Mokslas – Lietuvos ateitis / Science – Future of Lithuania
ISSN 2029-2341 / eISSN 2029-2252
2020 Volume 12, Article ID: mla.2019.10562, 1–7
https://doi.org/10.3846/mla.2020.10562

Information technologies and multimedia
Informacinės technologijos ir multimedija

INFORMACINIŲ TECHNOLOGIJŲ RIZIKOS VERTINIMO METODAI IR TOBULINIMO SPRENDIMAI

Roman JEVSEJEV*

Vilniaus Gedimino technikos universitetas, Vilnius, Lietuva

Gauta 2019 m. birželio 21 d.; priimta 2019 m. liepos 1 d.

Santrauka. IT plėtros konteksto atžvilgiu taikomos teisinės priemonės nesugeba išspręsti problemų, su kuriomis tenka susidurti visuomenei, antra vertus, tam tikrais atvejais stabdoma inovacijų plėtra. Informacinių sistemų ir technologijų plėtros intensyvumas reikalauja labai lanksčių ir adaptyvių kibernetinės saugos užtikrinimo metodų taikymo būdų. Vienas iš šių metodų – IT rizikos vertinimas. Šiuo metu yra daug metodologijų, kuriomis remiantis būtų galima efektyviai vertinti kibernetinių grėsmių riziką. Įstaigai, turinčiai daugybę rizikų, skirtingų pozicijų koreliacija gali būti neteisingai įvertinta. Žinomos rizikos matavimas yra dažna rizikos vertinimo praktikos problema. Siekiant sukurti paprastą IT rizikos vertinimo metodą, straipsnyje nagrinėjami esami IT rizikos vertinimo metodai, siūlomi IT rizikos vertinimo sprendimai ir pateikiami praktinio pritaikymo rezultatai.

Reikšminiai žodžiai: IT rizikos, metodas, kibernetinis saugumas, pažeidžiamumas, grėsmės.

Įvadas

Informacinių technologijų taikymas bendruomenės socialiniuose ir kultūriniuose procesuose suformavo nesankcionuotos prieigos ir duomenų praradimo rizikos valdymo aspektą. Kuo aukštesnis socialinių procesų informatizavimo lygis, tuo didesnė rizika ir platesnis kibernetinės saugos grėsmių spektras. Leidžiamasis organizacijų interesų kibernetinio aktyvumo lygis rizikos valdymo srityje pastaruoju metu sukelia daug ginčų, mokslinių diskusijų, susijusių su kibernetinių rizikų valdymo tema. Informacinių sistemų ir technologijų plėtros intensyvumas reikalauja labai lanksčių ir adaptyvių rizikos valdymo užtikrinimo metodų taikymo būdų.

Vienas iš šių metodų – IT rizikos vertinimas, pvz., ISO/IEC 27005, NIST SP 800-30 ir kt. Rizikos valdytojai kartais daro klaidų vertindami nuostolių tikimybę ar dydį (Stulz, 2008). Tai įvyksta dėl neteisingo rizikos veiksnių paskirstymo. Įstaigai, turinčiai daugybę rizikų, skirtingų pozicijų koreliacija gali būti neteisingai įvertinta. Žinomos rizikos matavimas yra dažna rizikos valdymo praktikos problema.

1. IT rizikos samprata

ISO standartai apibūdina IT riziką kaip tam tikrą grėsmę organizacijai, pasinaudojant turto ar turto grupės pažeidžiamumu. IT rizika vertinama pagal įvykio tikimybės ir jos pasekmių santykį (International Organization for Standardization [ISO], 2018). Jungtinių Amerikos Valstijų nacionalinio saugumo sistemų komitetas įvairiuose dokumentuose IT rizikos sąvoką traktuoja įvairiai. „Rizika – tai tam tikros grėsmės neigiamo poveikio IS galimybė, naudojanti ypatingą pažeidžiamumą“ (Committee on National Security Systems, 2015).

Nacionalinio saugumo telekomunikacijų ir informacinių sistemų saugumo instrukcijoje naudojamas tikimybės aspektas, panašus į NIST SP 800-30: „Rizika – tai grėsmės tikimybės derinys, nurodantis grėsmės įvykio sukeltą neigiamą poveikį ir pasekmes“ (Committee on National Security Systems, 2005). IT rizikos apibrėžimas taip pat traktuojamas įvairiai:

- pagal NIST SP 800-30 rizika – tai tikimybė, kad tam tikras grėsmės šaltinis turi ypatingą galimą pažeidžiamumą, dėl kurio organizacijai daromas neigiamas poveikis (National Institute of Standards and Technology, 2012);
- pagal NIST FIPS 200 rizika yra poveikio lygis organizacinėms operacijoms (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtui ar asmenims, atsirandantis dėl grėsmės ar jos tikimybės informacinei sistemai (National Institute of Standards and Technology, 2014).

*Autorius susirašinėti. El. paštas *romanjevsejev@gmail.com*

2. IT rizikos vertinimo metodų nagrinėjimas

Daugumos organizacijų situaciją apsunkina programinės įrangos, skirtos IT rizikai įvertinti ir valdyti, funkcionalumo apribojimai. Didelis programinės įrangos kiekis kuriamas nesivadovaujant IT rizikos vertinimo metodologija ir informacijos saugumo standartais, todėl netinkamai nustatomas ne tik IT rizikos lygis, bet ir atitikties laipsnis konkrečiam standartui. Metodai, kuriais remiantis vykdoma kibernetinės rizikos analizė (Chandrashekhar, Sachin Kumar ir Huded, 2015), yra CORAS, OCTAVE, CRAMM, nagrinėjamas jų funkcionalumas.

2.1. CORAS metodas

CORAS yra aiškiai apibūdinta knygoje „A Platform for Risk Analysis on Security Critical Systems – Model-based Risk Analysis Targeting Security“ (Bjørn, 2002). Metodas buvo sukurtas kaip „Information Society Technologies“ programos dalis (Dimitrakos, Ritchie, Raptis ir Stølen, 2002). Jos esmė yra „Event-Tree-Analysis“, Markovo grandinės, „HazOp“ ir „FMECA“ rizikos analizės metodų pritaikymas, tobulinimas ir derinimas. Metode taikoma UML technologija. Ji yra pagrįsta Australijos / Naujosios Zelandijos standartu „AS/NZS 4360: 1999 Risk Management“ ir „ISO/IEC 17799-1: 2000 Code of Practice for Information Security Management“. Šiame standarte atsižvelgiama į rekomendacijas, pateiktas „ISO/IEC TR 13335: 2001 Guidelines for the Management of IT Security“ ir „IEC 61508: 2000 Functional Safety of Electrical/Electronic/Programmable Safety Related“.

Vadovaujantis CORAS, informacinės sistemos vertinamos ne tik kaip panaudotos technologijos, bet kaip sudėtingas kompleksas, kuriame atsižvelgiama į žmogiškuosius veiksnius. Šio metodo taisyklės įgyvendinamos „Windows“ ir „Java“ programomis (CORAS Tool 2.0, n.d.). CORAS nenumato metodų veiksmingumo ir likutinės rizikos vertinimo būdų, tačiau jo privalumas tas, kad, taikant CORAS metodą, programinė įranga yra nemokama, ji nereikalauja didelių išteklių ją diegiant ir naudojant.

2.2. OCTAVE metodas

OCTAVE apima aktyvų informacijos savininkų dalyvavimą, nustatant kritinės informacijos turtą ir su tuo susijusią riziką. Metodas buvo sukurtas „Carnegie Mellon“ universiteto Programinės įrangos inžinerijos institute. Pagrindiniai OCTAVE elementai:

- kritinio informacijos turinio nustatymas;
- kritinio informacijos turto grėsmių nustatymas;
- pažeidžiamumų, susijusių su kritiniu informacijos turtu, nustatymas;
- rizikos vertinimas, susijęs su kritiniu informacijos turtu.

OCTAVE užtikrina didelį lankstumą, pasirenkant kriterijus, kuriuos įmonė gali naudoti taikydama metodą savo poreikiams. Metodas skirtas didelėms įmonėms, o jos populiarumas paskatino sukurti OCTAVE-S versiją mažoms įmonėms. Yra komercinių programinės įrangos produktų, įgyvendinančių OCTAVE nuostatas.

Nepaisant to, kad OCTAVE metodas atitinka rizikos kriterijus, rizikų stebėjimas yra jos silpnoji dalis (Alberts ir Dorofee, 2001, 2002). OCTAVE numato reguliarų IT rizikos vertinimą ir rezultatų atnaujinimą. Nustatant rizikos vertinimo strategiją, OCTAVE daro prielaidą, kad rizikų mažinimo priemonė naudojama tik rizikoms sumažinti ir priimti. Metodas nesuteikia aiškaus nurodymo, kaip pastebėti pavojų, tačiau pabrėžia rizikos dėl pavojaus egzistavimo svarbą.

2.3. CRAMM metodas

CRAMM metodą 1985 m. sukūrė Didžiosios Britanijos centrinės kompiuterių ir telekomunikacijų agentūros. Jis buvo taikomas tiek didelėms, tiek mažoms organizacijoms vyriausybiniame ir komerciniame sektoriuose.

CRAMM apima technologijas, kurių grėsmės ir pažeidžiamumas įvertinamas taikant netiesioginius veiksnius, be to, galima patikrinti rezultatus. Metodas turi informacinių sistemų saugumo perspektyvos modeliavimo mechanizmą, kuris naudoja išsamią atsakomųjų priemonių duomenų bazę. CRAMM vertina riziką ir efektyvumą, taikydamas įvairių atsakomųjų priemonių derinį.

Taikant CRAMM metodą, visiškai neatsižvelgiama į darbuotojų informavimą informacijos saugumo srityje, patvirtinamuosius dokumentus, pvz., verslo procesų aprašymą arba atliktų IT rizikos vertinimo ataskaitas (Insight Consulting, 2003). CRAMM apima tik rizikų mažinimo metodus. Rizikos vertinimo metodai, pvz., vengimas ar priėmimas, nėra priimtini. Taikant šį metodą pasitelkiami kiekybiniai ir kokybiniai IT rizikos įvertinimo metodai, tačiau nėra apibrėžtų sąlygų, kuriomis įmonės gali remtis.

3. IT rizikos vertinimo metodo patobulinimo sprendimai

IT rizikos vertinimo metodas patobulintas taikant analitinį rizikos būdą, kai rizikos rodikliai nustatomi esant objekto informacijos apibrėžtumui, naudojant bendrus rodiklių nustatymo kriterijus, sudarančius sąlygas taikyti metodą skirtingoms organizacijoms.

Siūlomą metodą sudaro šie 5 etapai:

1. IT rizikos apimties nustatymas. Vykdoma organizacijos aukščiausio lygio vadovo ir teisininko apklausa, nustatomi organizacijos IT rizikos vertinimo poreikiai. Siekiant nustatyti IT infrastruktūros reikalavimus, formuojama įmonės charakteristika, kuria remiantis nustatomos objektyvios organizacijos rizikos ir jų priklausomybė nuo duomenų kategorijos.
2. Organizacijos techninių dokumentų analizė. Analizuojama organizacijos IT ir saugumo tvarka.
3. Pažeidžiamumo ir grėsmių nustatymas. Remiantis techninių dokumentų analize, nustatomi pažeidžiamumai, grėsmės. Duomenims nustatyti taikomas matematinio modelio analitinis metodas, esant visiškam duomenų neapibrėžtumui, kai duomenims nustatyti taikomos ekspertinės žinios, analizuojant ir užpildant duomenų lenteles.

4. Personalo apklausa. Remiantis atlikta analize formuojama apklausos anketa, kuri bus pateikiama IT infrastruktūros techninio palaikymo specialistams. Naudojantis anketomis įvertinami pažeidžiamumo išnaudojimo asmenų potencialas, taikomų prevencijos priemonių efektyvumas, informacinių sistemų kritiškumas, procesų pažeidžiamumo lygis, organizacijos veiklos reguliavimas ir reputacijos lygis.
5. Galimo žalos lygio ir grėsmių realizavimo tikimybės įvertinimas. Galimi kiekvienos rizikos nuostoliai išreiškiami balais nuo 0,25 (maži nuostoliai) iki 1 (dideli nuostoliai). Kriterijai pateikti 1 ir 2 lentelėje. Įvertinama dalyvaujant atitinkamų kvalifikacijų specialistams.

Grėsmės realizavimo tikimybė skaičiuojama remiantis ISO/IEC 27005 standarto C ir D priedų duomenimis. Suminė grėsmių realizavimo tikimybė lygi 4 balams. Įvertinimas taip pat vyksta dalyvaujant atitinkamos kvalifikacijos specialistams.

Nustatytų grėsmių skaičius išreiškiamas kintamuoju n, kuris proporcingai kinta grėsmės realizavimo tikimybės $P(t)$ atžvilgiu. Pažeidžiamumų skaičius išreiškiamas kintamuoju i. Atitinkamai grėsmių skaičiui pažeidžiamumai kinta proporcingai $P(t)$ reikšmei. Grėsmių ir pažeidžiamumų reikšmės apvalinamos iki sveikojo skaičiaus, taikant standartinį apvalinimo metodą. Formuojamam metodui taikoma (1) formulė.

4. Patobulinto metodo praktinis pritaikymas ir gauti rezultatai

Metodo praktinis pritaikymas vykdomas pagal pasiūlytus rizikos vertinimo metodo etapus. Duomenys šiame skyriuje yra pakoreguoti pateiktos informacijos konfidencialumo tikslais. „Įmonė A“ – energetikos įmonė, kurios veiklos sritis – karšto ir geriamojo vandens tiekimas, geriamojo vandens gavyba, šilumos gamyba ir nuotekų tvarkymas. Dėl plataus veiklos spektro įmonės veikla išskaidyta į 11 padalinių.

Pagal įmonės charakteristiką ir analizę nustatomos galimos rizikos, pateiktos 3 lentelėje. Nustatytoms rizikoms atrankos būdu priskiriamos aktualios grėsmės ir pažeidžiamumai. Pavyzdžiui, laboratorijos duomenų suklastojimas negali būti susietas su radiacijos spinduliuotės poveikiu, todėl tai nėra pažeidžiamumas, bet personalo stebėjimo mechanizmų trūkumas – tai galimas pažeidžiamumas, dėl kurio gali įvykti neteisėtas duomenų apdorojimas ir gali kilti laboratorijos duomenų suklastojimo rizika.

1 lentelė. Galimo nuostolių lygio kriterijai (pavyzdys)
Table 1. Criteria for potential loss level (example)

Duomenų kategorija	Informacinės sistemos kritiškumams	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	Galimas nuostolių lygis *S*
Komercinė paslaptis	Labai kritinė	Kelių procesų sutrikimai, veiklos sustabdymas	Neplaninės komisijos patikros, baudos	Reputacija blogina-ma tarptautiniu lygiu	Labai aukštas
Gamybinė paslaptis	Kritinė	Proceso sutrikimai	Auditai, padidintas dėmesys	Reputacija blogina-ma regioniniu lygiu	Aukštas
Tarnybinė informacija	Iš dalies kritinė	Proceso greičio sumažinimas	Nurodymai be baudų ir auditų	Reputacija blogina-ma internetu	Vidutinis
Atvira informacija	Nekritinė	Nėra įtakos	Nėra jokių nurodymų	Reputacija neblogi-nama	Mažas

2 lentelė. Grėsmių realizavimo tikimybės kriterijai (pavyzdys)
Table 2. Criteria for probability of realization of threats (example)

Aktyvių grėsmių skaičius (T-Threats)	Pažeidžiamumų skaičius (A-Assets)	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas	Grėsmės realizavimo tikimybė *P(t)*
75–100 % (Tmax)	75–100 % (Amax)	Administratorius	Žemas	Labai aukšta inci-dento tikimybė
50–75 % (Tmax)	50–75 % (Amax)	Kiti darbuotojai	Vidutinis	Aukšta incidento tikimybė
25–50 % (Tmax)	25–50 % (Amax)	Buvusieji darbuotojai; programinės įrangos kūrėjai	Aukštas	Vidutinė incidento tikimybė
25 % (Tmax) < = 1 grėsmė	25 % (Amax) < = 1 grėsmė	Nekvalifikuoti asmenys	Labai aukštas	Žema incidento tikimybė

3 lentelė. Nustatytos rizikos, grėsmės ir pažeidžiamumai pagal ISO/IEC 27005
Table 3. Identified risks, threats and vulnerabilities in accordance with ISO/IEC 27005

Nr.	Veiklos procesai / nustatytos rizikos	Pažeidžiamumų skaičius	Grėsmės
Gamybiniai procesai			
1.	Technologijos valdymo sutrikimas	20	12
2.	Technologijos stebėjimo sutrikimas	11	9
Laboratoriniai procesai			
3.	Laboratorijos veiklos sutrikimas	10	7
4.	Laboratorijos duomenų praradimas / suklastojimas	14	7
Paslaugų teikimo procesai			
5.	Paslaugų teikimo valdymo sutrikimas	12	7
6.	Paslaugų teikimo stebėjimo sutrikimas	6	6
Klientų aptarnavimo procesai			
7.	Klientų aptarnavimo procesų sutrikimas	23	9
8.	Klientų duomenų nutekėjimas / praradimas	16	10
Vidaus resursų ir išteklių valdymo procesai			
9.	Finansų apskaitos valdymo procesų sutrikimas	17	10
10.	Finansų apskaitos duomenų praradimas	18	9
11.	Atsargų ir išteklių valdymo procesų sutrikimas	14	12
12.	Atsargų ir išteklių valdymo duomenų praradimas	18	9
13.	Personalo valdymo procesų sutrikimas	14	12
14.	Personalo duomenų praradimas	18	9
Ryšių su visuomene procesai			
15.	Ryšių su visuomene duomenų paviešinimas	12	11
16.	Ryšių su visuomene duomenų praradimas	7	5

Nustatyta, kad daugiausia pažeidžiamumų sukelia klientų aptarnavimo procesų rizika – 23 vnt. Antroje vietoje pagal pažeidžiamumų skaičių yra technologijų valdymo sutrikimų rizika – 20 vnt. Trečią vietą užima finansų apskaitos duomenų praradimo, atsargų ir išteklių valdymo duomenų praradimo, personalo duomenų praradimo rizikos – 18 vnt. Mažiausią pažeidžiamumų skaičių turi paslaugų teikimo stebėjimo rizika – 6 vnt.

Atsižvelgiant į grėsmių skaičių nustatyta, kad daugiausia grėsmių turi technologijos, atsargų ir išteklių, personalo valdymo procesų sutrikimų rizikos, kurių grėsmių dydis sudaro 12 vnt. Ryšių su visuomene duomenų paviešinimo rizikos grėsmių skaičius – 11 vnt. Klientų duomenų nutekėjimo / praradimo, finansų apskaitos valdymo sutrikimų rizikos turi po 10 grėsmių.

Įmonėje buvo apklausti IT specialistai, atsakingi už IT infrastruktūros funkcionavimą. Klausimyną sudarė 12 klausimų, sugrupuotų pagal įmonės vykdomus procesus, kurie kelia rizikas.

Apklausos rezultatai pateikti 4 lentelėje. Apklausos metu nustatytas pažeidžiamumų išnaudojimo asmenų potencialas, taikomų prevencijos priemonių efektyvumas, informacinių sistemų kritiškumas, procesų pažeidžiamumų lygis, organizacijos veiklos reguliavimas ir reputacijos lygis.

Pagal gautus apklausos duomenis nustatyta, kad didžiausią IS kritiškumą turi klientų aptarnavimo procesai – 3 balai, finansų apskaitos valdymo procesai, atsargų ir išteklių valdymo procesai – 2,75 balo. Trečioje vietoje – laboratorijos veikla, finansų apskaitos bei atsargų ir išteklių duomenys, ryšių su visuomene duomenų paviešinimas – 2,5 balo.

Didžiausią pažeidžiamumo lygį turi daug procesų: laboratorijos veiklos sutrikimas, klientų aptarnavimo, finansų apskaitos valdymo, atsargų ir išteklių valdymo, personalo valdymo procesų sutrikimai, kurių dydis – 4 balai.

Pagal veiklos reguliavimą didžiausius rezultatus turi klientų aptarnavimo procesų sutrikimas, klientų duomenų nutekėjimas / praradimas, finansų apskaitos duomenų praradimas, finansų apskaitos, atsargų ir išteklių valdymo procesų sutrikimai, kurių dydis – 3,5 balo.

Didžiausią įtaką organizacijos reputacijai turi paslaugų teikimo valdymo sutrikimai, personalo valdymo sutrikimai, kurių rezultatų dydis lygus 4 balams.

Technologijos stebėjimas, klientų, finansų apskaitos, atsargų ir išteklių, personalo valdymo duomenys turi didžiausią išnaudojimo asmenų potencialą – 4 balai.

Pagal taikomų prevencijos priemonių efektyvumą pirmauja 7 procesai. Mažiausią efektyvumą turi paslaugų stebėjimo procesas – 3,5 balo.

Gauti rezultatai rodo, kad didžiausią grėsmės realizavimo tikimybę sudaro technologijos valdymo procesai – 0,84 balo. Antroje vietoje personalo valdymo procesai – 0,78 balo. Trečią vietą užima technologijos stebėjimo sutrikimai – 0,75 balo. 5 ir 6 lentelėje pateikti grėsmės realizavimo tikimybės ir galimo žalos lygio kintamųjų skaičiavimai. Mažiausią

4 lentelė. Personalo apklausos rezultatai
Table 4. Staff survey results

Nr.	Nustatytos rizikos	Apklausos rezultatai					
		IS kritiškumas	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas
1.	Technologijos valdymo sutrikimas	1,5	3	2,5	1	3	2,5
2.	Technologijos stebėjimo sutrikimas	0,5	1	1	1	4	2,5
3.	Laboratorijos veiklos sutrikimas	2,5	4	3	3	3	2,5
4.	Laboratorijos duomenų praradimas / suklastojimas	1,5	2	2	1	3	1
5.	Paslaugų teikimo valdymo sutrikimas	1,5	2	2	4	3	2,5
6.	Paslaugų teikimo stebėjimo sutrikimas	1,5	1,5	1	1	3	3,5
7.	Klientų aptarnavimo procesų sutrikimas	3	4	3,5	3	3	0
8.	Klientų duomenų nutekėjimas / praradimas	0,5	2	3,5	3	4	0
9.	Finansų apskaitos valdymo procesų sutrikimas	2,8	4	3,5	3	3	0
10.	Finansų apskaitos duomenų praradimas	2,5	3	3,5	3	4	0
11.	Atsargų ir išteklių valdymo procesų sutrikimas	2,8	4	3,5	3	3	0
12.	Atsargų ir išteklių valdymo duomenų praradimas	2,5	2	2,5	1	4	0
13.	Personalo valdymo procesų sutrikimas	2	4	2	4	3	2,5
14.	Personalo duomenų praradimas	1,5	2	2,5	1	4	0
15.	Ryšių su visuomene duomenų paviešinimas	2,5	1	2,5	2	2,5	1,5
16.	Ryšių su visuomene duomenų praradimas	2,5	1,5	1	1	3	1,5

5 lentelė. Grėsmės realizavimo tikimybės skaičiavimai
Table 5. Calculations of threat realization probability

Nr.	Nustatytos rizikos	Aktyvių grėsmių kiekis	Aktyvių pažeidžiamumų kiekis	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas	*P(t)*
1.	Technologijos valdymo sutrikimas	1,00	0,87	0,75	0,75	0,84
2.	Technologijos stebėjimo sutrikimas	0,75	0,48	1	0,75	0,75
3.	Laboratorijos veiklos sutrikimas	0,58	0,43	0,75	0,75	0,63
4.	Laboratorijos duomenų praradimas / suklastojimas	0,58	0,61	0,75	0,25	0,55
5.	Paslaugų teikimo valdymo sutrikimas	0,58	0,52	0,75	0,75	0,65
6.	Paslaugų teikimo stebėjimo sutrikimas	0,50	0,26	0,75	1	0,63
7.	Klientų aptarnavimo procesų sutrikimas	0,75	0,00	0,75	0	0,38
8.	Klientų duomenų nutekėjimas / praradimas	0,83	0,70	1	0	0,63
9.	Finansų apskaitos valdymo procesų sutrikimas	0,83	0,74	0,75	0	0,58
10.	Finansų apskaitos duomenų praradimas	0,75	0,78	1	0	0,63
11.	Atsargų ir išteklių valdymo procesų sutrikimas	1,00	0,61	0,75	0	0,59
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,75	0,78	1	0	0,63
13.	Personalo valdymo procesų sutrikimas	1,00	0,61	0,75	0,75	0,78
14.	Personalo duomenų praradimas	0,75	0,78	1	0	0,63
15.	Ryšių su visuomene duomenų paviešinimas	0,92	0,52	0,75	0,5	0,67
16.	Ryšių su visuomene duomenų praradimas	0,42	0,30	0,75	0,5	0,49

grėsmės realizavimo tikimybę sudaro klientų aptarnavimo procesų sutrikimas – 0,38 balo.

Nustatyta, kad didžiausią žalą sudaro klientų aptarnavimo procesų sutrikimai – 4,5 balo, laboratorijos veiklos, finansų apskaitos bei atsargų ir išteklių valdymo procesų sutrikimai – 4 balai, finansų apskaitos duomenų praradimas – 3,75 balo. Mažiausią žalą sudaro technologijos stebėjimo sutrikimai – 1,75 balo. Pagal NIST 800-30 formulę $R = P(t) \times S$ vertinamos rizikos. Rizikų vertinimo rezultatai pateikti 7 lentelėje.

Nustatyta, kad didžiausią riziką turi personalo valdymo procesų sutrikimas – 2,73 balo, technologijos valdymo ir laboratorijos veiklos sutrikimai – 2,53 balo. Finansų apskaitos duomenų praradimo rizika – 2,37 balo, atsargų ir išteklių valdymo procesų sutrikimų ir duomenų prara-

6 lentelė. Galimo žalos lygio skaičiavimai
Table 6. Calculations of the potential level of damage

Nr.	Nustatytos rizikos	Duomenų kategorija	IS kritiškumas	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	*S*
1.	Technologijos valdymo sutrikimas	0,75	0,5	0,75	0,75	0,25	3,00
2.	Technologijos stebėjimo sutrikimas	0,75	0,25	0,25	0,25	0,25	1,75
3.	Laboratorijos veiklos sutrikimas	0,75	0,75	1	0,75	0,75	4,00
4.	Laboratorijos duomenų praradimas / suklastojimas	0,75	0,5	0,5	0,5	0,25	2,50
5.	Paslaugų teikimo valdymo sutrikimas	0,75	0,5	0,5	0,5	1	3,25
6.	Paslaugų teikimo stebėjimo sutrikimas	0,75	0,5	0,5	0,25	0,25	2,25
7.	Klientų aptarnavimo procesų sutrikimas	1,00	0,75	1	1	0,75	4,50
8.	Klientų duomenų nutekėjimas / praradimas	1,00	0,25	0,5	1	0,75	3,50
9.	Finansų apskaitos valdymo procesų sutrikimas	0,50	0,75	1	1	0,75	4,00
10.	Finansų apskaitos duomenų praradimas	0,50	0,75	0,75	1	0,75	3,75
11.	Atsargų ir išteklių valdymo procesų sutrikimas	0,50	0,75	1	1	0,75	4,00
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,50	0,75	0,5	0,75	0,25	2,75
13.	Personalo valdymo procesų sutrikimas	0,50	0,5	1	0,5	1	3,50
14.	Personalo duomenų praradimas	0,50	0,5	0,5	0,75	0,25	2,50
15.	Ryšių su visuomene duomenų paviešinimas	0,25	0,75	0,25	0,75	0,5	2,50
16.	Ryšių su visuomene duomenų praradimas	0,25	0,75	0,5	0,25	0,25	2,00

7 lentelė. Rizikos vertinimo rezultatai
Table 7. Results of risk assessment

Nr.	Nustatytos rizikos	*P(t)*	*S*	*R*
1.	Technologijos valdymo sutrikimas	0,84	3,00	2,53
2.	Technologijos stebėjimo sutrikimas	0,75	1,75	1,30
3.	Laboratorijos veiklos sutrikimas	0,63	4,00	2,52
4.	Laboratorijos duomenų praradimas / suklastojimas	0,55	2,50	1,37
5.	Paslaugų teikimo valdymo sutrikimas	0,65	3,25	2,12
6.	Paslaugų teikimo stebėjimo sutrikimas	0,63	2,25	1,41
7.	Klientų aptarnavimo procesų sutrikimas	0,38	4,50	1,69
8.	Klientų duomenų nutekėjimas / praradimas	0,63	3,50	2,21
9.	Finansų apskaitos valdymo procesų sutrikimas	0,58	4,00	2,32
10.	Finansų apskaitos duomenų praradimas	0,63	3,75	2,37
11.	Atsargų ir išteklių valdymo procesų sutrikimas	0,59	4,00	2,36
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,63	2,75	1,74
13.	Personalo valdymo procesų sutrikimas	0,78	3,50	2,73
14.	Personalo duomenų praradimas	0,63	2,50	1,58
15.	Ryšių su visuomene duomenų paviešinimas	0,67	2,50	1,68
16.	Ryšių su visuomene duomenų praradimas	0,49	2,00	0,99

dimo rizika lygi 2,36 balo. Mažiausią riziką turi ryšių su visuomene duomenų praradimas – 0,99 balo. Laboratorijos duomenų praradimo / suklastojimo rizika – 1,37 balo ir technologijos stebėjimo sutrikimo rizika – 1,30 balo.

Išvados

IT rizika, arba kibernetinė rizika, yra tiesiogiai susijusi su informacinėmis technologijomis. Informacija vertinama kaip vertingas ir svarbus turtas: žinių tobulinimas, ekonomikos augimas ir skaitmeninė revoliucija paskatino organizacijas plačiau naudoti informacijos, apdorojimo ir informacinių technologijų priemones. Yra daug metodų, kurie atitinka kibernetinio saugumo rizikos vertinimo poreikius. Kiekvienas metodas turi savo privalumų ir trūkumų. Skirtingoms organizacijoms metodai gali būti taikomi kaip atskira platforma, kuri adaptuojama pagal organizacijos poreikius, atsižvelgiant į organizacijos priklausomybę nuo informacijos. Taikant patobulintą metodą, nustatyta, kad tiriamos organizacijos personalo valdymo procesų sutrikimų rizikos lygis yra aukštas. Taikant pasiūlytas priemones, rizika sumažinta iki vidutinio lygio. Rizikų, pažeidžiamumo ir grėsmių nustatymo bei įvertinimo etapai leido tiksliai nustatyti IT infrastruktūros rizikas organizacijoje. Iš patobulinto ir pritaikyto metodo jautrumo analizės rezultatų matyti rizikos rezultatų priklausomybė nuo dviejų rizikos rodiklių – grėsmės realizavimo tikimybės – $P(t)$ ir galimos žalos lygio – S. Pasiūlytą metodą rekomenduojama taikyti pirminiam IT rizikos vertinimui, metodo rezultatai identifikuoja kritines IT infrastruktūros sritis.

Literatūra

Alberts, C. J., & Dorofee, A. J. (2001). *OCTAVE method implementation guide version 2.0*. Carnegie Mellon University. https://doi.org/10.21236/ADA634140

Alberts, C. J., & Dorofee, A. J. (2002). *Managing information security risks – the OCTAVE approach*. Boston: Addison Wesley. https://doi.org/10.21236/ADA634134

Bjørn, A. G. (2002). CORAS, a platform for risk analysis on security critical systems – model-based risk analysis targeting security. In *International Conference on Telemedicine (ICT2002)*, Regenburg. Prieiga per internetą: http://www.ewics.org/attachments/security-subgroup-boppard-2002/CORAS+framework.pdf

Chandrashekhar, A. M., Sachin Kumar, H. S., & Huded, Y. (2015). Advances in information security risk practices. *International Journal of Advanced Research in Datamining and Cloud Computing*, *3*, 47-48.

Committee on National Security Systems. (2015, April 6). *Committee on National Security Systems (CNSS) Glossary* (No. 4009). Prieiga per internetą: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Committee on National Security Systems. (2005). *National Policy on certification and Accreditation of National Security Systems* (No. 6). Prieiga per internetą: http://www.cnss.gov/Assets/pdf/CNSSP-6.PDF

CORAS Tool 2.0. (n.d.). *Programinės įrangos paketai*. Prieiga per internetą: https://sourceforge.net/projects/coras/

Dimitrakos, T., Ritchie, B., Raptis, D., & Stølen, K. (2002). Model based security risk analysis for web applications: the CORAS approach. In *EuroWeb 2002 Conference*, St Anne's College, Oxford, UK.

Standards Australia/Standards New Zealand Committee. (1999). *Risk management* (No. 4360). Prieiga per internetą: http://www.epsonet.eu/mediapool/72/723588/data/2017/AS_NZS_4360-1999_Risk_management.pdf

International Organization for Standardization. (2000). *Information technology — Security techniques — Code of practice for information security management* (No. 1799-1). Prieiga per internetą: http://antoanthongtin.vn/Portals/0/UploadImages/kiennt2/TieuChuanKyThuat/TCQT/ISO%20IEC%2017799-2005%20en.pdf

International Organization for Standardization. (2001). *Information technology — Guidelines for the management of IT Security* (No. TR 13335). Prieiga per internetą: https://www.sis.se/api/document/preview/897890/

Insight Consulting. (2003). *CRAMM expert walkthrough and overview*. Prieiga per internetą: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html

International Electrotechnical Commission. (1999). *Functional safety of electrical/electronic/programmable electronic safety-related systems* (Nr. 61508). Prieiga per internetą: http://www.cechina.cn/eletter/standard/safety/iec61508-2.pdf

International Organization for Standardization. (2018). *Information technology – Security techniques – Information security risk management* (ISO/IEC No. 27005). Prieiga per internetą: https://view.elaba.lt/standartai/view?search_from=aleph&id=1273235

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST SP No. 800-30). Prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2014). *FIPS publication 200: minimum security requirements for federal information and information systems*. Prieiga per internetą: https://csrc.nist.gov/publications/detail/fips/200/final

Stulz, M. (2008). Risk management failures: what are they and when do they happen? *Journal of Applied Corporate Finance*, *4*, 58-67. https://doi.org/10.2139/ssrn.1278073

INFORMATION TECHNOLOGY RISK ASSESSMENT METHODS AND IMPROVEMENT SOLUTIONS

R. Jevsejev

Abstract

The legal tools applied in the context of IT technology development failing to solve the problems facing society. On the other hand, the development of innovation is sometimes hindered. The intensity of the development of information systems and technologies requires highly flexible and adaptive approaches to cybersecurity. One of these approaches is IT risk assessment. There are currently many methodologies that can be used to effectively assess cyber threats. For institutions with multiple exposures, the correlation between different positions may not be correctly estimated. Measuring known risk is a common problem in risk assessment practice. In order to develop a simple IT risk assessment method, the article examines existing IT risk assessment methods, proposes IT risk assessment solutions and presents the results of practical application.

Keywords: IT risks, method, cybersecurity, vulnerabilities, threats.