššifruoti asimetrinio šifravimo šifrą (ARBA)
1.1.3.1. Bendroji RSA/ElGamal šifro analizė (ARBA)
1.1.3.2. Ištirti RSA/ElGamal silpnąsias vietas (ARBA)
1.1.3.3. Suderinti atakų prieš RSA/ElGamal laiką.
1.2. Sulaužyti simetrinio šifravimo kodą.
1.2.1. Sulaužyti simetrinio šifravimo kodą jėga (ARBA)
1.2.2. Iššifruoti simetrinio šifravimo šifrą.
2. Nustatyti simetrinį šifrą, naudojamą pranešimams užšifruoti, kitu būdu.

2.1. Apgaulės būdu priversti siuntėją užšifruoti pranešimą viešuoju kodu, kurio privatus kodas jau žinomas (ARBA)
2.1.1. Įtikinti siuntėją, kad suklastotas kodas (kurio privatus kodas yra žinomas) yra gavėjo kodas.
2.1.2. Įtikinti siuntėją užšifruoti pranešimą, naudojant kelis kodus – gavėjo kodą ir kodą, kuris jau yra žinomas.
2.1.3. Pasirūpinti, kad pranešimas būtų užšifruotas keliais atviraisiais kodais, siuntėjui apie tai nežinant.
2.2. Pasirūpinti, kad gavėjas užrašytų užšifruotą simetrinį šifrą (ARBA)
2.3. Patikrinti siuntėjo kompiuterio atmintį (ARBA)
2.4. Patikrinti gavėjo kompiuterio atmintį (ARBA)
2.5. Nustatyti šifrą, pasinaudojus pseudoatsitiktinių numerių generatoriumi (ARBA)
2.5.1. Nustatyti randset.bin vietą pranešimo šifravimo metu (ARBA)
2.5.2. Įdiegti programą (virusą), kuri savavališkai perprogramuotų randset.bin režimą (ARBA)
2.5.3. Įdiegti programą, kuri tiesiogiai veiktų simetrinio kodo pasirinkimą.
2.6. Įdiegti virusą, kuris atskleistų simetrinį šifro raktą.
3. Pasirūpinti, kad gavėjas iššifruotų (padėtų iššifruoti) pranešimą (ARBA)
3.1. Pasirinkto šifruoto teksto nukreipimas prieš simetrinį šifro raktą (ARBA)
3.2. Pasirinkto šifruoto teksto nukreipimas prieš atvirąjį kodą (ARBA)
3.3. Pranešimo originalo išsiuntimas gavėjui (ARBA)
3.4. Gavėjo siunčiamų pranešimų stebėsena (ARBA)
3.5. Pranešimo originalo laukelių „Atsakyti“ arba „Nuo“ klastojimas (ARBA)
3.6. Perskaityti pranešimą po to, kai jį perskaito gavėjas.
3.6.1. Persikopijuoti pranešimą iš gavėjo kietojo disko arba virtualiosios atminties (ARBA)
3.6.2. Persikopijuoti pranešimą iš atsarginių kopijų laikmenų (ARBA)
3.6.3. Stebėti tinklo informacijos srautus (ARBA)
3.6.4. Pasinaudoti elektromagnetinio šnipinėjimo technologija ir perskaityti pranešimą, kai jis parodomas ekrane (ARBA)
3.6.5. Perskaityti išspausdintą pranešimą.
4. Gauti privatų gavėjo šifro kodą.
4.1. Suskaidyti RSA į modulius/apskaičiuoti ElGamal slaptą šifrą (ARBA)
4.2. Gauti privatų kodą iš gavėjo kodų žiedo (ARBA)
4.2.1. Gauti užšifruotą privačių kodų žiedą (IR)
4.2.1.1 Nukopijuoti jį iš vartotojo kietojo disko (ARBA)

4.2.1.2. Nukopijuoti jį iš disko atsarginių kopijų (ARBA)
4.2.1.3. Stabėti tinklo informacijos srautus (ARBA)
4.2.1.4. Įdiegti virusą/kirminą, kuris atskleistų užkoduotą privatų šifro raktą.
4.2.2. Iššifruoti privatų šifro raktą (ARBA)
4.2.2.1. Sulaužyti IDEA šifrą (ARBA)
4.2.2.1.1. Sulaužyti IDEA jėga (ARBA)
4.2.2.1.2. Iššifruoti IDEA.
4.2.2.2 Sužinoti slaptažodį.
4.2.2.2.1. Stebėti klaviatūrą, vartotojui įvedant slaptažodį (ARBA)
4.2.2.2.2. Įtikinti vartotoją atskleisti slaptažodį (ARBA)
4.2.2.2.3. Panaudoti klaviatūros programavimo programą vartotojo slaptažodžiui susekti jo įvedimo metu (ARBA)
4.2.2.2.4. Atspėti slaptažodį.
4.3. Stebėti gavėjo kompiuterio atmintį (ARBA)
4.4. Įdiegti virusą, kuris atskleistų privatų šifro raktą (ARBA)
4.5. Sukurti gavėjui nesaugią atviro/privataus kodo porą.

7.3.1 pav. Atakų, nukreiptų į PGP, medis.

Sudarius atakų medį, iš karto tampa aišku, kad RSA arba IDEA šifravimo algoritmų sulaužymas nėra patys rentabiliausi atakų prieš PGP būdai. Yra daug galimybių perskaityti kieno nors per PGP užšifruotą pranešimą, nelaužant šifro kodo. Galima užfiksuoti ekrano vaizdą, kai jame rodomas iššifruotas pranešimas (pasinaudojus „Trojos arkliu“, pvz., „landas“, „TEMPEST“ gavikliu arba slapta kamera), galima nustatyti slaptažodį įvedimo momentu (vėlgi, per „ landas“ arba tikslinį kompiuterinį virusą), atkurti slaptažodį (sekant klaviatūrą, per „landų“ programas arba „TEMPEST“ gaviklį), arba paprasčiausiai pamėginti sulaužyti slaptažodį jėga (galiu užtikrinti, kad tai pareikalaus daug mažiau pastangų, negu 128 bitų IDEA šifro rakto kodavimas). Matyti, kad algoritmo pasirinkimas ir šifro rakto ilgis PGP saugumui turi mažiausiai įtakos. Bū-

tina užtikrinti ne tik pačios PGP saugumą, ši programa turi būti naudojama fizinėje saugioje aplinkoje.

Atakų medžio sudarymas

Kaip sudaryti tokį atakų medį? Pirma, reikia nustatyti galimus atakos tikslus. Kiekvienam atakos tikslui reikia sudaryti atskirą medį, nors kai kurios galimybės ir prielaidos gali būti identiškos. Tuomet pasistenkite įsivaizduoti visus įmanomus tikslo pasiekimo būdus ir įtraukite juos į schemą. Kartokite šį procesą, kol susiformuos atakų medis. Parodykite sudarytą atakų medžio schemą savo kolegoms, paprašykite jų įvertinti galimybes ir, jeigu jie sugalvotų naujų, įtraukite jas į schemą. Kartokite procesą, jeigu įmanoma, net keletą mėnesių. Visuomet yra galimybė, kad kuri nors ataka bus pamiršta, bet kuo daugiau laiko skirsite atakų medžio sudarymui, tuo ši galimybė bus mažesnė. Kaip ir bet kuriai kitai rizikos analizei, atakų medžio sudarymui reikalinga specifinė mąstysena ir praktiniai įgūdžiai.

Sudarius atakų medį ir jį išanalizavus, pasitelkiant įvairias mazgų vertes (po tam tikro laiko, šios vertės gali kisti, sukaupus daugiau ir tikslesnių žinių apie galimas atakas), atakų medį galima panaudoti, priimant sprendimus dėl saugos priemonių. Šakninių mazgų vertės parodys, ar sistema pažeidžiama. Galima nustatyti sistemos pažeidžiamumą konkrečioms atakoms, pvz., galimybė atspėti slaptažodį. Pasinaudojus atakų medžiu, galima sudaryti sistemos saugos prielaidų sąrašą, pvz., PGP sauga gali reikalauti, kad niekas negalėtų sėkmingai papirkti programuotojų. Galite įvertinti sistemos modifikacijos rezultatus arba nustatyto naujo pažeidžiamumo veiksnį: perskaičiuokite vertes, remdamiesi nauja informacija, ir pamatysite, kaip pasikeičia tikslo įgyvendinimo mazgo

vertė. Taip pat jūs galite lyginti atakas tarpusavyje ir įvertinti, kuri pigesnė, kurios pasisekimas labiau tikėtinas ir pan.

Vienas iš įdomiausių šios analizės aspektų yra tai, kad paaiškėjo, jog sritys, kurias žmonės paprastai laiko pažeidžiamomis, iš tikrųjų tokios nėra. Pavyzdžiui, PGP atveju žmonės paprastai nerimauja dėl šifro rakto ilgio: ar jiems naudoti 1024 bitų RSA, ar 2048 bitų RSA? Tačiau pažvelgus į atakų medį, paaiškėja, kad RSA šifro rakto ilgis iš tiesų nėra svarbus. Yra daug kitokių galimybių atakai įgyvendinti: galima įrengti klaviatūros stebėjimą arba modifikuoti programinę įrangą aukos kietajame diske, ir tai daug paprasčiau, negu sulaužyti RSA atvirąjį kodą. Didinti šifro rakto ilgį nuo 1024 bitų iki 2048 bitų tolygu pastatyti didžiulį stulpą vidury plyno lauko ir tikėtis, kad užpuolikas atsitrenks tiesiai į jį. Daug geriau aplink taikinį pastatyti sieną, nors ir žemesnę. Taigi atakų medis parodo visos sistemos perspektyvą.

Vienas iš didžiausių atakų medžio privalumų yra tai, kad jis leidžia pakartotinai pritaikyti surinktas žinias. Sudarius PGP atakos medį, jį galima naudoti bet kokioms su PGP susijusioms analizėms. PGP atakos medis gali tapti didesnio atakų medžio dalimi. Pavyzdžiui, 7.4.1 pav. parodytas atakų medis, kuriame atakų tikslas – perskaityti konkretų pranešimą, išsiųstą iš „Windows 95“ kompiuterio. Jeigu pažvelgsite į pagrindinių galimybių laukelius, pamatysite, kad į šį medį įeina ir PGP atakavimo, ir seifo atidarymo scenarijai.

Tikslas: Perskaityti konkretų pranešimą, išsiųstą iš „Windows 95“ kompiuterio į kitą kompiuterį
1. Įtikinti siuntėją parodyti pranešimą (ARBA)
1.1. Papirkti vartotoją
1.2. Panaudoti šantažą
1.3. Pagrasinti vartotojui

1.4. Apgauti vartotoją
2. Perskaityti pranešimą jo įvedimo į kompiuterį momentu (ARBA)
2.1. Stebėti kompiuterio ekrano elektromagnetinį spinduliavimą (Kontrpriemonė – „TEMPEST“ kompiuteris)
2.2. Stebėti kompiuterio ekraną vizualiai.
3. Perskaityti pranešimą, išsaugotą siuntėjo kietajame diske (Kontrpriemonė – kietojo disko duomenų šifravimas per SFS) (IR)
3.1. Gauti prieigą prie kietojo disko (Kontrpriemonė – įrengti visų durų ir langų užraktus)
3.2. Perskaityti rinkmeną, užšifruotą per SFS.
4. Perskaityti pranešimą siuntimo metu (Kontrpriemonė: PGP) (IR)
4.1. Perimti pranešimą tranzito taške (Kontrpriemonė: perdavimo lygių šifravimo programa)
4.2. Perskaityti pranešimą, užšifruotą per PGP
5. Įtikinti gavėją parodyti pranešimą (ARBA)
5.1. Papirkti vartotoją
5.2. Panaudoti šantažą
5.3. Pagrasinti vartotojui
5.4. Apgauti vartotoją
6. Perskaityti pranešimą, kai jį skaito gavėjas (ARBA)
6.1. Stebėti kompiuterio ekrano elektromagnetinį spinduliavimą (Kontrpriemonė – „TEMPEST“ kompiuteris) (ARBA)
6.2. Stebėti kompiuterio ekraną vizualiai.
7. Perskaityti pranešimą, išsaugotą gavėjo kietajame diske (Kontrpriemonė – kietojo disko duomenų šifravimas per SFS) (IR)
7.1. Gauti pranešimą, išsaugotą gavėjo kietajame diske po iššifravimo (Kontrpriemonė: šifruoti kietojo disko duomenis per SFS) (IR)
7.1.1. Gauti prieigą prie kietojo disko (Kontrpriemonė – įrengti visų durų ir langų užraktus) (ARBA)
7.1.2. Perskaityti rinkmeną, užšifruotą per SFS.
7.2. Perskaityti iššifruotą pranešimą, saugomą atsarginių kopijų laikmenose.
8. Gauti išspausdintą pranešimą (Kontrpriemonė: saugoti išspausdintus pranešimus seife) (IR)
8.1. Gauti fizinį priėjimą prie seifo turinio
8.2. Atidaryti seifą.

7.4.1 pav. Bendrosios kompiuterių sistemos atakos medis.

Tokia struktūra reiškia, kad jūs nebūtinai turite būti visų sričių specialistas. Jeigu savo sistemoms taikote PGP, jums nebūtina žinoti visų PGP atakos medžio detalių – jums tereikia žinoti šakninio mazgo reikšmę. Jeigu jūs – kompiuterių saugos specialistas, jums nebūtina žinoti, ar sunku išlaužti konkretaus modelio seifą, jums vėlgi užtenka žinoti pagrindinių mazgų vertes. Sudarę atskirų kompiuterinių programų, durų ir langų užraktų, tinklo saugos protokolų ir kitų elementų atakavimo schemų rinkinį, prireikus, galėsite naudotis juo kiekvieną kartą. Nacionalinėms saugos tarnyboms, kurioms reikalingas atakų ekspertinių žinių rūšiavimas, tokia sistema gali būti labai naudinga.

Atakų medžio analizė – tai formali sistemų ir posistemių saugos analizės metodika. Ji suteikia galimybę apgalvoti saugą, įvertinti ir pakartotinai naudoti saugos ekspertų išvadas bei reaguoti į saugos sistemos pokyčius. Sauga – tai ne produktas, tai – procesas. Atakų medis suteikia atspirties tašką perprasti šį procesą.

8. Gero planavimo principai

Toliau išdėstyti principai rekomenduojami kaip gairės, pasirenkant saugos valdymo ir kontrolės priemonių alternatyvas.

Užuot pasirinkus siaurus sprendimus, verčiau rinktis plataus pobūdžio sprendimus. Rinkitės plataus pobūdžio saugos sprendimus, taikytinus visai įmonei, apimančius įvairias programas, skirtingus išteklius ir užtikrinančius apsaugą nuo įvairių pavojų. Nesirinkite tų, kurie saugo tik nuo vienos grėsmės. Tokia praktika beveik visada pasirodo besanti efektyvesnė, negu bandymas sudaryti konkrečioms programoms, ištekliams arba grėsmėms taikomų priemonių rinkinį.

Rinkitės baigtinius sprendimus, o ne tarpiniams etapams taikomus sprendimus. Rinkitės nuo tinklo nepriklausančius šifravimo sprendimus, užtikrinančius pranešimų šifravimą nuo siuntėjo iki gavėjo. Toks pasirinkimas dar labiau pageidautinas, jeigu programa jautri, o tinklas nesaugus. Minėtas sprendimas yra patikimesnis ir efektyvesnis, negu mėginimas nustatyti visus pažeidžiamus tarpinius taškus ir pritaikyti jiems saugos priemones.

Planuokite nuo viršaus į apačią, diekite saugą iš apačios į viršų. Planavimas turi būti grindžiamas funkcijų sklaidos ir jų tobulinimo principu, tuo tarpu sprendimų diegimas turi būti vykdomas pradedant nuo žemiausio lygio. Paslaugas ir įrenginius, kuriuos naudosite ilgą laiką, įdiekite kuo anksčiau.

Darykite viską teisingai iš pirmo karto. Infrastruktūrą įrenkite taip, kad „stovėtų per amžius“. Stenkitės viską padaryti teisingai iš pirmo karto. Tokia strategija patikimesnė ir efektyvesnė, negu „skylių lopymo“ principas, kuris buvo taikomas anksčiau saugos sistemoms.

Planuokite, o ne taisykite. Užuot eksperimentavę, dirbkite pagal planą. Visi reikalingi eksperimentai turi būti tiksliai nustatyti, apibrėžti ir kontroliuojami.

Rinkitės ilgalaikius, o ne trumpalaikius sprendimus. Taikomosios sistemos tampa vis svarbesnės, o aplinka grėsmingesnė ir pavojingesnė. Nors daugeliui gali būti priimtina, kad programa įdiegiama be apsaugos, o saugos priemonių įdiegimui numatomas vėlesnis terminas, nesivadovaukite principu „pagyvensim – pamatysim“.

Saugos priemonės turi pasiteisinti organizacijoje per tam tikrą laiką. Saugos priemonės turi pasiteisinti visos organizacijos mastu, taip pat per visą programos arba įrangos darbo laiką. Remiantis šiuo principu, reikia rinktis saugos priemones, reikalaujančias prognozuojamų ir reguliarių išlaidų grėsmių prevencijai, o ne neprognozuojamų ir nereguliarių išlaidų sistemų atkūrimui. Išlaidos turi pasiteisinti per laikotarpį, nustatytą atsižvelgiant į įprastinį įvykių dažnumą. Pateisinti išlaidas saugos priemonėms tokiu būdu daug paprasčiau, negu pateisinti jas lokaliai arba per trumpą laikotarpį. Siekiant pateisinti išlaidas saugos priemonėms, būtina atsižvelgti į tai, kad programinė įranga tampa vis jautresnė ir įgyja vis daugiau tarpusavio sąsajų, o aplinka, kurioje ji veikia, darosi vis mažiau patikima ir mažiau saugi.

Atsižvelkite į saugos priemonių ekonomiškumą. Sistemų eksploatavimo sauga turi reikalauti kiek galima mažesnių vartotojų pastangų. Pavyzdžiui, vartotojui turėtų pakakti užsiregistruoti įmonėje arba serveryje tik vieną kartą per dieną.

Atsižvelkite į stiliaus vienodumą. Saugos priemonės visoje organizacijoje turi atrodyti panašiai, kaip ir kompiuterinės programos, sistemos ar platformos.

Saugos priemonės turi būti prognozuojamos ir intuityvios. Sistemų veikimas turėtų gerinti procesus. Į sistemas turėtų būti įtrauktos eksploatavimo instrukcijos, kad iškilus būtinybei, vadovas ir vartotojas galėtų lengvai gauti reikalingą informaciją.

Užtikrinti naudojimo paprastumą. Sistemos turi būti sukonstruotos taip, kad būtų lengva dirbti.

Rinkitės mechanizmus, kurių paskirtis akivaizdi. Venkite sudėtingų ir neaiškių mechanizmų, nes jie skatina klaidas arba net padeda nuslėpti piktnaudžiavimo faktus. Pavyzdžiui, rinkitės tokia tvarka: tiesioginė transakcija, EDI, saugaus formato elektroninis paštas, suformatuotas elektroninis paštas, elektroninis paštas, rinkmenų persiuntimas. Tiesioginė transakcija visada akivaizdi ir prognozuojama, nes žinant įvestis, galima lengvai numatyti rezultatus. Tuo tarpu, nors rinkmenos persiuntimo tikslas gali atrodyti akivaizdus, nebūtinai bus taip.

Specialių žinių integravimas. Reikalingos specialios žinios turi būti įtrauktos į dokumentus arba į programinę įrangą.

Rinkitės paprastumą; slėpkite sudėtingumą. Pavyzdžiui, jeigu kitos charakteristikos yra tolygios, užuot pasirinkus sudėtingą mechanizmą, reikia rinktis paprastą. Taip pat geriau rinktis vieną mechanizmą vietoj dviejų, ir integruotą mechanizmą vietoj daugybinių. Pavyzdžiui, geriau, kai parodomas vieningas vaizdas ekrane, o ne daug įvairių skirtingų sistemų vaizdų.

Saugos priemones įrenkite kuo arčiau turto. Paprastai kitoms charakteristikoms esant tolygioms, pageidautina, kad saugos priemonės būtų įrengtos kuo arčiau turto. Kuo arčiau turto jos bus įrengtos, tuo patikimesnė apsauga, tuo didesnis atsparumas trik-

džiams, tuo menkesnė saugos apėjimo galimybė. Saugos priemonės turėtų būti įdiegtos panaudojant tarnybines stotis, o ne vartotojo kompiuterį.

Pasistenkite, kad saugos priemonių valdymas būtų sukoncentruotas ten, kur personalas turi reikiamų žinių ir kur galima stebėti priemonių poveikį. Pavyzdžiui, saugos priemones turėtų valdyti turto savininkas, grupės vadovas, sistemos vadybininkas arba vartotojų vadovas, o ne tariamas saugos administratorius. Netgi turėdamas specialių saugos priemonių administravimo įgūdžių, tariamas saugos administratorius mažiau žinos apie priemonių paskirtį ir jų efektyvumą. Jis negalės stebėti poveikio ir imtis koregavimo.

Rinkitės saugos priemonių ir jos duomenų koncentraciją. Paprastai kitoms savybėms esant vienodoms, reikėtų rinktis kuo paprastesnius sprendimus, paremtus kiek galima mažesniu sudėtinių dalių skaičiumi ir kuo didesne jų koncentracija vienoje vietoje. Tokie sprendimai ne tik efektyvesni ir naudingesni, juos lengviau aprėpti, suvokti ir pademonstruoti. Funkcijos ir duomenys turi būti paskirstyti išimtinai pagal darbo, patikimumo užtikrinimo, prieinamumo, naudojimo arba kontrolės poreikius.

9. Kiekybinių ir kokybinių rizikos analizės metodų palyginimas

Šioje analizėje nebus aptariamos specifinių priemonių ar metodų charakteristikos. Greičiau bus įvertinti bendrojo pobūdžio „už“ ir „prieš“, susiję su kiekybiniais ir kokybiniais metodais. Organizacijos, patenkintos savo rizikos analizės metodais, paprastai yra sukūrusios sąlygiškai paprastas procedūras, kurios gali būti adaptuotos ir pritaikytos įvairiems veiklos padaliniams, taip pat įtraukia į procesą tiek veiklos operacijas išmanančius žmones, tiek tuos, kurie išmano techninius nagrinėjamų sistemų aspektus.

Kokybinė analizė – „už“

- Skaičiavimai, jeigu tokių prireikia, yra paprasti, suprantami ir lengvai atliekami.
- Paprastai nereikia nustatyti piniginės informacijos vertės (jos prieinamumo, konfidencialumo ir vientisumo).
- Nereikia nustatyti kiekybinės grėsmių tikimybės ir jų poveikio vertybėms.
- Nereikia apskaičiuoti rekomenduojamų saugos priemonių kaštų ir atlikti kaštų-naudos analizės.
- Nustatomos svarbiausios rizikos sritys.
- Užtikrinamas proceso ir atsiskaitymo lankstumas.
- Galima vizualiai pateikti rizikos klasifikaciją, užtikrinant geresnį jos suprantamumą.

- Lengviau pasiekti bendrą susitarimą.
- Į procesą lengviau įtraukti žmones, kurie nesijaučia esą saugos arba kompiuterių ekspertais.

Kokybinė analizė – „prieš“

- Rizikos analizė ir jos rezultatai yra subjektyvūs tiek proceso, tiek matavimo prasme. Vengiama naudoti nepriklausomus objektyvius duomenis.
- Nesiekiama nustatyti objektyvios piniginės analizuojamo informacinio turto vertės, todėl pasirinkta vertė gali neatspindėti realios riziką patiriančio turto vertės.
- Nesukuriama bazė rizikos mažinimo priemonių kaštų-naudos analizei, o subjektyvūs vertinimai yra problemiški.
- Neįmanoma objektyviai įvertinti rizikos valdymo priemonių veikimo efektyvumo, kadangi visos priemonės yra subjektyvios.
- Rezultatai priklauso išskirtinai nuo rizikos analizės grupės kompetentingumo.
- Neaiškūs skirtumai tarp įvairių rizikos rūšių.

Kiekybinė analizė – „už“

- Analizė ir jos rezultatai grindžiami nepriklausomais objektyviais procesais ir matavimais. Tokiu būdu įmanoma prasminga statistinė analizė.
- Informacijos (jos prieinamumo, konfidencialumo ir vientisumo) vertė racionaliai išreiškiama pinigine verte, ir tai suprantamiau. Tokiu būdu tampa suprantamesnė ir tikėtino nuostolio reikšmė.
- Užtikrinama patikima rizikos mažinimo priemonių kaštų-naudos analizė. Tokiu būdu sukuriamas pagrindas sprendimų dėl informacijos saugos finansavimo priėmimui.

- Rizikos valdymo priemonių efektyvumas gali būti nustatytas ir įvertintas.
- Rizikos analizės rezultatai išreiškiami vadovybei suprantamomis sąvokomis, piniginėmis išraiškomis, procentais ir metinėmis tikimybėmis. Rizika geriau suprantama.
- Daug pastangų skiriama turto vertei nustatyti ir rizikai mažinti.
- Grėsmių prioritetai nustatomi pagal potencialų finansinį poveikį, vertybių svarba – pagal jų finansinę vertę.
- Vėliau pakartotos analizės tikslumas didėja, kadangi organizacija įgyja patirties ir sukaupia praeities duomenų bazę.

Kiekybinė analizė – „prieš“

- Apskaičiavimai sudėtingi. Jeigu jie nebus suprasti ar tinkamai išaiškinti, vadovybė gali prarasti pasitikėjimą „juodosios dėžės“ skaičiavimų rezultatais.
- Mėginti atlikti kiekybinę rizikos analizę nepraktiška, jei nėra automatizuotų priemonių ir reikalingų žinių. Netgi naudojantis lentelėmis ir statistine programine įranga, kiekybinei rizikos analizei atlikti darbuotojams gali prireikti 10-20 kartų daugiau laiko, negu dirbant su gera automatizuota rizikos analizės programa.
- Būtina surinkti gana daug duomenų apie informacines vertybes ir jų IT aplinką.
- Kol kas nėra sukurta nepriklausomų standartų ir nepriklausomos grėsmių paplitimo bei jų dažnumo duomenų bazės. Taigi vartotojui tenka pasikliauti automatizuotų analizės priemonių gamintojo duomenimis arba pačiam atlikti grėsmių tyrimą.
- Analizė paprastai neįvertina žmonių ir organizacijų bendravimo ypatumų.
- Analizei įgyvendinti reikalingi ekspertai, todėl dalyvius sunku sudominti proceso metu.

- Sunku pakeisti analizės kryptį.
- Grėsmėms priskiriamos poveikio vertės remiasi subjektyvia dalyvių nuomone.
- Patikimiems rezultatams gauti ir bendram susitarimui pasiekti reikia labai daug laiko.
- Rezultatai išreiškiami tik piniginėmis išraiškomis, ir techninės kvalifikacijos neturintiems žmonėms gali būti sunku juos interpretuoti.

10. Bendroji rizikos analizės procedūra

Rizikos analizės procesas turi būti pradėtas vadovybės įsakymu ir remtis informacijos saugos politika (paprastai jis atliekamas, perėjus į iš anksto numatytą etapą, pradedant naują IT projektą arba prieš įgyvendinant esminius pokyčius organizacinėje arba techninėje aplinkoje). Įsakyme turi būti:

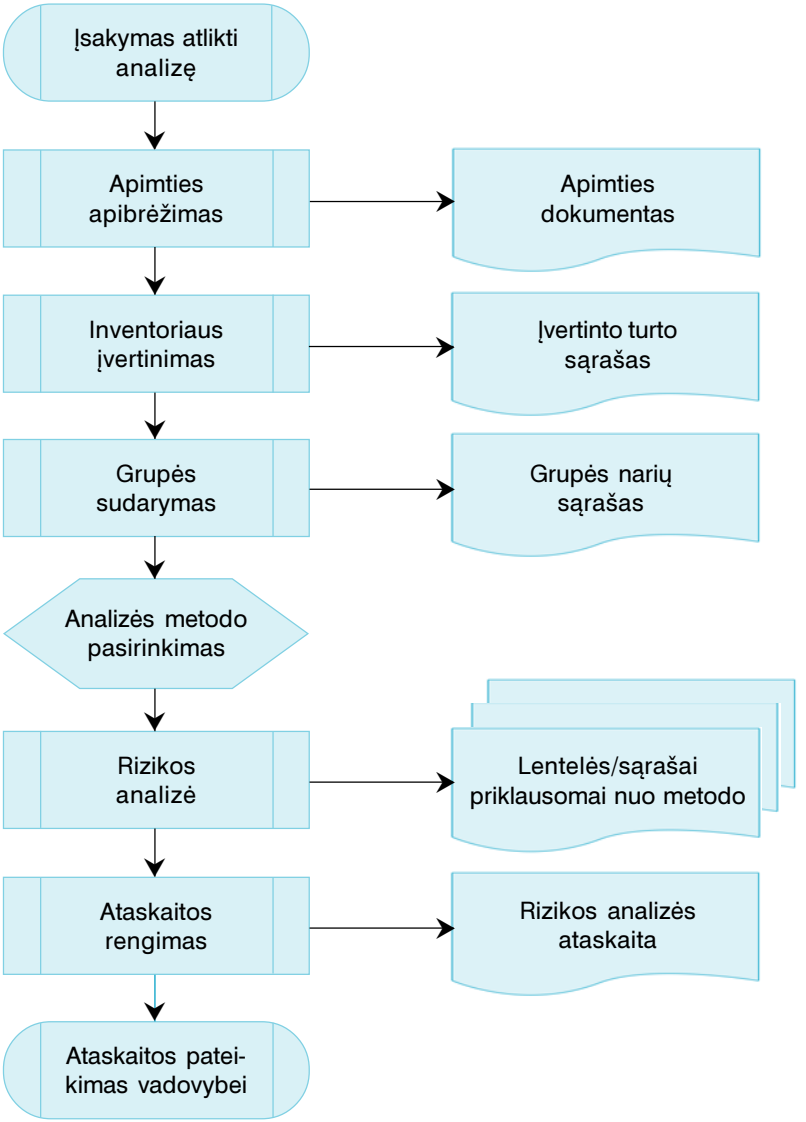
1) nustatyti ir įgalioti (suformuoti grupę, surinkti duomenis apie vertybes ir išanalizuoti atitinkamus dokumentus) atsakingi asmenys atlikti rizikos analizę;
2) apibrėžta analizės apimtis;
3) nustatyta analizės pabaigos data.

Rizikos analizės rezultatas turėtų būti rizikos analizės ataskaitos parengimas. Rizikos analizės ataskaita turėtų sukurti pagrindą sprendimams dėl finansavimo, saugos priemonių pasirinkimo ir rizikos mažinimo procedūrų. Rizikos analizės ataskaitoje turėtų būti:

- Įvadas:
  - Pagrindai: šioje dalyje turėtų būti paaiškinta, kodėl buvo atliekama rizikos analizė ir kokie veiklos poreikiai sąlygojo išteklių skyrimą kokybinei rizikos analizei atlikti.
  - Analizės apimčių apibrėžimas: rizikos analizės apimčių apibrėžimas turėtų būti pateiktas kartu su paaiškinimais, kodėl buvo pasirinkta konkreti apimtis.
  - Metodo paaiškinimas: pasirinkto metodo aprašymas turėtų būti pateiktas kartu su trumpu jo etapų apibūdinimu.

- Bendroji apžvalga: bendras visos procedūros apibūdinimas ir jos santrauka turėtų būti pateikti viename-dviejuose puslapiuose. Tekste turi būti nuoroda į pridedamą grupės narių sąrašą.
- Vertybių nustatymas ir įvertinimas: šioje dalyje turi būti pateiktas analizuojamų vertybių sąrašas ir jų įvertinimas (piniginis, atliekant kiekybinę analizę, ir kokybinis, atliekant kokybinę analizę).
- Grėsmių identifikacija: šioje dalyje turėtų būti aprašyta grėsmių identifikacijos procedūra ir pateikta informacija apie taikytą grėsmių klasifikacijos metodą.
- Nustatyti rizikos veiksniai.
- Saugos priemonių nustatymas.
- Kaštų-naudos analizė.
- Rekomendacijos: šioje dalyje turi būti pateiktos grupės rekomendacijos dėl taikytinų saugos priemonių ir galimų alternatyvų.
- Priedai (rekomenduojami priedai):
  - Grupės narių sąrašas,
  - Sąvokos ir apibrėžimai,
  - Vertybių sąrašas,
  - Grėsmių klasifikacija,
  - Ataskaitos ir lentelės, panaudotos rizikos analizės metu.

Asmuo, atsakingas už rizikos analizės įgyvendinimą, turėtų suplanuoti procesą, vadovauti grupės susirinkimams ir organizuoti bendradarbiavimą su kitais organizacijos padaliniais. Paprastai rizikos analizė neturėtų trukti ilgiau kaip tris savaites. Jeigu rizikos analizė visos organizacijos mastu atliekama pirmą kartą ir analizuotinos vertybės dar nėra nustatytos, rizikos analizės procesas gali trukti iki penkių savaičių.



10.1. pav. Bendroji rizikos analizės procedūra.

1. BS 7799-2:2002 Information security management systems – Specification with guidance for use, BSI, 2002, p. 32
2. Bruce Schneier, Attack Trees, *Dr. Dobb's Journal* December 1999
3. Christopher King, Ertem Osmanoglu, Curtis Dalton, *Security Architecture: Design, Deployment and Operations,* Osborne/McGraw-Hill, 2001, p. 481, ISBN 0072133856
4. CobIT, 3rd edition, Control Objectives, ISACA, 2000, p. 148
5. CobIT Management Gudelines, ISACA, 2000, p. 122
6. CobtIT Online v3.2, www.itgi.org
7. David McNamee, Joseph Pleier and Dr. John D. Tongren, Risk Management: Best Practices, Case Studies and Related Materials, 1999, CDROM only, Pleier corp., www.pleier.com
8. *Guide to BS 7799 Risk Assessment*, British Standards Institution, 2002, p. 47
9. Harold F. Tipton, Micki Krause, *Information Security Management Handbook, Fourth Edition, Volume III,* Auerbach Pub, 2001, p. 848, ISBN 0849311276
10. Harold F. Tipton, Micki Krause, *Information Security Management Handbook,* Auerbach Pub, 1998, p. 729, ISBN 0849399475
11. ISO/IEC Giude 73, *Risk management – Vocabulary – Gudelines for use in standards,* ISO/IEC, 2002, p. 15
12. James C. Barnes, *A guide to business continuity planning*, Wiley, 2001, p. 174, ISBN 9780471530152
13. Jon Williams Toigo, *Disaster Recovery Planning: Strategies for Protecting Critical Information Assets*, Prentice Hall, 2003, p. 512, ISBN 0130462829
14. Kenneth N. Myers, *Manager's Guide to Contingency Planning for Disasters : Protecting Vital Facilities and Critical Operations,* Wiley, 1999, p. 256, ISBN 047135838X
15. LST ISO/IEC 13335-1:2000, *Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 1 dalis. Informacijos technologijų saugos sąvokos ir modeliai (tapatus ISO/IEC TR 13335-1:1996,* Lietuvos standartizacijos departamentas, 2000, p. 17

16. LST ISO/IEC 13335-2:2000, *Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 2 dalis. Informacijos technologijų saugumo valdymas ir planavimas (tapatus ISO/IEC TR 13335-2:1997,* Lietuvos standartizacijos departamentas, 2000, p. 16
17. LST ISO/IEC 13335-3:2000, *Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 3 dalis. Informacijos technologijų saugumo valdymo metodai (tapatus ISO/IEC TR 13335-3:2000,* Lietuvos standartizacijos departamentas, 2000, p. 40
18. LST ISO/IEC 13335-4:2002, *Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 4 dalis. Saugos priemonių parinkimas (tapatus ISO/IEC TR 13335-4:2000,* Lietuvos standartizacijos departamentas, 2002, p. 61
19. LST ISO/IEC 13335-5:2002, *Informacijos technologija. Informacijos technologijų saugumo valdymo gairės. 5 dalis. Tinklo saugumo valdymo patarimai (tapatus ISO/IEC TR 13335-5:2001,* Lietuvos standartizacijos departamentas, 2002, p. 31
20. LST ISO/IEC 17799:2004, *Informacijos technologija. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799:2000)*, Lietuvos standartizacijos departamentas, 2004, p. 62
21. ISO/IEC 21827:2002, Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM®), p.123.
22. *The Security Risk Management Guide v1.1,* Microsoft Corp., 2004, v1.1, Download: http://go.microsoft.com/fwlink/?LinkId=32050
23. Thomas R. Peltier, *Information Security Risk Analysis*, Auerbach Pub, 2001, p. 281, ISBN 0-8493-0880-1

PRIEDAI. Pavyzdinės formos

6.1.1 lentelė. KRA – dešimties žingsnių metodas. Rizikos veiksniai

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

RIZIKOS VEIKSNIAI

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Žalos pobūdis**	**Rizikos veiksnys**

6.1.6 lentelė. Dešimties žingsnių metodas. Saugos priemonių nustatymas

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

SAUGOS PRIEMONIŲ IDENTIFIKAVIMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Galima saugos priemonė**	**Rizikos veiksnys**

6.1.7 lentelė. Dešimties žingsnių metodas. Saugos priemonių nustatymas

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

SAUGOS PRIEMONIŲ NUSTATYMAS

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos kategorija**	**Galima saugos priemonė**	**Priemonės kaštai**

6.2.2 lentelė. KRA – trijų žingsnių metodas. Kokybinės rizikos analizės pavyzdys

FINANSINIAI NUOSTOLIAI

Finansiniai nuostoliai	**Įvertinimas taškais**
Mažiau negu 2 tūkstančiai EUR	1
Tarp 2 ir 15 tūkstančių EUR	2
Tarp 15 ir 40 tūkstančių EUR	3
Tarp 40 ir 100 tūkstančių EUR	4
Tarp 100 ir 300 tūkstančių EUR	5
Tarp 300 tūkstančių ir 1 milijono EUR	6
Tarp 1 ir 3 milijonų EUR	7
Tarp 3 ir 10 milijonų EUR	8
Tarp 10 ir 30 milijonų EUR	9
Daugiau kaip 30 milijonų EUR	10

TEISINĖS PASEKMĖS

Teisinės pasekmės	**Įvertinimas taškais**
Mažiau negu 5 tūkstančiai EUR	1
Tarp 5 ir 10 tūkstančių EUR	4
Tarp 10 ir 50 tūkstančių EUR	5
Tarp 50 tūkstančių ir 1 milijono EUR ir (arba) bausmė IT vadovui	8
Per 1 milijoną EUR ir (arba) bausmė bendrovės vadovybei	10

VERTINGUMAS KONKURENTAMS

Vertingumas konkurentams	Įvertinimas taškais
Mažiau negu 50 tūkstančių EUR	1
Tarp 50 ir 100 tūkstančių EUR	4
Tarp 100 tūkstančių ir 10 milijonų EUR	5
Per 10 milijonų EUR ir (arba) bausmė bendrovės vadovybei	7

VEIKLOS SUTRIKDYMAS

Veiklos sutrikdymas	Įvertinimas taškais
Veiklos sutrikimas, apsiribojantis vienu projektu arba objektu	1
Veiklos sutrikimas, veikiantis kitas grupes arba visą padalinį	2
Veiklos sutrikimas, veikiantis visą organizaciją	3
Veiklos sutrikimas, kuris gali būti paskelbtas vietinėje žiniasklaidoje	5
Veiklos sutrikimas, kuris gali būti paskelbtas nacionalinėje žiniasklaidoje	7
Veiklos sutrikimas, veikiantis akcijų kursą	10

KOKYBINĖS RIZIKOS ANALIZĖS PAVYZDYS

Vertybių grupių įvertinimas, atsižvelgiant į poveikį jų prieinamumui, konfidencialumui ir vientisumui	**Finansiniai nuostoliai**	**Teisinės pasekmės**	**Konfidencialumas**	**Veiklos sutrikdymas**	
Paskelbimas					
Pakeitimas					
Neprieinamumas					
Praradimas					

6.2.7 lentelė. KRA – trijų žingsnių metodas. Saugos spragų analizė

		Žala (poveikis)		
		Maža	**Vidutinė**	**Didelė**
Didelė	3	6	9	
Vidutinė	2	5	8	
Maža	1	4	7	

	Taškai					
	Paskelbimas	**Pakeitimas**	**Neprieinamumas**	**Praradimas**	**Pažeidžiami taškai**	
Analizuojama vertybė:					**Jeigu saugos priemonės netaikomos**	**Jeigu saugos priemonės taikomos**
Rizika:						

6.3.1 lentelė. ISRA – „30 minučių“. Rizikos analizės matrica

	Vientisumas	**Konfidencialumas**	**Prieinamumas**
Nesąmoningi veiksmai			
Sąmoningi veiksmai			

6.4.1 lentelė. Rizikos analizės procesas pagal BS 7799. Vertybių identifikavimas

Vertybė	Vieta	Valdytojas

6.4.2 lentelė. Rizikos analizės procesas pagal BS 7799. Vertybių įvertinimas

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

Vertybė	Konfidencialumas	Vientisumas	Prieinamumas

6.4.3 lentelė. Rizikos analizės procesas pagal BS 7799. Saugos reikalavimų identifikavimas

KLASIFIKACIJA

Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
1	2	3	4	5

Vertybė	**Grėsmė**	**Pažeidžia-mumas**	**Įstatymų/ sutarčių ir veiklos reikalavimai**	**Vertė**

6.4.5 lentelė. Rizikos analizės procesas pagal BS 7799. Saugos rizikos apskaičiavimas

Poveikis	Vertybė	Rizika
Atskleidimas		
Modifikacija		
Neprieinamumas		
Sunaikinimas		

6.4.6 lentelė. Rizikos analizės procesas pagal BS 7799. Rizikos tvarkymo pasirinkčių identifikavimas ir įvertinimas. Saugos priemonių pasirinkimas

Rizika	Rizikos tvarkymas	Saugos priemonė

Va42 Rizikos analizės vadovas. Vilnius: Vaga, 2005. – 160 p.

ISBN 5-415-01827-1

Rizikos analizės vadovas skiriamas valstybinėms institucijoms, kurios valdo informacinių technologijų išteklius ir dirba su įvairios svarbos elektroniniais duomenimis.

Pateiktoje knygoje nagrinėjama rizikos analizės strategija bei metodai, padedantys sumažinti iki leistino lygio nepriimtiną riziką, nurodomi gero planavimo principai.

UDK 65.011

RIZIKOS ANALIZĖS VADOVAS

Autorius Robertas Vageris
Redaktorė Lidija Girevičienė
Dailininkė Deimantė Rybakovienė
Maketavo Jurga Morkūnienė

Leidykla VAGA,
Gedimino pr. 50, LT-01110 Vilnius
el.p. info@vaga.lt; http://www.vaga.lt
tel. +370 5 2498121; faks. +370 5 2498122

Spausdino UAB Vilniaus spauda,
Viršuliškių skg. 80, LT-05131 Vilnius

VIDAUS REIKALŲ MINISTERIJA

Projekto koordinatorius
Vidaus reikalų ministerijos
Informacinės politikos
departamentas

BlueBridge

Projekto vykdytojas
UAB „Blue Bridge“