PATVIRTINTA
NKSC prie KAM direktoriaus
2020 m. lapkričio 30 d.
įsakymu Nr. 1-54

NACIONALINIŲ KIBERNETINIO SAUGUMO PRATYBŲ „KIBERNETINIS SKYDAS 2020“ ATASKAITA VISUOMENEI

KIBERNETINIS SKYDAS 2020

TLP: WHITE

Turinys

1. SANTRAUKA

A. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu (toliau – KTU), 2020 m. spalio 20-22 dienomis surengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2020“ (toliau – KS2020). 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. 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.

C. Pratybose iš viso dalyvavo 73 organizacijos, iš jų - 64 valstybinių informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai. Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijos ir joms pavaldžios įstaigos). Taip pat pratybose dalyvavo asmens sveikatos priežiūros įstaigos, energetikos bendrovės, vandens tiekėjai, savivaldybės, bankai, universitetai, mobilaus ryšio operatoriai ir kt. organizacijos.

D. Populiariausios, dažniausiai dalyvaujančių organizacijų pasirinktos pratybų siužeto linijos buvo slaptažodžių parinkimo metodu atliktas įsilaužimas į interneto svetainę bei įsilaužimas į organizacijos tinklą per užvaldytą nuotolinę darbo vietą.

E. 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 - 184) nebuvo pasiektas.

F. 91% vietinių instruktorių apklausos respondentų pritarė teiginiui, kad pratybos KS2020 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, 2020 m. spalio 20-22 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2020“ (toliau – KS2020). 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.

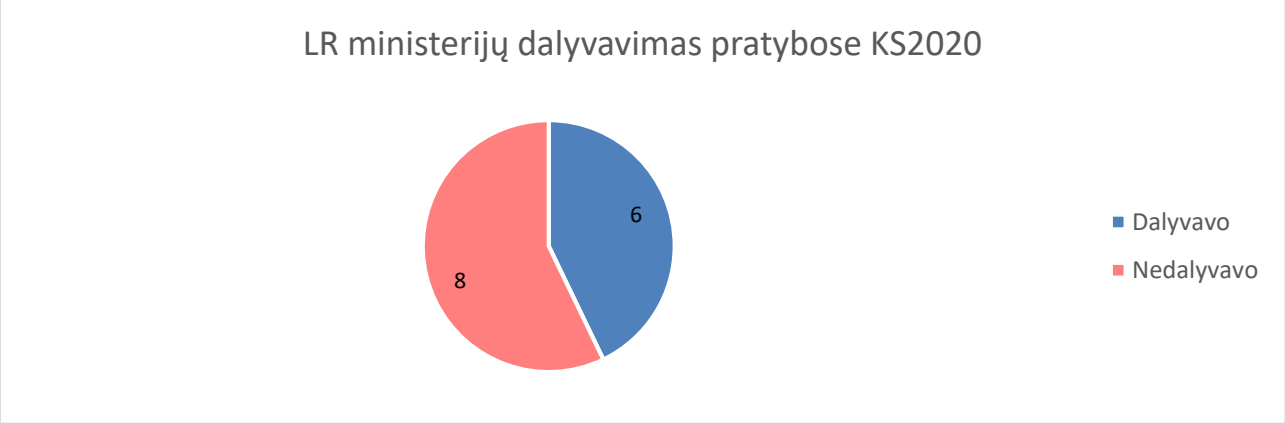
4. PRATYBŲ DALYVIAI

A. Pratybose KS2020 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). Papildomai, NKSC dalyvauti pratybose kvietė mažesniąsias sveikatos priežiūros įstaigas, vandens tiekėjus ir kitas organizacijas. Toliau visi pratybų dalyviai bendrai vadinami Pratybų auditorija.

B. Iš viso pratybose KS2020 dalyvavo daugiau nei 760 žmonių iš 73 organizacijų. 64 dalyvavusios organizacijos yra valstybinių informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai. Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijos ir joms pavaldžios įstaigos). Taip pat pratybose dalyvavo asmens sveikatos priežiūros įstaigos,

energetikos bendrovės, vandens tiekėjai, savivaldybės, bankai, universitetai, mobilaus ryšio operatoriai ir kt. organizacijos.

C. Šiemet kaip ir praėjusiais metais, 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 - 184) nebuvo pasiektas. Pavyzdžiui, iš keturiolikos LR ministerijų dalyvavo tik šešios, o joms pavaldžių įstaigų dalyvavimas dar pasyvesnis. Siekiant nustatyto kriterijaus ateityje, būtina rasti būdus kaip paskatinti KSS dalyvavimą.



5. PRATYBŲ TIKSLAS IR SIEKINIAI

A. Pratybų tikslas

Pratybų dalyvių praktinių kibernetinio saugumo įgūdžių gerinimas.

B. Pratybų siekiniai

(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 institucijų ir KSS vidines kibernetinio incidento valdymo procedūras.

(3) Treniruoti Pratybų Auditoriją aptikti ir analizuoti kibernetinius incidentus.

(4) Treniruoti Pratybų Auditoriją dalintis kibernetinių incidentų informacija, gerinti bendradarbiavimą, naudotis Kibernetinio saugumo informacinio tinklo paslaugomis.

6. PRATYBŲ KONCEPCIJA

A. Organizuojant pratybas KS2020 remtasi NATO kibernetinės gynybos pratybų „Kibernetinė koalicija“ (angl. *Cyber Coalition*) modeliu. Vienas pagrindinių jų principų

– kuo didesnis realistiškumas (angl. *train as you fight*). Buvo siekiama, kad pratybos vyktų aplinkoje, kuri yra kuo artimesnė kasdieninei Pratybų auditorijos aplinkai. Kitaip sakant, 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. Kibernetiniai incidentai buvo įvykdyti KTU pratyboms paruoštoje infrastruktūroje, o dalyviams pateikti artefaktai (tarnybinių (Linux/Windows) arba darbo stočių (Windows) diskų atvaizdai (angl. *image*), žurnalai (angl. *log*), perimtų tinklo paketų kopijos (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 IR DALYVIAI

A. Pakvietimą dalyvauti pratybose ir į jų planavimą paskirti savo organizacijos atstovą (vietinį instruktorių) NKSC išsiuntė 473 organizacijoms (iš jų 323 – KSS).

B. Pagrindinė pratybų planavimo konferencija internetu surengta 2020 m. balandžio 8 dieną. Birželio 18 d. ir rugsėjo 3 d. internetu surengtos papildomos konferencijos, kuriomis buvo siekiama dar neapsisprendusias organizacijas paskatinti dalyvauti pratybose KS2020.

C. Iš viso į NKSC kvietimą atsiliepė ir atstovą pratybų planavimui nurodė 152 organizacijos.

D. Rugsėjo mėnesį Vilniuje ir internetu vietiniams instruktoriams buvo surengtos scenarijaus rašymo konferencijos. Jų metu buvo pristatytas tipinis pratybų scenarijus ir kibernetiniai incidentai, paaiškinta vietinio instruktoriaus atsakomybė, pasiruošimo pratyboms metu reikalingi atlikti darbai. Vietiniai instruktoriai pradėjo tipinio pratybų scenarijaus pritaikymą savo organizacijai. Scenarijaus rašymo konferencijose dalyvavo vietiniai instruktoriai iš maždaug 80 organizacijų.

E. Šiemet pirmą kartą rengti mokymai kibernetinio saugumo specialistams, dalyvaujantiems pratybose. Rugsėjo mėn. organizuoti parengiamieji pratybų KS2020 mokymai, kuriuose buvo pademonstruotas pratybų „Kibernetinis skydas 2019“ kibernetinių incidentų tyrimas. Šiuo renginiu buvo siekiama suteikti dalyviams aiškumo, ką ir kaip reikės atlikti per pratybas. 2020 m. lapkričio 11 d. organizuotuose mokymuose pademonstruota, kokiu būdu buvo galima ištirti pratyboms KS2020 parengtus kibernetinius incidentus.

F. Pratybose spalio 20-20 dienomis iš viso dalyvavo 73 organizacijos. Apklausos, kurią užpildė 55 vietiniai instruktoriai, duomenimis vidutiniškai pratybose iš organizacijos dalyvavo 14 darbuotojų (mediana – 6 darbuotojai), įskaitant ne tik kibernetinio saugumo

specialistus, IT administratorius, bet ir viešųjų ryšių specialistus, teisininkus, aukščiausio bei vidutinio lygmens vadovus.

G. Dauguma organizacijų, kurios ketinimą dalyvauti pratybose buvo išreiškę, bet vėliau dalyvauti pasirengime nustodavo, dėl tokio sprendimo pratybų organizatorių neinformuodavo. Tos organizacijos, kurios apie nedalyvavimą informuodavo, dažniausiai tokio sprendimo priežastimis nurodydavo Covid-19 pandemijos sukeltas kliūtis (dažniausiai – sveikatos priežiūros įstaigos), rinkimų į LR Seimą organizavimą (dažniausiai – savivaldybės, kuriose pratybų savaitę vyko išankstinis balsavimas), personalo trūkumą.

8. PRATYBŲ SCENARIJUS

A. Pratyboms paruoštas scenarijus susidėjo iš 4 dalių, vadinamųjų siužeto linijų (toliau - SL). Vietiniai instruktoriai turėjo pasirinkti, kurios SL jų organizacijai yra aktualiausios ir kuriose iš jų organizacija dalyvaus, pritaikyti jas savo organizacijos poreikiams ir koordinuoti pratybų eigą savo organizacijos viduje. Pratyboms buvo paruoštos tokios SL:

(1) Įsilaužimas į svetainę panaudojant slaptažodžių parinkimo metodą (angl. *brute-force*), failo su kenkėjiška programine įranga patalpinimas ir darbo stoties užvaldymas.

(2) Įsilaužimas į svetainę panaudojant SQL užklausos metodą (angl. *SQL injection*), failo su kenkėjiška programine įranga išplatinimas, darbo stoties užšifravimas.

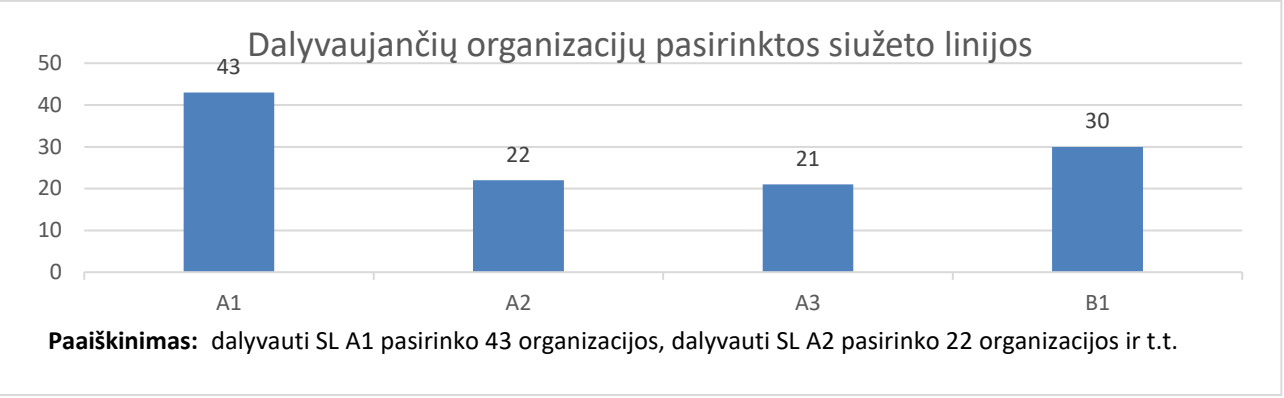
(3) Įskiepio pažeidžiamumo organizacijos turinio valdymo sistemoje išnaudojimas, duomenų bazės su asmens duomenimis eksfiltravimas, failo su kenkėjiška programine įranga išplatinimas, nuotolinės administratoriaus darbo vietos užvaldymas, įsilaužimas į įmonės vidinį tinklą, įmonės darbuotojų asmens duomenų eksfiltravimas į išorę.

(4) Nuotolinės administratoriaus darbo stoties užvaldymas panaudojant socialinę inžineriją, įsilaužimas į įmonės vidinį tinklą, įmonės darbuotojų asmens duomenų eksfiltravimas į išorę, kenkėjiškos programinės įrangos išplatinimas.

B. Populiariausios, dažniausiai dalyvaujančių organizacijų pasirinktos pratybų siužeto linijos buvo slaptažodžių parinkimo metodu atliktas įsilaužimas į interneto svetainę (1) bei įsilaužimas į organizacijos tinklą per užvaldytą nuotolinę darbo vietą (4).

C. Visoms SL buvo paruošti techniniai artefaktai, kuriuos dalyviai galėjo ištirti ir remiantis vidinėmis organizacijos procedūromis pateikti tyrimo rezultatus savo organizacijos saugos personalui, kuris savo ruožtu turėjo informuoti NKSC, Valstybinę duomenų apsaugos inspekciją, Policiją.

D. Visoms SL taip pat buvo pateikti el. laiškų pavyzdžiai, kuriais remiantis vietiniai instruktoriai galėjo inicijuoti kibernetinių incidentų valdymą ir tyrimą savo organizacijose.



Paaiškinimas: dalyvauti SL A1 pasirinko 43 organizacijos, dalyvauti SL A2 pasirinko 22 organizacijos ir t.t.

Paaiškinimas: 36 organizacijos dalyvavo vienoje SL, 15 organizacijų dalyvavo dvejose SL ir t.t.;
Kita - 4 organizacijos modifikavo/apjungė pasiūlytas SL, pridėjo savo sukurtas SL.

9. GEOSTRATEGINĖ SITUACIJA

Geostrateginės situacijos aprašymas buvo patvirtintas kartu su specifikacija, bet politinių vertinimų reikalaujančio žaidimo pratybose KS2020 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

A. APIBENDRINTI VIETINIŲ INSTRUKTORIŲ APKLAUSOS REZULTATAI

Pratybų „Kibernetinis skydas 2020“ ataskaitos priedas

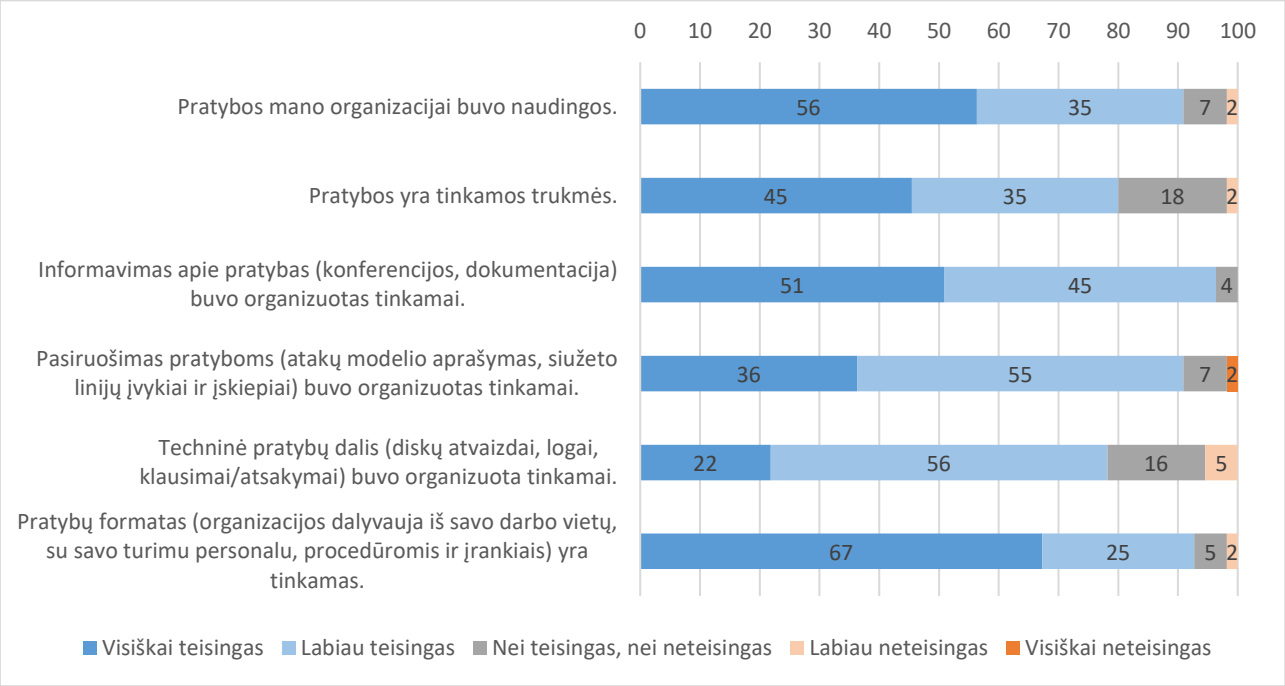
APIBENDRINTI VIETINIŲ INSTRUKTORIŲ APKLAUSOS REZULTATAI

1. ĮVADAS

Pasibaigus pratyboms visi dalyvavusių organizacijų vietiniai instruktoriai buvo paprašyti užpildyti apklausą. Atsakymus pateikė 55 vietiniai instruktoriai iš 73 pratybose dalyvavusių organizacijų. Apklausa buvo siekiama sužinoti kaip vietiniai instruktoriai vertina pasiruošimą pratyboms, pratybų vykdymą ir kibernetinio saugumo būklę savo organizacijoje.

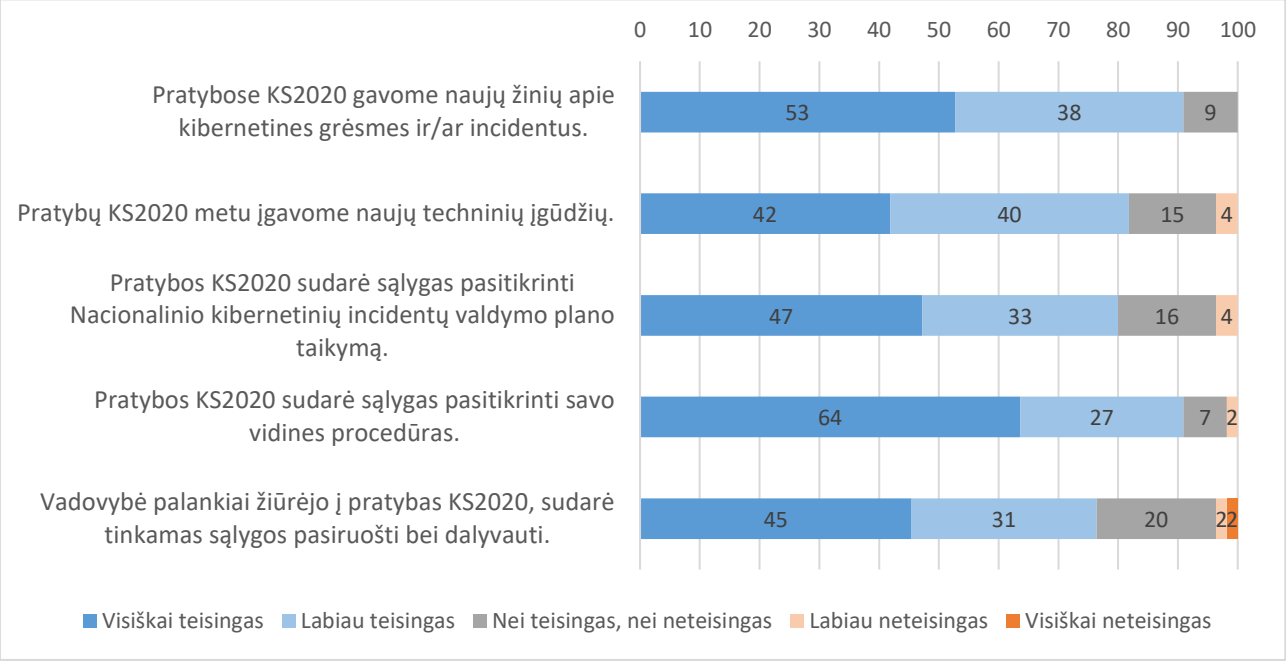
2. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE PRATYBŲ ORGANIZAVIMĄ REZULTATAI.

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

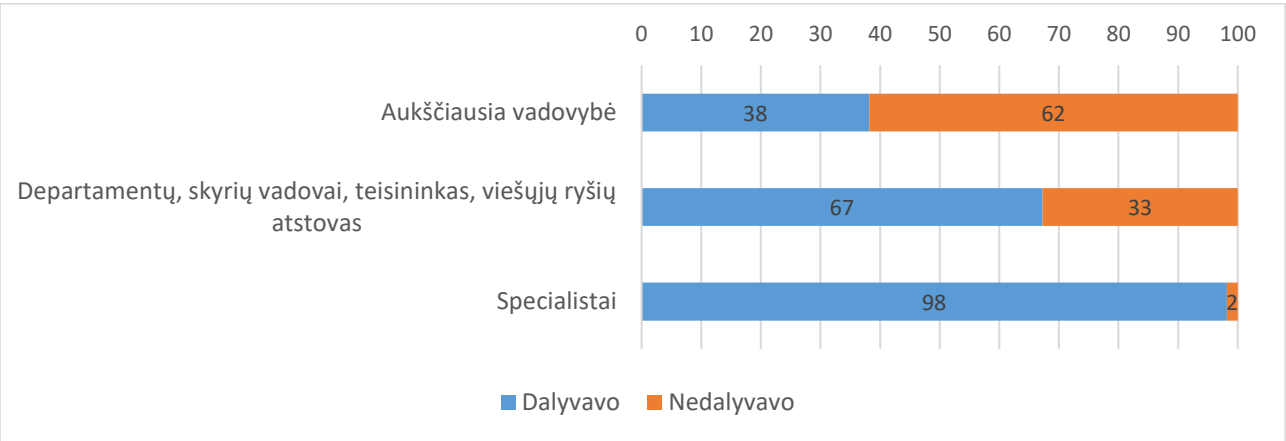


3. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE DALYVAVIMĄ PRATYBOSE REZULTATAI

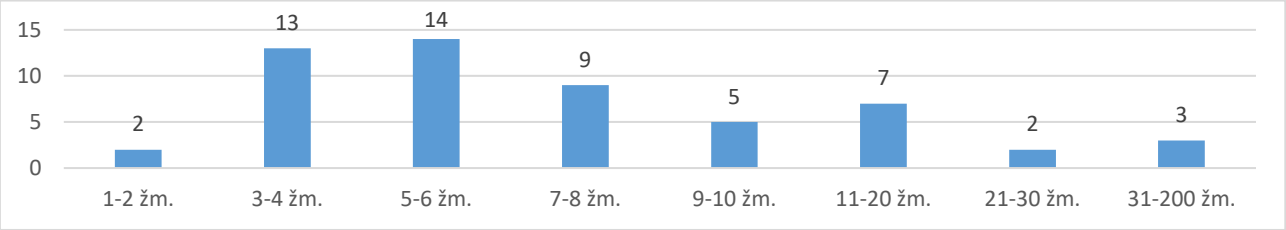
A. Vietinių instruktorių buvo klausiama, kiek, jų nuomone, yra teisingi teiginiai.



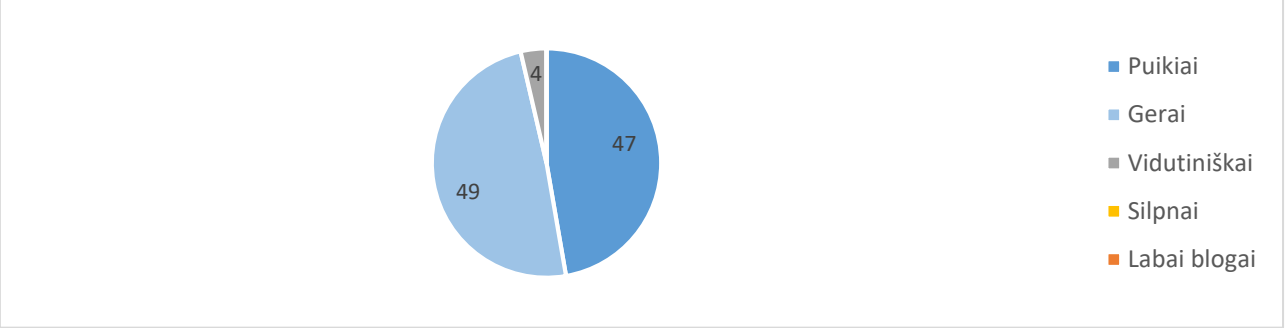
B. Kurie Jūsų organizacijos lygmenys įsitraukė į pratybas KS2020?



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



D. Koks yra Jūsų bendras pratybų „Kibernetinis skydas 2020“ vertinimas?



4. VIETINIŲ INSTRUKTORIŲ APKLAUSOS APIE KIBERNETINIO SAUGUMO BŪKLĘ ORGANIZACIJOJE REZULTATAI

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