ISSN: 2029-2341 / eISSN: 2029-2252

VILNIUS TECH
Vilnius Gediminas Technical University

SCIENCE – FUTURE of LITHUANIA

2025
Volume 17
Article ID: mla.2025.25252
Pages 1–9
https://doi.org/10.3846/mla.2025.25252

Information technologies and multimedia
Informacinės technologijos ir multimedija

ŽMOGIŠKOJO FAKTORIAUS ĮTAKA PRIIMANT SPRENDIMUS KIBERNETINĖS SAUGOS PRATYBOSE

Karina KULIKAUSKAITĖ ✉

Vilniaus Gedimino technikos universitetas, Vilnius, Lietuva

▪ gauta 2025 m. spalio 7 d.
▪ priimta 2025 m. lapkričio 7 d.

Santrauka. Kibernetinė sauga – tai tarpdisciplininė sritis, apimanti informacinių technologijų, kriminalistikos, incidentų valdymo aspektus bei žmogiškąjį faktorių. Kibernetinėje saugoje sprendimų priėmimą veikia specialisto techninės žinios, kompetencijos, profesinės veiklos patirtis. Tačiau ekstremaliose bei sudėtingose situacijose priimamus sprendimus veikia emocijos, motyvacija, socialiniai įgūdžiai, kognityviniai gebėjimai. Todėl šiame darbe buvo tiriamas žmogiškasis faktorius, darantis įtaką kibernetinės saugos pratybų dalyvių sprendimų priėmimui, ir pasiūlytas daugiamatis sprendimo priėmimo karkasas. Atliktas tyrimas analizuojant kibernetinių saugos pratybų „Gintarinė migla" duomenis parodė, jog integruotas techninių kompetencijų ir žmogiškojo faktoriaus vertinimas leidžia tiksliau nustatyti kibernetinio saugumo specialisto sprendimų priėmimą ir jį prognozuoti. Nustatyta, kad analizuojant sprendimų priėmimą kibernetinės saugos pratybose būtina atsižvelgti į žmogiškąjį faktorių. Tyrimo rezultatai gali būti naudojami tobulinant kibernetinės saugos specialistų rengimo metodologijas ir programas.

Reikšminiai žodžiai: kibernetinės saugos pratybos, žmogiškasis faktorius, sprendimų priėmimas.

✉Autorius susirašinėti. El. paštas *karina.kulikauskaite@vilniustech.lt*

1. Įvadas

Didėjantis kibernetinių išpuolių ir atakų skaičius bei jų sudėtingumas rodo, kad įmonės ir organizacijos privalo stiprinti kibernetinę gynybą ir nuolat tobulinti kibernetinės saugos specialistų kompetenciją. Kibernetinių atakų skaičius per pastaruosius penkerius metus išaugo 90 %. Ypač padaugėjo atakų, nukreiptų prieš valstybinio sektoriaus organizacijas (European Union Agency for Cybersecurity [ENISA], 2023; IBM Trust Center, 2022). Tai rodo, kad šis sektorius yra taip pat patrauklus kaip ir finansinis, o daugelis valstybinių organizacijų kibernetinei saugai skiria per mažai dėmesio. Reikia atkreipti dėmesį ir į tai, kad organizacijų naudojamų komunikacinių kanalų ir socialinių platformų įvairovė didina kibernetinio pažeidžiamumo perimetrą ir sukuria papildomas galimybes kenkėjiškai veiklai bei neteisėtai prieigai prie duomenų. Baltijos šalyse situaciją dar labiau apsunkina politiškai motyvuotos kibernetinės atakos, kurių skaičius nuolat auga (Lietuvos Respublikos krašto apsaugos ministerija, 2023, 2024). Siekiant užkardinti kibernetinius išpuolius ir atakas būtina didinti organizacijų atsparumą ir gebėjimą prisitaikyti prie globalių ir regioninių kibernetinio saugumo pokyčių.

Kibernetinė sauga – tai tarpdisciplininė sritis, jungianti informacines technologijas, kibernetinių grėsmių ir rizikų valdymą, skaitmeninių nusikaltimų tyrimą, kognityvinius mokslus, žmogiškąjį faktorių (Kott et al., 2014). Vien tik techninių kibernetinės saugos specialisto žinių ir kompetencijų nepakanka, siekiant užtikrinti visapusišką atsparumą kibernetinėms grėsmėms, o ypač sofistikuotoms kibernetinėms atakoms (Barford et al., 2010; Colabianchi et al., 2025). Sprendimų priėmimas kibernetinės saugos srityje glaudžiai susijęs su žmogiškaisiais faktoriais, tokiais kaip emociniu atsparumu, streso valdymu ir gebėjimu priimti sprendimus esant įtampai (Dutt et al., 2013; Von Solms & Van Niekerk, 2013). Kognityviniai procesai, susiję su kibernetinės saugos specialistų elgsena, daro reikšmingą poveikį kibernetinės gynybos efektyvumui ir atsparumui. Empiriniai tyrimai rodo, kad 49 % kibernetinių pažeidimų lemia netyčinės žmogaus klaidos (Langlois et al., 2023). Specialistų klaidos leidžia piktavaliams tęsti kibernetines atakas prieš organizacijos informacines sistemas ir bandyti gauti prieigą prie duomenų. Apklausų rezultatai rodo, kad trečdalis kibernetinio saugumo specialistų iššūkius sieja ne tik su IT techninių žinių spragomis, bet ir su socialiniais bei psichologiniais veiksniais. Tyrimais nustatyta, kad IT sistemų atsparumas kibernetinėms grėsmėms tiesiogiai priklauso ne tik nuo specialistų techninio pasirengimo, bet ir nuo jų emocinio atsparumo bei gebėjimo priimti sprendimus stresinėse situacijose (Hagen et al., 2025). Atlikto tyrimo

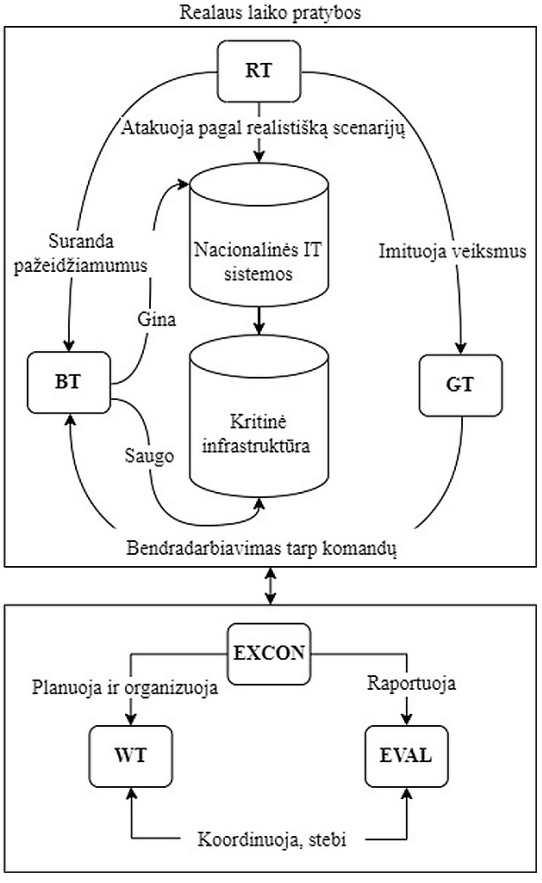
metu net 45 % dalyvių patvirtino patiriantys aukštesnį nei vidutinį streso lygį, o daugiau nei 75 % jautė reikšmingą streso padidėjimą. Lietuvos valstybinės duomenų apsaugos inspekcijos duomenimis, 2024 m. – 52 %, 2023 m. – 72 %, o 2022 m. – 60 % visų asmens duomenų saugos pažeidimų Lietuvoje kilo dėl žmogiškųjų klaidų. Tik 15 % visų pažeidimų buvo susiję su išorinėmis kibernetinėmis atakomis, įskaitant socialinę inžineriją ir išpirkos reikalaujančias programas. VDAI, išanalizavusi per 2025 m. I pusmetį gautus pranešimus apie asmens duomenų saugumo pažeidimus, nustatė, kad 57 % pažeidimų įvyko dėl žmogiškosios klaidos, t. y. dėl žmogaus padaromų veiksmų, kurie pasireiškia neapdairumu, nežinojimu, kad veiksmai gali sukelti asmens duomenų saugumo pažeidimus, taip pat dėl veiksmų, nuo kurių apsaugoti negali taikomos techninės ir organizacinės priemonės. Ataskaitoje pažymėta, kad 11 % pažeidimų įvyko dėl kitų priežasčių, t. y. dėl IT sistemų klaidų, netinkamai atliktų programavimo darbų (Valstybinė duomenų apsaugos inspekcija, 2023, 2024, 2025). Pateikti duomenys akivaizdžiai rodo, kad siekiant didinti priimamų sprendimų tikslumą ir efektyvumą, būtina daugiau dėmesio skirti žmogiškojo faktoriaus valdymui, įskaitant kibernetinės saugos specialisto psichologinį pasirengimą, emocinį atsparumą ir sprendimų priėmimo kultūros stiprinimą vidinės organizacijos struktūroje. Siekiant stiprinti organizacijų atsparumą ir sumažinti pažeidžiamumus informacinių sistemų apsaugos srityje, būtina skirti dėmesį emociniam intelektui, streso valdymui ir sprendimų priėmimo procesams (Scott & Bruce, 1995).

Kibernetinės saugos pratybos (KSP) laikoma viena iš praktinio mokymosi priemonių, skirtų kritinės infrastruktūros, karinių struktūrų specialistams gilinti kibernetinės saugos žinias. Per kibernetinės saugos pratybas kuriami incidentų scenarijai, kurių metu vertinami kibernetinės saugos specialistų gebėjimai identifikuoti, analizuoti, užkardyti kibernetinius incidentus, koordinuoti veiksmus bei bendradarbiauti. Pratybose atakuojama ir ginama hipotetinė IT infrastruktūra, jose atakų scenarijai dažniausiai kuriami ankstesnių pratybų pagrindu, bet apima ir naujus kibernetinius incidentus, atspindinčius dabartines saugos tendencijas ar geopolitines grėsmes. Pratybose imituojamos realios kibernetinės atakos, todėl čia taikomas holistinis atvejais grįstas mokymasis. Sprendimų priėmimo efektyvumas kibernetinių saugos pratybų metu vertinamas pagal iš anksto nustatytus rodiklius. Tyrimai rodo, kad žmogiškieji veiksniai, tokie kaip streso valdymas, emocinis atsparumas ir kognityviniai šališkumai, daro tiesioginę įtaką sprendimų kokybei (Khadka & Ullah, 2025; Hagen et al., 2025). Kibernetinės saugos pratybose šie veiksniai tampa ypač aktualūs, nes dalyviai treniruojasi realaus laiko sąlygomis, kuriomis yra riboti resursai, žmogiškieji ištekliai, užduočių atlikimo laikas, aplinka. Visa tai sukelia papildomą įtampą ir stresą, dėl to sprendimų priėmimo efektyvumas krenta. Visi anksčiau paminėti faktai rodo, kad, analizuojant kibernetinės saugos pratybų metu priimtus sprendimus, būtina atsižvelgti į žmogiškojo faktoriaus įtaką, todėl šio tyrimo tikslas – ištirti žmogiškojo faktoriaus poveikį priimant sprendimus kibernetinės saugos pratybų metu ir pasiūlyti daugiamatį sprendimo priėmimo vertinimo modelį, įtraukiant žmogiškąjį faktorių kaip papildomą komponentą (Khadka & Ullah, 2025). Tyrimo metu gauti rezultatai prisideda prie kibernetinės saugos specialistų rengimo metodologijos ir vertinimo sistemos tobulinimo.

2. Žmogiškasis faktorius kibernetinės saugos pratybose

Kibernetinio saugumo pratybos tampa vis aktualesnės, augant sudėtingų kibernetinių grėsmių kiekiui bei sparčiai tobulėjant puolimo technologijoms, todėl kibernetinės saugos pratybų tikslas – didinti organizacijų darbuotojų kibernetinį atsparumą ir parengti juos galimoms kibernetinėms grėsmėms ir atakoms. Pratybos leidžia ne tik tikrinti IT infrastruktūros atsparumą, bet ir lavinti sprendimų priėmimo, streso valdymo bei tarpusavio komandų bendradarbiavimo gebėjimus (Maennel et al., 2023). Skirtingai nei teoriniai mokymai, kibernetinės saugos pratybos suteikia dalyviams galimybę veikti nuolat dinamiškai besikeičiančioje, spaudimą keliančioje aplinkoje, imituojančioje realaus kibernetinio incidento eigą.

Pratybų metu modeliuojami scenarijai yra nuolat atnaujinami, kad atspindėtų naujausias kibernetines taktikas ir taktikų keitimąsi. Kibernetinės saugos pratybose dalyviai suskirstomi į specializuotas komandas, kurios atlieka skirtingas funkcijas. Komandos sėkmė priklauso nuo jos narių



1 paveikslas. Kibernetinės saugos pratybų procesas

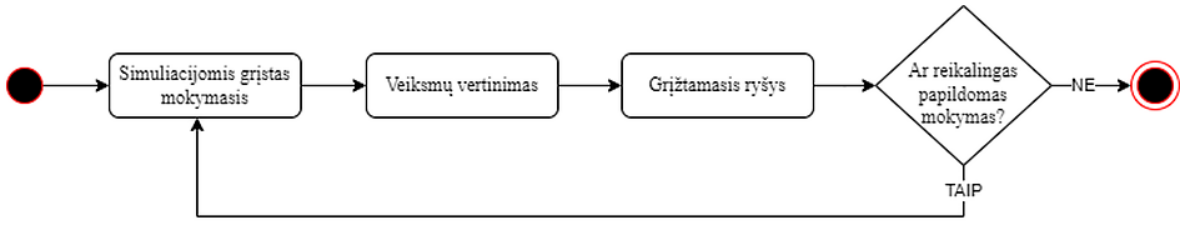
gebėjimo dirbti kartu, bendradarbiauti, pasidalinti užduotimis, informacija, padėti komandos nariui ir t. t. Kibernetinės saugos pratybų schema, komandų tipai, jų funkcijos ir pratybų vykdymo procesas pavaizduotas 1 paveiksle. Kibernetinės saugos pratybų procesas inicijuojamas, kai Raudonoji komanda (RT) pradeda vykdyti imituojamas kibernetines atakas, nukreiptas į IT infrastruktūros pažeidžiamas vietas. Mėlynoji komanda (BT) gina ir stengiasi apsaugoti IT infrastruktūrą bei informacines sistemas nuo kibernetinių atakų taikydama gynybines strategijas. Žalioji komanda (GT) stebi infrastruktūrą ir tiekia Mėlynajai komandai (BT) techninius duomenis, metrikas ir informaciją apie vykstančius incidentus. Tai leidžia įvertinti atakos apimtis ir nuostolius. Visų komandų veiklą centralizuotai koordinuoja Pratybų valdymo komanda (EXCON), kuri stebi komandinį darbą, vykdo informacinio srauto kontrolę. Baltoji komanda (WT) atsakinga už pratybų planavimą, organizavimą ir sklandžią jų eigą. Pratybų eigą stebi, analizuoja ir vertina kiekvienos komandos veiksmus Vertinimo komanda (EVAL). Ji taip pat analizuoja iš anksto nustatytus komandų vertinimo kriterijus bei skaičiuoja kibernetinio saugumo veiksmingumo rodiklius.

Mokymasis kibernetinių pratybų metu vyksta remiantis uždaru simuliacijomis ir problemomis grįstu mokymosi principu, kur kiekvienos pratybų dienos pabaigoje EVAL komanda pateikia grįžtamąjį ryšį, dienos užduočių analizę, pagrindines klaidas, taip pat teikiamos rekomendacijos kitos dienos pratyboms (2 pav.). Toks iteracinis mokymosi metodas užtikrina, kad iškilę klausimai ir problemos būtų sprendžiamos greitai.

Pratybų metu vertinamos ne tik profesinės kompetencijos, bet ir žmogiškieji faktoriai. 1 lentelėje pateikiamos kibernetinių saugos pratybų komandų funkcijos ir komandų vertinimo kriterijai. Matome, kad, vertinant komandos darbą, atsižvelgiama ne tik į technines kompetencijas, t. y. vykdomų atakų efektyvumą, incidentų valdymą, sistemų atkūrimą, bet vertinami ir žmogiškieji komandos faktoriai: kūrybiškumas, reagavimo greitis, komunikacija, objektyvumas.

Žmogiškasis faktorius priimant sprendimus pratybose tampa svarbus dar ir dėl to, kad, imituojant realias atakas, specialiai sukuriamos stresinės sąlygos, dalyvius veikia psichologinis spaudimas, tai daro įtaką sprendimų priėmimui, todėl tik koordinuoti veiksmai, komandinis darbas ir bendradarbiavimas gali užtikrinti, kad atakos bus tinkamai užkardintos, o incidentai išspręsti (Granåsen & Andersson, 2015; Dykstra & Lyn Paul, 2018).

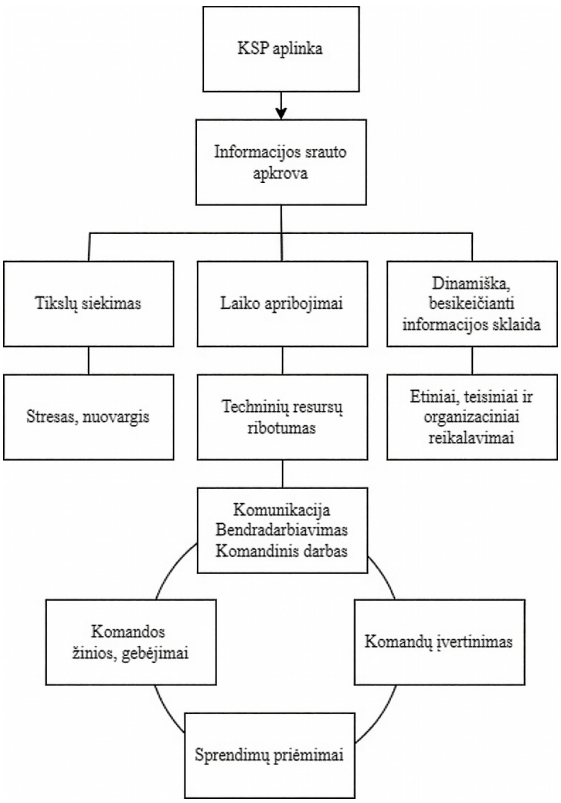
Kibernetinės saugos pratybose aplinka yra greitai besikeičianti, t. y. pratybų dalyviai gauna didelį informacijos srautą, bet kartu juos riboja nustatyta pratybų trukmė, o tai verčia greitai apdoroti informaciją ir priimti sprendimus (3 pav.). Be to, fizinis ir emocinis išsekimas, informacinio srauto apkrova ir laiko trūkumas sukuria kognityvinę įtampą. Riboti techniniai ištekliai ir personalas (dažnai ne visi komandos nariai gali dalyvauti pratybose) sukelia stresą. Ilgai besitęsiančios pratybos sukelia nuovargį. Dalyvių veiksmus riboja organizatorių nustatyti etiniai, teisiniai ir organizaciniai reikalavimai, kibernetinės saugos reglamentai, tai taip pat generuoja psichologinį spaudimą. Riboto laiko sąlygomis komunikacija, bendradarbiavimas ir komandinis darbas tampa problemiški, o komandų vertinimas ir reitingavimas skatina rezultatų siekimą bet kokia kaina. Apibendrinant galima teigti, kad kibernetinės saugos pratybos sukuria sudėtingą mokymosi ir mokymo aplinką, todėl dalyvių žinios, gebėjimai ir sprendimų priėmimas turi būti vertinami remiantis ne tik formaliais rezultatais, bet įtraukiant žmogiškuosius faktorius, darančius įtaką sprendimų priėmimų kokybei pratybų metu.



2 paveikslas. Mokymosi modelis kibernetinių pratybų metu

1 lentelė. Kibernetinės saugos pratybų komandų funkcijos ir vertinimo kriterijai

Komanda	Funkcijos	Vertinimo kriterijai
Raudonųjų komanda (*Red Team*, RT)	Simuliuoja priešiškas grėsmes ir įsilaužimus	Kūrybiškumas, pažeidžiamumų identifikavimas, atakų efektyvumas
Mėlynųjų komanda (*Blue Team*, BT)	Atsakinga už sistemų apsaugą, incidentų atpažinimą, atsaką	Reagavimo greitis, incidentų valdymas, sistemų atkūrimas
Žaliųjų komanda (*Green Team*, GT)	Teikia techninę paramą ir analizę	Metrikų kokybė, komunikacijos tikslumas, situacijos stebėsena
Baltųjų komanda (*White Team*, WT)	Vertina komandų veiklą, fiksuoja klaidas ir teikia grįžtamąjį ryšį	Objektyvumas, analizės kokybė, grįžtamojo ryšio pateikimas
Pratybų valdymo grupės (EVAL, EXCON *Team*)	Koordinuoja pratybų scenarijų eigą ir palaiko dinamišką mokymosi procesą	Vertina visų komandų atliktų veiksmų kokybę ir pasekmes, didelis dėmesys komandiniam darbui, informacijos dalinimuisi ir bendradarbiavimui

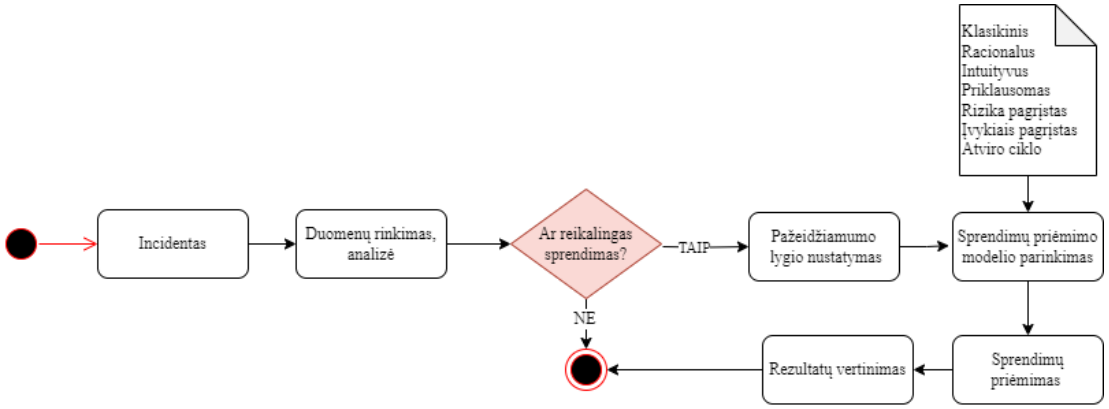


3 paveikslas. Aplinkos faktoriai kibernetinių pratybų metu

3. Sprendimų priėmimas kibernetinių pratybų metu

Sprendimų priėmimas kibernetinėje saugoje apibrėžiamas kaip veiklos procesas, kurio metu identifikuojama problema, renkama informacija, nustatomas pažeidžiamumo lygis, apibrėžiamos ir vertinamos alternatyvos ir, pritaikius sprendimo priėmimo metodą, priimamas sprendimas (Ganin et al., 2020). Procesas užbaigiamas validuojant pasirinktą sprendimą (4 pav.). Kibernetinio saugumo specialistai nuolat priima sprendimus kibernetinės saugos pratybų metu sprendžiant incidentus, todėl svarbu tinkamai suprasti sprendimų priėmimo proceso eigą ir atlikti holistinį sprendimų priėmimo vertinimą, analizuojant ne tik techninius įgūdžius ir patirtį, bet ir žmogiškąjį faktorių, pratybų aplinką bei emocijas. Yao et al. (2025) apibūdino sprendimų priėmimą kaip kognityvinę procedūrą, vaizduojančią, kaip žmogus susidoroja su problema. Tai reiškia, kad kiekvienas žmogus taiko skirtingus informacijos suvokimo ir analizės metodus. Moksliniuose šaltiniuose nagrinėjami tokie sprendimų priėmimo modeliai: klasikinis, racionalus, intuityvus, priklausomas, rizika ir įvykiais paremtas, atviro ciklo sprendimų priėmimo modelis.

Klasikinis sprendimų priėmimo modelis paremtas klasikine sprendimų teorija, kurią taikant daroma prielaida, kad sprendimų priėmėjas yra logiškai mąstantis ir racionalus, o sprendimas priimamas atsižvelgiant į organizacijos interesus (Harren, 1979). Šis modelis nėra realistiškas, bet naudojamas lyginti su kitais sprendimų priėmimo metodais. Taikant racionalų sprendimų priėmimo modelį siekiama priimti pagrįstą ir optimalų sprendimą, paremtą faktais, įrodymais bei nuoseklia logine seka. Modelis susideda iš septynių žingsnių, t. y. problemos identifikavimas, informacijos rinkimas, alternatyvų nustatymas, įrodymų analizė, sprendimo pasirinkimas, veiksmų įgyvendinimas, rezultatų peržiūra. Šis modelis pasižymi ciklišku, informacijos analize ir vertinimu, o tai leidžia valdyti sudėtingus sprendimus, tai ypač aktualu kibernetinėje saugoje. Intuityvus sprendimų priėmimo modelis grindžiamas emocijomis, nuojauta. Jis labai priklauso nuo prognozių, instinktų ir emocijų. Sprendimai priimami impulsyviai, reaguojant į emocijas, o ne susitelkiant į informacijos srautą ir jo apdorojimą. Priklausomas sprendimų priėmimo modelis grindžiamas tuo, kad sprendimas gali būti priimamas priklausomas nuo tam tikrų priežasčių – aplinkybių, konteksto, autoritetingų asmenų rekomendacijų, t. y. jį veikia kognityviniai šališkumai (Harren, 1979). Asmuo pasirenka veiksmų kryptį remdamasis kitų įtaka, taip sumažindamas sprendimo riziką bei sudėtingumą. Kibernetinio saugumo srityje dažnai taikomas rizika pagristas sprendimų priėmimo modelis. Šiame modelyje alternatyvos formuojamos atsižvelgiant į tikslus ir kontekstą, o jų vertinimas atliekamas remiantis rizikos metrika. Tačiau šio metodo taikymas yra gana sudėtingas dėl neapibrėžtumo, nes alternatyvos yra dažnai nežinomos ir neaiškios. Įvykiais paremtas sprendimų priėmimo modelis taip pat dažniausiai naudojamas kibernetinio saugumo gynybos pratybose. Jis paremtas atviruoju ciklu ir panašus į racionalaus sprendimų priėmimo modelį, tačiau rišasi prie kibernetinio saugumo architektūros.



4 paveikslas. Sprendimo priėmimo procesas kibernetinių pratybų metu

4. Sprendimo priėmimo karkasas

Remiantis ISO/IEC 27035-1:2023 standartu, kibernetinės saugos incidentas – tai vienas ar keli įvykiai, kurie neigiamai veikia ar gali paveikti informacijos konfidencialumą, vientisumą ar prieinamumą. Incidentų valdymas yra viena svarbiausių kibernetinės saugos pratybų dalių, su kuria nuolat susiduria Mėlynoji ir Žalioji komandos. Incidentų valdymas apima nuoseklią veiksmų seką, t. y. monitoringą ir informacijos rinkimą, incidento identifikavimą, klasifikavimą ir prioritetų nustatymą, alternatyvų analizę ir pasirinkimą, veiksmų įgyvendinimą bei incidento įvertinimą ir mokymąsi (Ahmad et al., 2021; ENISA, 2021). Sprendimų priėmimas sprendžiant incidentus susijęs su žmogiškuoju faktoriumi, emociniu atsparumu, gebėjimu priimti sprendimus stresinės būsenos, todėl analizuojant sprendimų priėmimo seką, būtina įvertinti ir žmogiškąjį faktorių.

5 paveiksle pateiktas pasiūlytas sprendimų priėmimo karkasas kibernetinės saugos pratybose, kuris iliustruoja, kad sprendimų priėmimas yra ne tik linijinis techninis procesas, susidedantis iš anksčiau paminėtų žingsnių, bet glaudžiai sąveikauja su žmogiškuoju faktoriumi, kuris apima keturias pagrindines grupes, t. y. kognityvinius, psichologinius, socialinius ir organizacinius, profesinius ir techninius veiksnius.

Žmogiškojo faktoriaus įtaka kognityviniuose veiksniuose apima situacinę įžvalgą, kognityvinį krūvį, šališkumus ir intuiciją. Šie veiksniai lemia pratybų dalyvio gebėjimą identifikuoti anomalijas, greitai apdoroti informaciją incidento metu, tačiau kognityviniai šališkumai bei informacijos pertekliaus sukeltas krūvis didina klaidų tikimybę ir mažina priimtų sprendimų tikslumą (Greitzer et al., 2019).

Situacinė įžvalga siejama su gebėjimu suvokti ir interpretuoti pratybų aplinką bei įžvelgti ryšius tarp įvykių, net jei gauta informacija fragmentiška ar neapibrėžta. Pavyzdžiui, kibernetinės saugos pratybų metu komandų dalyviai nuolat analizuoja žurnalinius įrašus, tinklo srautą, vartotojų veiklą, komandos narių komunikaciją, todėl tinkama situacinė įžvalga leidžia pasirinkti prioritetinius kriterijus, pavyzdžiui, ar pirmiausia skirti resursus kibernetinės atakos stabdymui, ar analizuoti incidento priežastis. Psichologiniai veiksniai susiję su streso ir laiko trūkumo valdymu, emociniu atsparumu, motyvacija, nerimu ir baime suklysti. Patiriamas stresas ir nerimas pratybų metu silpnina analitinį mąstymą, o emocinis atsparumas leidžia efektyviau priimti sprendimus dinamiškose situacijose. Socialiniai ir organizaciniai veiksniai glaudžiai susiję su komandinės dinamikos, lyderystės, aiškaus vaidmenų pasiskirstymo, komunikacijos efektyvumu ir organizacine kultūra. Tyrimai rodo, kad sprendimų efektyvumą incidentų metu labiausiai lemia aiški vaidmenų struktūra komandoje. Komandiniu pasitikėjimu grįsta kultūra skatina bendradarbiavimą ir mokymąsi iš klaidų.

Profesiniai ir techniniai faktoriai susiję su KSP specialistų turimomis žiniomis, įgūdžiais, nuolatiniais mokymais, pratybomis, adaptyvumu bei turima darbo patirtimi. Šie žmogiškieji faktoriai lemia, ar priimtas sprendimas bus

5 paveikslas. Sprendimų priėmimo karkasas, įvertinant žmogiškąjį faktorių

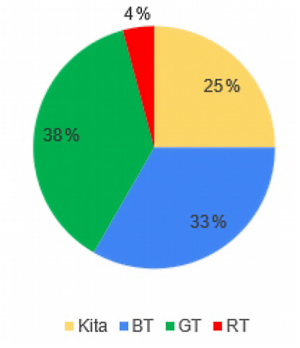
pagrįstas tinkamais techniniais sprendimais atskleidžiant KSP dalyvių profesionalumo reikšmę kibernetinėse pratybose. Turimos ar įgytos kompetencijos ne tik pratybų metu užtikrina efektyvią incidentų analizę ir tinkamų sprendimų įgyvendinimą. Pasiūlytas sprendimų priėmimo karkasas rodo, kad sprendimų priėmimas incidentų sprendimo metu yra holistinis ir kompleksinis procesas. Šiame procese techniniai veiksmai glaudžiai sąveikauja su žmogaus psichologiniais, kognityviniais ir socialiniais aspektais. Holistinis požiūris, integruojantis technologijas ir žmogiškąjį faktorių, leidžia užtikrinti didesnį kibernetinio saugumo pratybų efektyvumą bei organizacijų atsparumą.

5. Eksperimentinis tyrimas

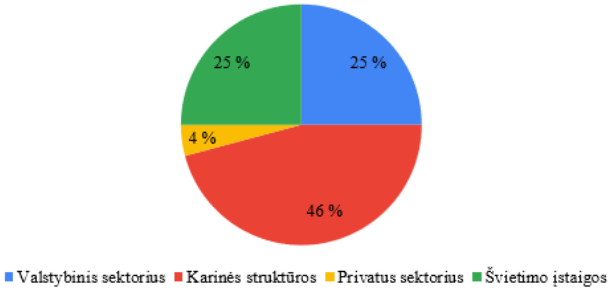
Siūlomam sprendimų priėmimo karkasui validuoti buvo naudojama kibernetinės saugos pratybų „Amber Mist 2024“ atvejo analizė. „Amber Mist“ – tai kasmetinės, tarptautinės kibernetinės saugos pratybos, kurias koordinuoja Lietuvos kariuomenė. 2024 m. pratybose dalyvavo daugiau nei 300 kibernetinės saugos ekspertų iš 12 šalių, taip pat Lietuvos privačiojo ir viešojo sektorių, universitetų ir pirmaujančių IT įmonių saugos specialistai. Po pratybų buvo atliktas kokybinis tyrimas, siekiant suprasti ir nustatyti saugos specialistų profesinius įgūdžius, patirtį, žmogiškuosius faktorius, darančias įtaką jų sprendimų priėmimui pratybų metu. Apklausoje dalyvavo 24 kibernetinio saugumo specialistai iš BT, GT ir RT komandų, t. y. GT sudarė 38 % visų apklausos dalyvių, BT – 33 %, RT – 4 %, o 25 % apklaustųjų priklausė kitoms komandoms (6 pav.). RT komanda vykdė kibernetines atakas, o BT ir GT komandos glaudžiai bendradarbiavo gindamos infrastruktūrą, t. y. GT buvo atsakinga už kompiuterinių sistemų stebėseną bei incidentų registravimą sistemoje, o BT incidentų analizę, sprendimą ir informacijos pateikimą WT. Anketiniai dalyvių duomenys rodo, kad 46 % respondentų atstovavo kariniam sektoriui, vyriausybinis ir švietimo sektoriai sudarė po 25 %, privatus – 4 % (7 pav.).

Analizuojant KSP dalyvių išsilavinimą (8 pav.) nustatyta, kad aukštąjį universitetinį išsilavinimą turinčių dalyvių skaičius yra didžiausias visose komandose, ypač GT komandoje, kur net 89 % dalyvių turėjo aukštąjį universitetinį išsilavinimą. BT komandoje tokių dalyvių buvo 74 %, o kitose grupėse 68 %. Tai rodo aukštą KSP dalyvių akademinį pasirengimą. Pateiktas grafikas leidžia įvertinti dalyvių kompetencijų potencialą pagal išsilavinimą ir padeda analizuoti, ar komandinė sudėtis gali turėti įtakos sprendimų priėmimo kokybei bei rezultatams pratybose.

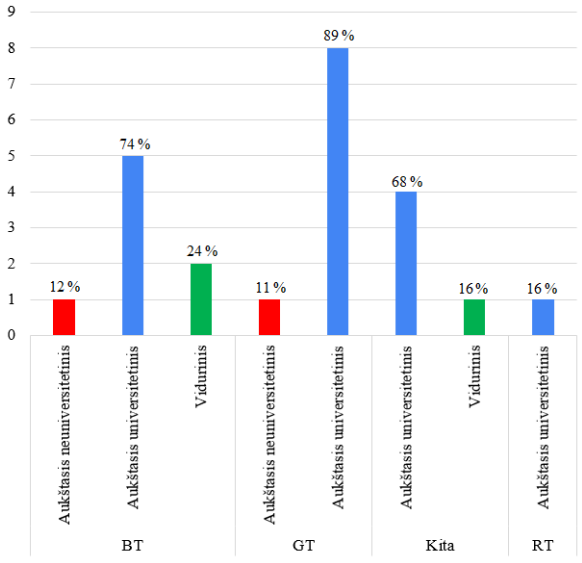
9 paveiksle parodytas KSP dalyvių pasiskirstymas pagal amžių. Matome, kad 48 % dalyvių priklausė 41–50 m. amžiaus grupei, o po 26 % dalyvių priklausė nuo 20–30 ir 31–40 m. amžiui. 10 paveiksle pateikta stulpelinė diagrama, kurioje vaizduojami KSP dalyvių žmogiškieji faktoriai, darantys įtaką sprendimų priėmimui kibernetinės saugos pratybose. Vertikalioje ašyje nurodyti veiksniai, o horizontalioje – vidutiniai įverčiai skalėje nuo 1 iki 5, kur 5 reiškia



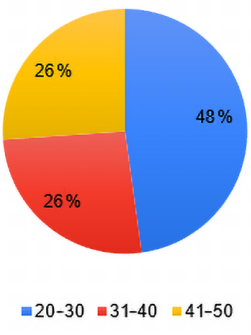
6 paveikslas. KSP procentinis dalyvių komandų pasiskirstymas



7 paveikslas. KSP dalyvių pasiskirstymas sektoriuose



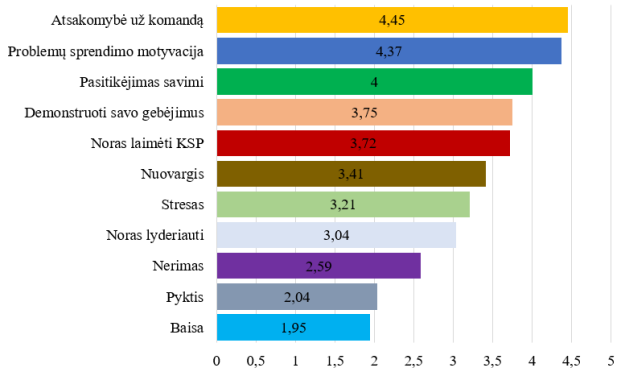
8 paveikslas. KSP dalyvių išsilavinimas



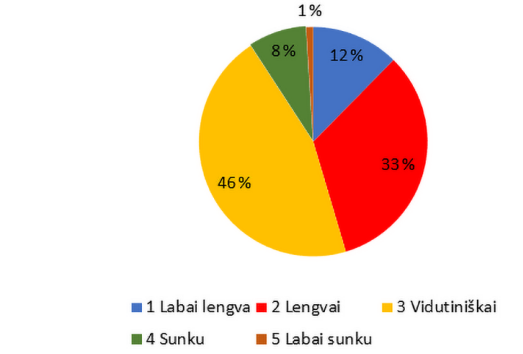
9 paveikslas. KSP dalyvių amžiaus pasiskirstymas

aukščiausią įtakos lygį. Sprendimo priėmimą KSP metu labiausiai veikia atsakomybė už komandą (4,45) ir problemų sprendimo motyvacija (4,37). Tai rodo, kad pagrindiniai dalyvių elgesį motyvuojantys veiksniai buvo susiję su komandine atsakomybe ir vidine motyvacija spręsti sudėtingas situacijas. Šie rezultatai atskleidžia aukštą dalyvių įsitraukimo lygį bei stiprų tapatinimąsi su komandos tikslais, tai itin svarbu KSP kontekste, kur sėkmingas incidentų sprendimas priklauso nuo bendradarbiavimo komandose. Kitas svarbus veiksnys – dalyvių pasitikėjimas savimi (4,0), kuris rodo, kad tai glaudžiai siejasi su gebėjimu priimti sprendimus stresinėse situacijose ir suvaldyti emocinį spaudimą. Noras demonstruoti savo gebėjimus (3,75) ir laimėti (3,72) atskleidžia konkurencinę motyvaciją, kuri skatina produktyvų darbą, tačiau tam tikrais atvejais sukelia stresą. Nuovargis (3,41), stresas (3,21) ir noras lyderiauti (3,04) pateko į vidutinį intervalą. KSP pratybos buvo intensyvios, dalyviai gebėjo išlaikyti emocinį stabilumą. Vidutiniai streso ir nuovargio rodikliai rodo efektyvų psichologinį pasirengimą ir emocijų kontrolę. Žemiausi įverčiai nustatyti nerimui (2,59), pykčiui (2,04) ir baisai (1,95). Tai reiškia, kad neigiamos emocijos turėjo mažiausią įtaką sprendimų priėmimui, o dalyviai gebėjo išlaikyti racionalų mąstymą net esant stresinei aplinkai. Tyrimas atskleidė, kad dominuojantys žmogiškieji faktoriai yra atsakomybė, motyvacija ir pasitikėjimas savimi. Šie aspektai siejami su teigiamais kognityviniais procesais ir sprendimų kokybe KSP metu. Neigiamos emocijos (nerimas, pyktis, baimė) buvo minimalios, o tai patvirtina, kad dalyviai gebėjo išlaikyti savikontrolę ir emocinį atsparumą.

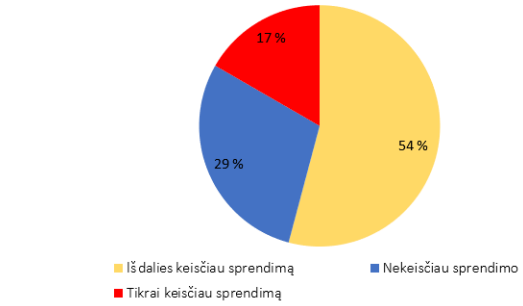
Suvokto sprendimo priėmimo sudėtingumo lygis pateiktas skritulinėje diagramoje 11 paveiksle, joje vaizduojama, kaip KSP dalyviai įvertino sprendimų priėmimo sudėtingumą pratybų metu. Vertinimas atliktas penkiabalėje skalėje, kur 1 reiškia „labai lengva“ priimti sprendimą, o 5 – „labai sunku“. Apibendrinant pateiktus rezultatus matyti, kad 79 % dalyvių sprendimų priėmimą vertino kaip lengvą arba vidutinio sunkumo, tai reiškia gerą pasirengimą ir efektyvią reakciją į incidentų scenarijus. Tik 9 % dalyvių pažymėjo, kad KSP metu sprendimų priėmimas jiems buvo sunkus ir labai sunkus. Tikėtina, kad užduočių kompleksiškumas ir emocinis stresas darė poveikį sprendimų priėmimui. Gauti duomenys leidžia daryti prielaidą, kad pratybų scenarijai buvo tinkamai subalansuoti, o dalyvių kompetencijos lygis atitiko užduočių sudėtingumą.



10 paveikslas. Žmogiškojo faktoriaus įtaka kibernetinės saugos pratybose priimant sprendimus



11 paveikslas. Suvokto sprendimo priėmimo sudėtingumo lygis



12 paveikslas. Sprendimų refleksinis vertinimas

Skritulinėje 12 paveikslo diagramoje pavaizduota, kaip kibernetinių saugumo pratybų dalyviai vertino savo priimtų sprendimų tinkamumą po užduočių atlikimo. Procentinė išraiška rodo, kokia dalis dalyvių keistų savo sprendimus ar jų nekeistų, jei turėtų galimybę. Matome, kad 54 % respondentų nurodė, kad iš dalies keistų sprendimą. Tuo remiantis, galima teigti, kad dalyviai turėjo kritinį, konstruktyvų požiūrį į savo veiksmus, bet iš esmės savo sprendimų nelaikė klaidingais. Kita dalis apklaustųjų, t. y. 29 %, buvo visiškai patenkinti savo sprendimais ir jų pasekmėmis, tai rodo tvirtai argumentuotą sprendimų stabilumą, aukštesnį techninės kompetencijos lygį, didesnę darbo patirtį, greitą sprendimo priėmimą stresinėse situacijose. Mažesnė dalis, t. y. 17 %, norėtų visiškai pakeisti sprendimą. Tai susiję su aukštesniu emociniu krūviu, laiko spaudimu, nepakankama ar ne visiškai suprasta informacija. Pateikti tyrimo rezultatai rodo, kad dalyviai pasižymėjo aukštu refleksijos, komandinio darbo, savianalizės lygiu, tai yra svarbus žmogiškojo faktoriaus rodiklis kibernetinės saugos kontekste, leidžiantis mažinti klaidų tikimybę valdant incidentus.

6. Išvados

Atlikus tyrimą nustatyta, kad žmogiškasis faktorius yra svarbus komponentas sprendimų priėmimo procese kibernetinės saugos pratybose. Tyrimas patvirtino, kad sprendimų

kokybę lemia ne tik techninės kompetencijos, bet ir psichologiniai, kognityviniai bei socialiniai aspektai. Pasiūlytas sprendimų priėmimo karkasas, integruojantis techninius ir žmogiškuosius faktorius, leidžia tiksliau vertinti ir prognozuoti specialistų elgseną kibernetinių incidentų metu ir yra tinkamas incidentų sprendimų analizei. Nustatyta, kad dominuojantys faktoriai, darantys įtaką sprendimų priėmimui, yra atsakomybė už komandą, motyvacija išspręsti problemą ir aukštas pasitikėjimo savimi lygis. Suvokto sprendimų priėmimo sudėtingumas daugumai yra valdomas, t. y. 79 % dalyvių sprendimų priėmimą įvertino kaip lengvą arba vidutinį ir tik 9 % – kaip sunkų ar labai sunkų. Tai rodo užduočių kompleksiškumo ir dalyvių kompetencijų atitiktį. Sprendimų refleksinis vertinimas parodė, kad 54 % dalyvių iš dalies keistų savo sprendimus, 29 % nekeistų, 17 % keistų iš esmės. Tai rodo, kad dauguma dalyvių kritiškai vertina savo sprendimus, o refleksiją mato kaip svarbų mokymosi proceso etapą. Kibernetinės saugos pratybose siekiant didinti sprendimų priėmimo efektyvumą, būtinas aiškus vaidmenų pasiskirstymas komandoje, tarpusavio pasitikėjimu grįsta komunikacija ir bendradarbiavimas. Integruotas techninių ir žmogiškųjų faktorių vertinimas turėtų būti įtrauktas į kibernetinės saugos specialistų rengimo programas. Tai leistų formuoti visapusiškai pasirengusius specialistus, gebančius veikti sudėtingose, stresinėse ir neapibrėžtose situacijose.

Literatūra

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., & Yen, J. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Advances in information security*: *Vol. 46*. *Cyber situational awareness* (pp. 3–13). Springer. https://doi.org/10.1007/978-1-4419-0140-8_1

Colabianchi, S., Costantino, F., Nonino F., & Palombi G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge*, *10*(3), 1–25. https://doi.org/10.1016/j.jik.2025.100695

Dykstra, J., & Lyn Paul, C. (2018). *Cyber Operations Stress Survey* (*COSS*): *Studying fatigue, frustration, and cognitive workload in cybersecurity operations*. National Security Agency (NSA). https://www.nsa.gov/portals/75/documents/news-features/news-stories/2018/measuring-stress-in-a-high-risk-environment/usenix_cybersecurity_ops_stress.pdf

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, *55*(3), 605–618. https://doi.org/10.1177/0018720812464045

European Union Agency for Cybersecurity. (2023). *Threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*, 183–199. https://doi.org/10.1111/risa.12891

Granåsen, M., & Andersson, D. (2015). Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study. *Cognition, Technology & Work*, *18*, 121–143. https://doi.org/10.1007/s10111-015-0350-2

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019). Positioning your organization to respond to insider threats. *IEEE Engineering Management Review*, *47*(2), 75–83. https://doi.org/10.1109/EMR.2019.2914612

Hagen, R. A., Øverlier, L., & Helkala, K. (2025). Human factors in AI-driven cybersecurity: Cognitive biases and trust issues. *Digital Threats*: *Research and Practice*. https://doi.org/10.1145/3759260

Harren, V. A. (1979). A model of career decision making for college students. *Journal of Vocational Behavior*, *14*(2), 119–133. https://doi.org/10.1016/0001-8791(79)90065-4

Yao, A., Huang, C., Zhang, W., Dong, C., Lu, M., Mao, J., Liu, X., & Li, X. (2025). Enhancing cyber defense strategies with discrete multi-dimensional Z-numbers: A multi-attribute decision-making approach. *Complex & Intelligent Systems*, *11*, Article 216. https://doi.org/10.1007/s40747-025-01786-z

IBM Trust Center. (2022). *Annual report*. https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2022.pdf

International Organization for Standardization. (2023). *Information technology — Information security incident management*. *Part 1*: *Principles and process* (ISO/IEC Standard No. 27035-1:2023). https://www.iso.org/standard/78973.html

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*, Article 119. https://doi.org/10.1007/s10207-025-01032-0

Kott, A., Wang, C., & Erbacher, R. F. (Eds.). (2014). *Cyber defense and situational awareness*. Springer International Publishing. https://doi.org.10.1007/978-3-319-11391-3

Langlois, P., Pinto, A., Hylender, D., & Widup, S. (2023). *2023 Data Breach Investigations Report: 10K 20K 30K*. https://doi.org/10.13140/RG.2.2.32362.70085

Lietuvos Respublikos krašto apsaugos ministerija. (2023). *Lietuvos kibernetinio saugumo būklės apžvalga*: *svarbiausia informacija 2023 m*. https://kam.lt/wp-content/uploads/2024/06/KS-ataskaitos-2023-Santrauka-LT_final.pdf

Lietuvos Respublikos krašto apsaugos ministerija. (2024). *Nacionalinė kibernetinio saugumo būklės ataskaita*. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2024.pdf

Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., Maennel, O., Majore, G., & Sütterlin, S. (2023). A multidimensional cyber defense exercise: Emphasis on emotional, social, and cognitive aspects. *Sage Open*, *13*(1). https://doi.org/10.1177/21582440231156367

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement*, *55*(5), 818–831. https://doi.org/10.1177/0013164495055005017

Valstybinė duomenų apsaugos inspekcija. (2023). *2023 m. veiklos ataskaita*. https://vdai.lrv.lt/lt/administracine-informacija/veiklos-ataskaitos/

Valstybinė duomenų apsaugos inspekcija. (2024). *Pranešimų apie asmens duomenų saugumo pažeidimus* (*ADSP*) *apžvalga 2024 m*. https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2024-m/

Valstybinė duomenų apsaugos inspekcija. (2025). *Pranešimų apie asmens duomenų saugumo pažeidimus* (*ADSP*) *apžvalga 2025 m*. https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-saugumo-pazeidimai-lietuvoje-2025-m-i-pusm-PJS/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

THE INFLUENCE OF THE HUMAN FACTOR IN DECISION-MAKING IN CYBER SECURITY EXERCISES

K. Kulikauskaitė

Abstract

Cybersecurity is an interdisciplinary field that encompasses aspects of information technology, forensics, incident management, and the human factor. In cyber security, decision-making is influenced by the specialist's technical knowledge, competencies, and professional experience. However, decisions made in extreme and complex situations are influenced by emotions, motivation, social skills, and cognitive abilities. Therefore, this paper investigated the human factor influencing decision-making of participants in cyber security exercises, and proposed a multidimensional decision-making framework. A study conducted by analyzing the data of the cyber security exercise "Amber Mist" showed that an integrated assessment of technical competencies and the human factor allows for a more accurate determination of the decision-making of a cyber security specialist and its prediction. It was determined that when analyzing decision-making in cyber security exercises, it is necessary to take the human factor into account. The results of the study can be used to improve methodologies and programs for training cyber security specialists.

Keywords: cybersecurity exercises, human factor, decision making.