PATVIRTINTA
NKSC prie KAM direktoriaus
2019 m. gruodžio d.
įsakymu Nr.

PRATYBŲ „KIBERNETINIS SKYDAS 2019“ ATASKAITA VISUOMENEI

TLP: WHITE

Turinys

1. SANTRAUKA

A. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu, 2019 m. spalio 22-24 dienomis surengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2019“ (toliau – KS2019). Nacionalinių kibernetinių saugumo pratybų rengimas yra numatytas Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Lietuvos Respublikos (toliau – LR) Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818.

B. Pratybose buvo kviečiami dalyvauti valstybės informacinių išteklių valdytojai ir tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai, taip pat kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija) bei pavojingo kibernetinio incidento valdymą koordinuojančios institucijos (LR Vyriausybės kanceliarija, LR Seimo kanceliarija, LR Prezidento kanceliarija, LR valstybės saugumo departamentas, LR Krašto apsaugos ministerija). Be to, į dalyvauti pratybose buvo kviesti ir naujienų portalai.

C. Pratybomis buvo siekiama formuoti praktinius pratybų dalyvių kibernetinio saugumo įgūdžius, patikrinti kibernetinių incidentų valdymo procedūras, gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių ir (ar) tiriančių institucijų ir kibernetinio saugumo subjektų.

D. Atsižvelgiant į platų dalyvaujančių organizacijų spektrą, skirtingą kibernetinio saugumo brandos lygį, kiekviena organizacija galėjo pasirinkti įsitraukimo į pratybas laipsnį ir tipinį, KS2019 organizatorių paruoštą, pratybų scenarijų prisitaikyti savo poreikiams.

E. Iš viso pratybose KS2019 dalyvavo daugiau nei 830 žmonių iš 101 organizacijos. Tai buvo didžiausios iki šiol Lietuvoje surengtos nacionalinės kibernetinio saugumo pratybos. Nepaisant rekordinio dalyvių skaičiaus, Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane, patvirtintame LRV 2019 m. liepos 3 d. nutarimu Nr. 709, nustatytas kriterijus (Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų skaičius - 168) nebuvo pasiektas.

F. 90% vietinių instruktorių apklausos respondentų pritarė teiginiui, kad pratybos KS2019 jų organizacijai buvo naudingos.

2. NUORODOS

A. Lietuvos Respublikos Kibernetinio saugumo įstatymas (2014 m. gruodžio 11 d. Nr. XII-1428);

B. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos Kibernetinio saugumo įstatymo įgyvendinimo“;

C. Lietuvos Respublikos Vyriausybės 2017 m. kovo 13 d. nutarimas Nr. 167 „Dėl Lietuvos Respublikos Vyriausybės programos įgyvendinimo plano patvirtinimo“;

D. Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimas Nr. 709 „Dėl nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio plano patvirtinimo.

3. ĮVADAS

A. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu, 2019 m. spalio 22-24 dienomis surengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2019“ (toliau – KS2019). Nacionalinių kibernetinių saugumo pratybų rengimas yra numatytas Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Lietuvos Respublikos (toliau – LR) Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818.

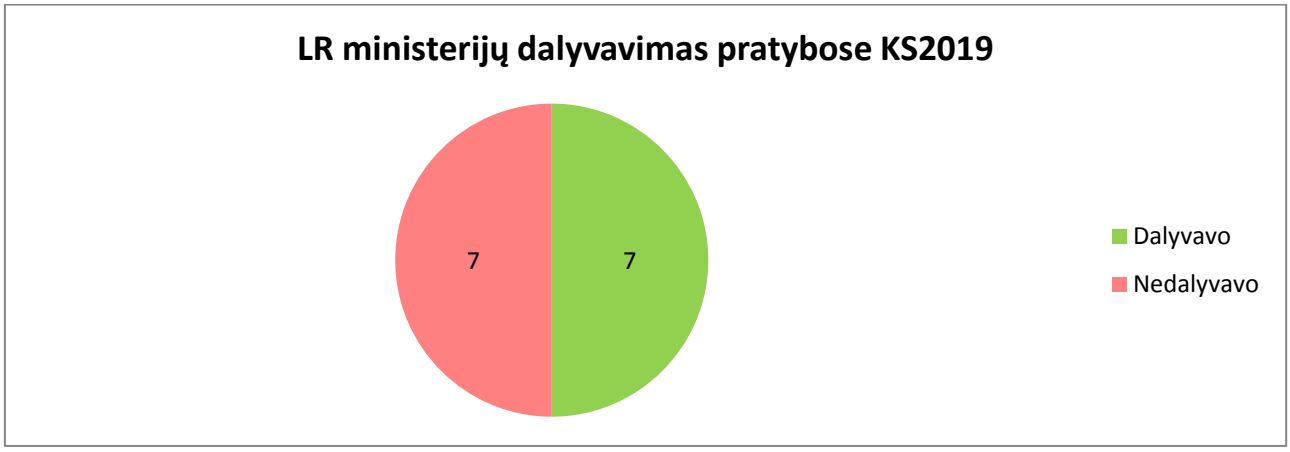
B. Šia ataskaita siekiama visuomenei, pratybų dalyviams ir vadovybei pristatyti pratybų koncepciją, eigą, pasiektus rezultatus ir iš dalyvių gautą grįžtamąjį ryšį. Taip pat ataskaitoje pateikti statistiniai duomenys bus aktualūs ateityje vertinant praktinių informacinės infrastruktūros valdytojų kibernetinio saugumo įgūdžių formavimo progresą.

4. PRATYBŲ DALYVIAI

A. Pratybose KS2019 buvo kviečiami dalyvauti kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai (toliau bendrai – kibernetinio saugumo subjektai, sutrumpintai - KSS), taip pat kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (toliau KIVT institucijos) bei pavojingo kibernetinio incidento valdymą koordinuojančios institucijos (toliau – KIVK institucijos). Atsižvelgiant į 2018 m. pasirašytą bendradarbiavimo susitarimą tarp Krašto apsaugos ministerijos, Nacionalinio kibernetinio saugumo centro ir interneto portalų, pirmą kartą į šias pratybas buvo pakviesti ir naujienų portalų atstovai. Toliau visi pratybų dalyviai bendrai vadinami Pratybų auditorija.

B. Iš viso pratybose KS2019 dalyvavo daugiau nei 830 žmonių iš 101 organizacijos. Tai buvo didžiausios iki šiol Lietuvoje surengtos nacionalinės kibernetinio saugumo pratybos. Nepaisant rekordinio dalyvių skaičiaus, Nacionalinės kibernetinio saugumo

strategijos įgyvendinimo tarpinstituciniame veiklos plane, patvirtintame LRV 2019 m. liepos 3 d. nutarimu Nr. 709, nustatytas kriterijus (Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų skaičius - 168) nebuvo pasiektas. Pavyzdžiui, dalyvavo tik pusė LR ministerijų, o joms pavaldžių įstaigų dalyvavimas nesiekia 50%. Siekiant nustatyto kriterijaus ateityje, būtina rasti būdus kaip KSS paskatinti dalyvauti nacionalinėse kibernetinio saugumo pratybose.



5. PRATYBŲ TIKSLAS IR SIEKINIAI

A. Pratybų tikslas (angl. *Training Objective*)

Formuoti praktinius pratybų dalyvių kibernetinio saugumo įgūdžius, patikrinti procedūras, gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių ir (ar) tiriančių institucijų ir kibernetinio saugumo subjektų.

B. Pratybų siekiniai (angl. *Exercise Objectives*)

(1) Patikrinti ir treniruoti KIVT institucijų ir KSS gebėjimus vykdyti Kibernetinių incidentų valdymo plane (toliau – NKIVP) nustatytus veiksmus; identifikuoti tobulintinas NKIVP sritis.

(2) Patikrinti KIVT ir KSS vidines organizacijos kibernetinio incidento valdymo procedūras.

(3) Treniruoti KSS aptikti ir tirti kibernetinius incidentus.

(4) Treniruoti KSS naudotis KSIT priemonėmis.

6. PRATYBŲ KONCEPCIJA

A. Organizuojant pratybas KS2019 pirmą kartą remtasi NATO kibernetinės gynybos pratybų „Kibernetinė koalicija“ (angl. *Cyber Coalition*) modeliu. Vienas pagrindinių jų principų – kuo didesnis realistiškumas (angl. *train as you fight*). Siekėme, kad pratybos vyktų aplinkoje, kuri yra kuo artimesnė kasdieninei Pratybų auditorijos aplinkai. Tai reiškia, kad organizacija turėjo dalyvauti su tokiais pajėgumais, personalu, procedūromis, kuriuos realiai turi. Nebuvo formuojami laikini personalo dariniai, skirti

specialiai pratyboms, kurie kasdien neegzistuoja, nebuvo perkama specialiai pratyboms skirta įranga. Pratybos vyko organizacijų patalpose, personalas dalyvavo iš savo darbo vietų, incidentus valdė, tyrė savo turimais įrankiais, pagal savo kasdienines procedūras.

B. Vietiniai instruktoriai savo nuožiūra parinko savo organizacijos įsitraukimo laipsnį, kuriuos pratybų organizatorių paruoštus kibernetinius incidentus jų organizacija turėjo tirti ir valdyti pratybų metu. Atsižvelgiant į šį pasirinkimą, organizacijos struktūrą ir procedūras vietinis instruktorius turėjo pritaikyti tipinį pratybų scenarijų savo organizacijai.

C. Skirtingai nuo anksčiau organizuotų pratybų „Kibernetinis skydas“ šiemet nebuvo sukurta „gyva“ informacinių technologijų (toliau – IT) infrastruktūra prie kuriuos Pratybų auditorija jungtųsi, saugotų, gintų ir t.t.. Kibernetiniai incidentai buvo įvykdyti KTU pratyboms paruoštoje infrastruktūroje, o dalyviams pateikti artefaktai (tarnybinių (Linux) arba darbo stočių (Windows) diskų atvaizdai (angl. *image*), žurnalai (angl. *log*), perimtų tinklo paketų kopija (angl. *pcap*)), tinklo srauto įrašai (angl. *Netflow*)). Informaciją apie įvykius ir incidentus pratybų erdvėje vietinis instruktorius pratybų auditorijai pateikdavo el. paštu. Dalyviai darė prielaidą, kad kibernetiniai incidentai įvyko jų organizacijos IT infrastruktūroje.

7. PRATYBŲ RENGINIAI

A. Pakvietimą dalyvauti pratybose ir į jų planavimą paskirti savo organizacijos atstovą (vietinį instruktorių) NKSC išsiuntė 334 KSS. Į šį pakvietimą atsiliepė ir pagrindinėje pratybų planavimo konferencijoje, surengtoje 2019 m. birželio 5 dieną Vilniuje, dalyvavo 154 KSS deleguoti vietiniai instruktoriai.

B. Rugsėjo mėnesį Kaune ir Vilniuje mažoms vietinių instruktorių grupėms (iki 20 žmonių) buvo surengtos vienuolika vienos dienos trukmės scenarijaus rašymo konferencijų. Jų metu buvo pristatytas tipinis pratybų scenarijus ir kibernetiniai incidentai, paaiškinta vietinio instruktoriaus atsakomybė, ruošiantis pratyboms reikalingi atlikti darbai. Vietiniai instruktoriai pradėjo tipinio pratybų scenarijaus pritaikymą savo organizacijai. Scenarijaus rašymo konferencijose dalyvavo vietiniai instruktoriai iš 120 organizacijų.

C. Pačiose pratybose spalio 22-24 dienomis iš viso dalyvavo 101 organizacija. Apklausos, kurią užpildė 90 vietinių instruktorių iš 101, duomenimis iš viso pratybose KS2019 dalyvavo 833 dalyviai (įskaitant ne tik specialistus, bet ir aukščiausio bei vidutinio lygmens vadovus).

8. PRATYBŲ SCENARIJUS

A. Pratyboms paruoštas scenarijus susidėjo iš 6 dalių, vadinamųjų scenarijaus linijų (angl. *story line*, toliau SL). Vietiniai instruktoriai turėjo pasirinkti, kuriuose scenarijaus linijose jų organizacija dalyvauja, pritaikyti jas savo poreikiams ir koordinuoti pratybų eigą savo organizacijos viduje. Pratyboms buvo paruoštos tokios SL:

(1) Kenksmingos programinio kodo įrangos patalpinimas organizacijos internetinėje svetainėje.

(2) Organizacijos darbo stoties užvaldymas.

(3) Organizacijos failų serverio užkrėtimas ir failų su jautria informacija eksfiltravimas.

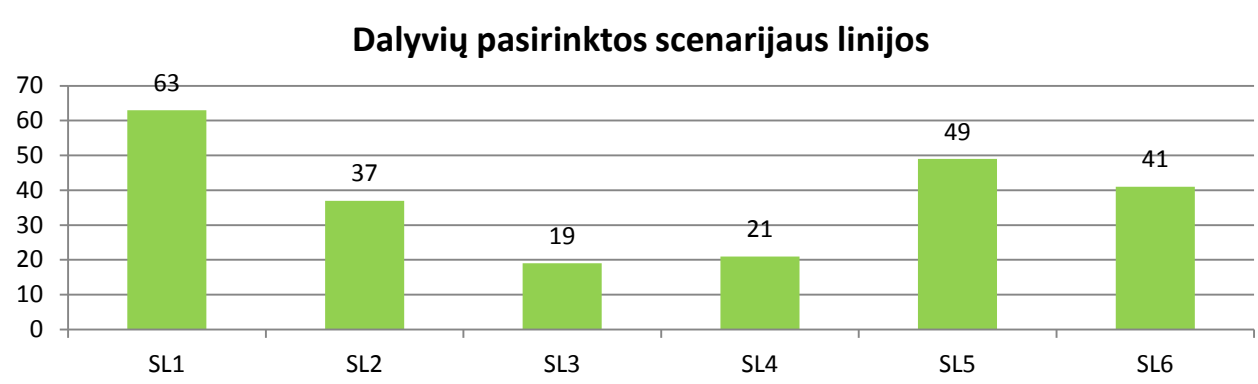
(4) Kripto valiutos kasimo skripto patalpinimas į organizacijos internetinę svetainę.

(5) Suklastotas vadovo el. laiškas finansistui (-ei) reikalaujantis atlikti skubų pavedimą.

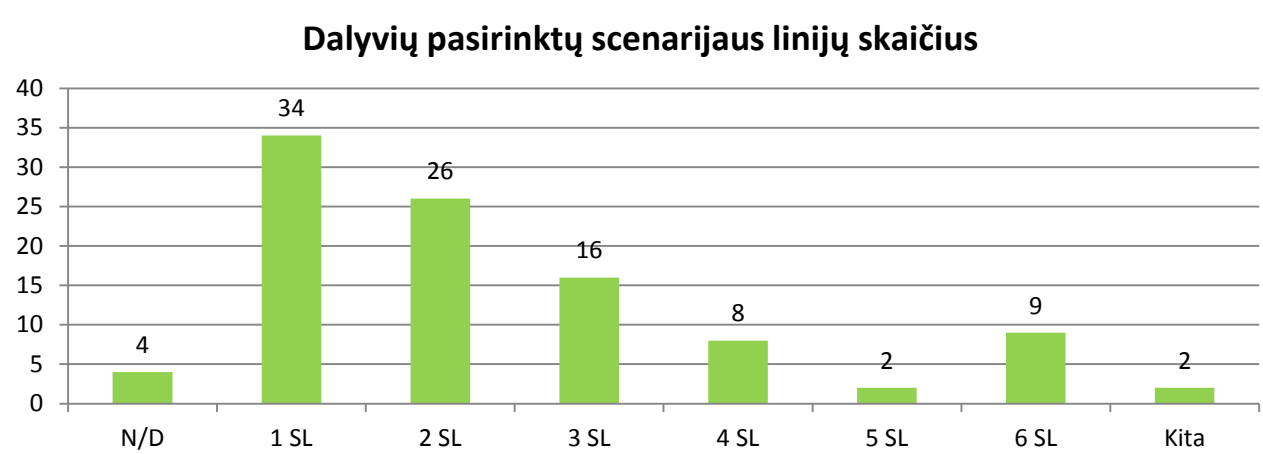
(6) Šantažuojantis laiškas vadovui su reikalavimu mokėti išpirką, jeigu norima išvengti jautrių duomenų paskelbimo ir darbo stoties disko užšifravimas.

B. Visoms SL buvo paruošti el. laiškų pavyzdžiai, kuriais remiantis vietiniai instruktoriai galėjo inicijuoti kibernetinių incidentų valdymą ir tyrimą savo organizacijose.

C. 1-4 SL buvo paruošta ir techniniai artefaktai, kuriuos KSS personalas turėjo ištirti ir remiantis vidinėmis organizacijos procedūromis pateikti tyrimo rezultatus savo organizacijos saugos personalui.



Paaiškinimas: SL1 pasirinko dalyvauti 63 organizacijos, SL2 pasirinko dalyvauti 37 organizacijos ir t.t.



Paaiškinimas:
N/D - 4 organizacijos nenurodė keliose SL dalyvavo;
1 SL, 2 SL, ir t.t. - 34 organizacijos dalyvavo vienoje SL, 26 organizacijos dalyvavo dvejose SL ir t.t.;
Kita - 2 organizacijos modifikavo/apjungė pasiūlytas SL, pridėjo savo sukurtas SL.

9. GEOSTRATEGINĖ SITUACIJA

Geostrateginės situacijos aprašymas buvo patvirtintas kartu su specifikacija, bet atsižvelgiant į visiškai naują pratybų modelį ir siekiant suvaldyti pratybas, politinių vertinimų reikalaujančio žaidimo pratybose KS2019 nuspręsta neplėtoti. Ateityje norint plėtoti pratybų žaidimą, susijusį ne tik su techniniu, bet ir geostrateginiu scenarijumi**,** pratybose ir jų planavime turi dalyvauti atitinkamas kompetencijas turintis personalas.

10. PRIEDAS

APIBENDRINTI VIETINIŲ INSTRUKTORIŲ APKLAUSOS REZULTATAI

Pratybų „Kibernetinis skydas 2019“ ataskaitos
1 priedas

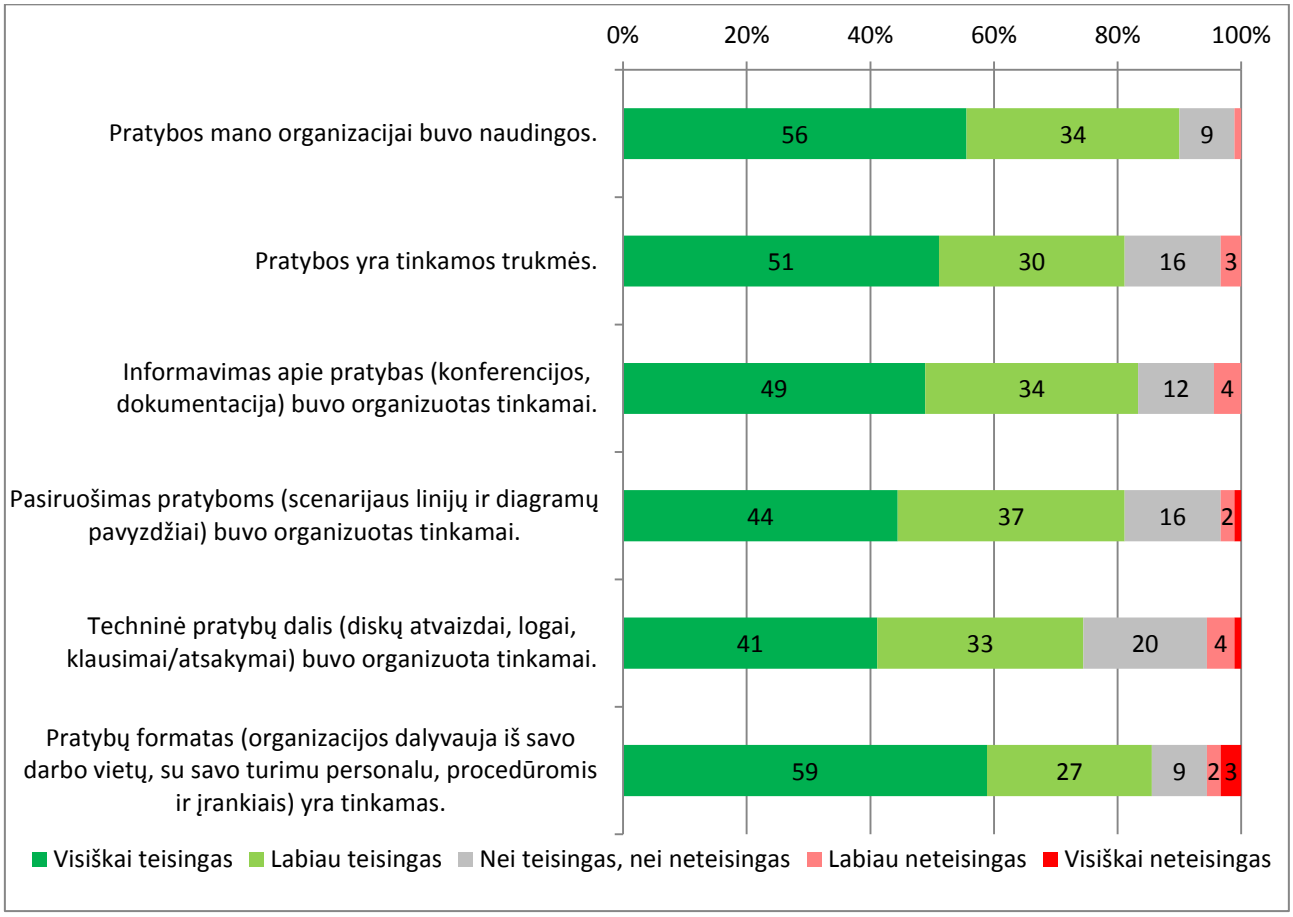
APIBENDRINTI VIETINIŲ INSTRUKTORIŲ APKLAUSOS REZULTATAI

1. ĮVADAS

Pasibaigus pratyboms visi dalyvavusių organizacijų vietiniai instruktoriai buvo paprašyti užpildyti apklausą. Atsakymus pateikė 90 vietinių instruktorių iš 101. Apklausa buvo siekiama sužinoti kaip vietiniai instruktoriai vertina pasiruošimą pratyboms, pratybų vykdymą ir kibernetinio saugumo būklę savo organizacijoje.

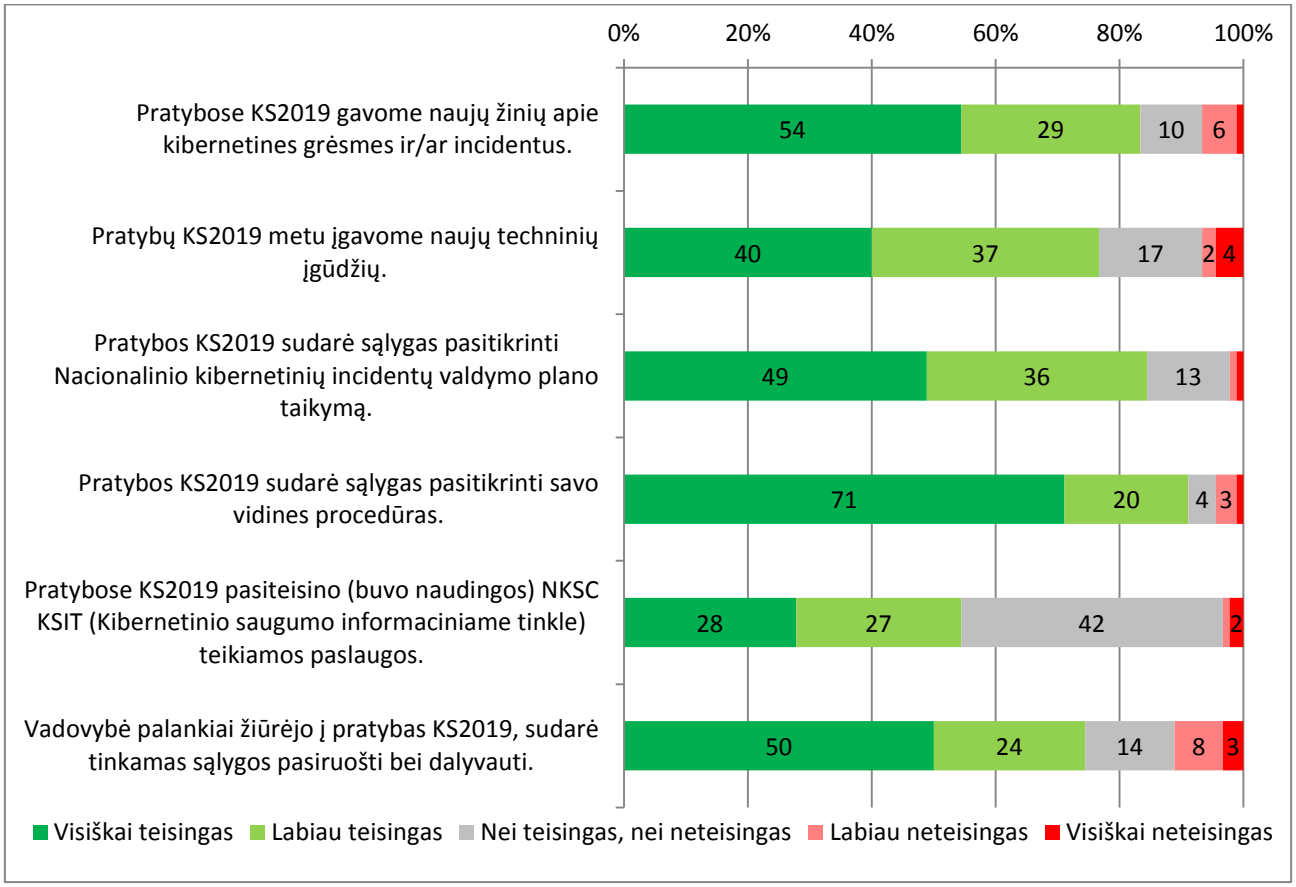
2. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE PRATYBŲ ORGANIZAVIMĄ REZULTATAI

A. Vietinių instruktorių buvo klausiama, kiek, jų nuomone, yra teisingi teiginiai.

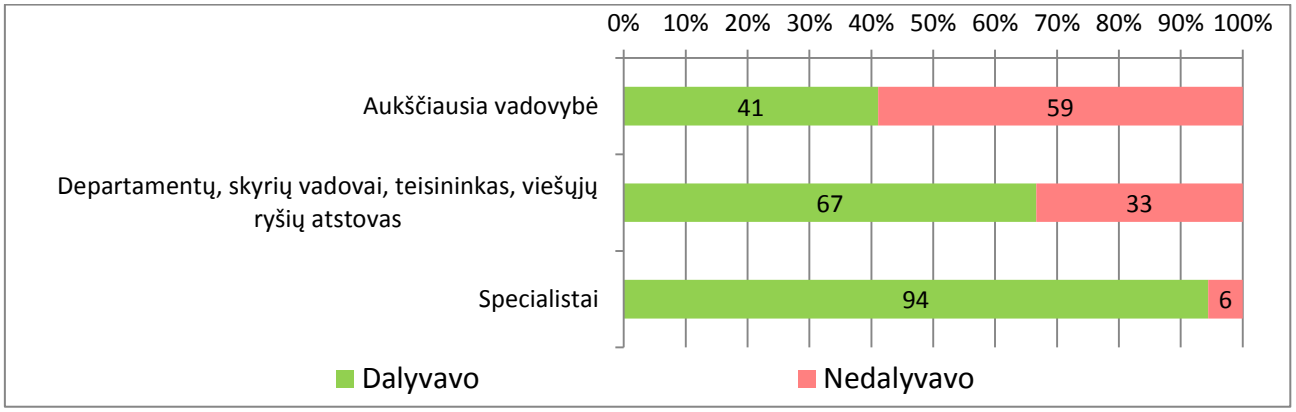


3. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE DALYVAVIMĄ PRATYBOSE REZULTATAI

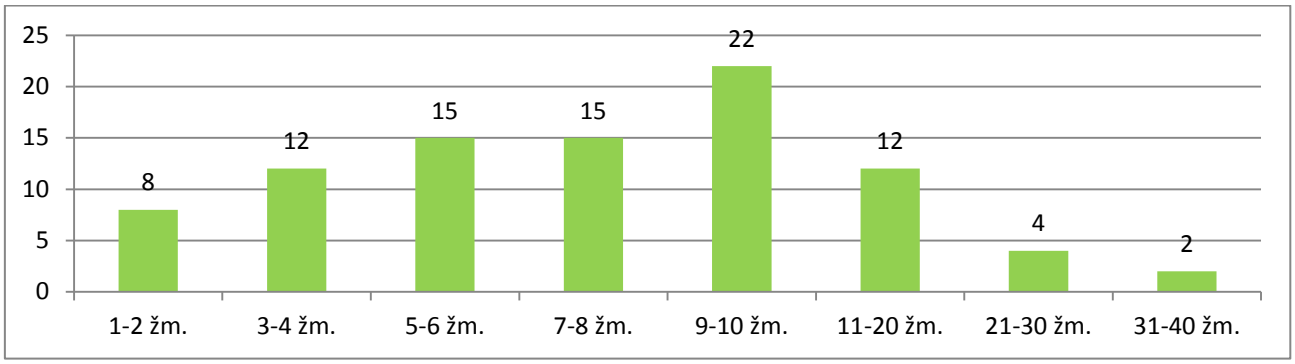
A. Vietinių instruktorių buvo klausiama, kiek, jų nuomone, yra teisingi teiginiai.



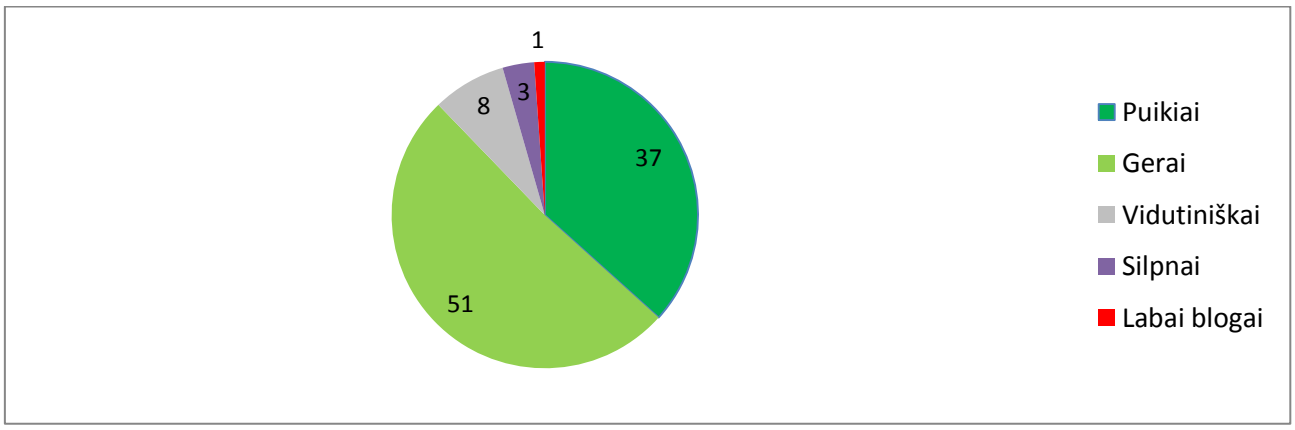
B. Kurie Jūsų organizacijos lygmenys įsitraukė į pratybas KS2019?



C. Kiek Jūsų organizacijos personalo (neskaitant vietinio instruktoriaus) dalyvavo pratybose?



D. Koks yra Jūsų bendras pratybų Kibernetinis skydas 2019 vertinimas?



4. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE KIBERNETINIO SAUGUMO BŪKLĘ ORGANIZACIJOJE REZULTATAI

A. Vietinių instruktorių buvo klausiama, kiek, jų nuomone, yra teisingi teiginiai.