NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
prie krašto apsaugos ministerijos

Gedimino pr. 40, Vilnius, tel. 1843, www.nksc.lt, el. p. info@nksc.lt

Kibernetinio saugumo centro rekomendacijos kibernetinio saugumo subjektams

Žalia CIS kontrolė

Žalia – žemiausios kategorijos Interneto saugumo centro (angl. *Center for Internet Security*, toliau – CIS) kontrolės priemonė rekomenduojama mažoms ar vidutinėms įmonėms, turinčioms ribotą informacinių technologijų (toliau – IT) ir kibernetinio saugumo patirtį, skirta IT turto ir personalo apsaugai. Pagrindinis šių įmonių tikslas yra užtikrinti verslo tęstinumą. Duomenų, kuriuos įmonė bando apsaugoti, jautrumas yra mažas ir tokie duomenys dažniausiai susiję su darbuotojais ir jų finansine informacija.

Oranžinė CIS kontrolė

Oranžinė – vidutinės kategorijos CIS kontrolės priemonė rekomenduojama įmonės darbuotojams, atsakingiems už IT infrastruktūros valdymą ir apsaugą, ir įmonėms, turinčioms departamentus su skirtingais rizikos profiliais. Taip pat, įmonėse, kuriose apdorojami jautrūs įmonės ar klientų duomenys, gali trumpam sutrikti veikla. Taip pat rekomenduojama įmonėms, kurioms pažeidimas sukeltų didelę reputacinę žalą. Oranžinė CIS kontrolė apima ir žalias CIS kontrolės priemones.

Raudona CIS kontrolė

Raudona – aukščiausios kategorijos CIS kontrolės priemonė rekomenduojama saugos ekspertams, kurie specializuojasi įvairiuose kibernetinio saugumo srityse (pvz., rizikos valdymo, įsilaužimo testavimo, programų saugumo). Taip pat rekomenduojama įmonėms, kurių duomenys yra riboto naudojimo (viešai neskelbtini), arba įmonėms, kurios vykdo funkcijas, susijusias su teisiniu reguliavimu, atitikties vertinimu ir priežiūra, ir įmonėms, kurios turi atkreipti dėmesį į paslaugų prieinamumą ir jautrių duomenų konfidencialumą ir vientisumą. Raudona CIS kontrolė apima žalias ir oranžines CIS kontrolės priemones.

SAUGUMĄ DIDINANTI PRIEMONĖ	APRAŠYMAS

01 Organizacijos techninės įrangos identifikavimas ir valdymas (angl. *Inventory and Control of Enterprise Assets*)

Veiksmingai valdyti (inventorizuoti, stebėti ir koreguoti trūkumus) organizacijos tinkle veikiančią techninę įrangą ir užtikrinti tinkamą organizacijos tinklo resursų naudojimą.

- Sudaryti ir nuolat atnaujinti leistinų įrenginių sąrašus.
- Užtikrinti neleistinų įrenginių aptikimo procesą.
- Naudoti specializuotą įrankį neleistiniems įrenginiams aptikti.
- Rinkti dinaminio protokolo (angl. *Dynamic Host Configuration Protocol* (DHCP)) audito įrašus.
- Naudoti pasyvų neleistinų įrenginių aptikimo įrankį.

02 Organizacijos programinės įrangos (toliau – PĮ) identifikavimas ir valdymas (angl. *Inventory and Control of Software Assets*)

Veiksmingai valdyti (inventorizuoti, stebėti ir šalinti trūkumus) organizacijos prietaisuose veikiančią PĮ ir užtikrinti tik leistinos PĮ naudojimą.

- Inventorizuoti ir prižiūrėti detalų įrenginiuose įdiegtos PĮ sąrašą.
- Užtikrinti, kad įdiegta PĮ būtų palaikoma gamintojų.
- Užtikrinti, kad neleistina PĮ būtų nenaudojama organizacijos įrenginiuose arba turėtų dokumentuotas naudojimo išimtis.
- Naudoti PĮ inventorizavimo įrankius.
- Sudaryti leistinos PĮ sąrašą ir užtikrinti jo laikymąsi techninėmis priemonėmis.
- Sudaryti leistinų PĮ bibliotekų sąrašą ir užtikrinti jo laikymąsi techninėmis priemonėmis.
- Sudaryti leistiną vykdomojo kodo (angl. *scripts*) sąrašą ir užtikrinti jo laikymąsi techninėmis priemonėmis.

03 Duomenų apsauga (angl. *Data Protection*)

Taikyti procesus ir technines kontrolės priemones, skirtas duomenims identifikuoti, klasifikuoti, apdoroti, išlaikyti ir sunaikinti.

- Sukurti ir nuolat atnaujinti duomenų valdymo procesą.
- Pagal duomenų valdymo procesą inventorizuoti duomenis ir palaikyti inventorizacijos aktualumą.
- Taikyti duomenų prieigos kontrolę, vadovaujantis „būtina žinoti“ principu.
- Užtikrinti duomenų saugojimą.
- Saugiai šalinti duomenis.
- Šifruoti duomenis naudotojų įrenginiuose.
- Sukurti ir nuolat atnaujinti duomenų klasifikavimo schemą.
- Dokumentuoti duomenų srautus.
- Šifruoti duomenis nešiojamosiose laikmenose.
- Šifruoti siunčiamus duomenis.
- Šifruoti saugomus duomenis.
- Klasifikuotus duomenis apdoroti ir saugoti klasifikacijos lygį atitinkančioje aplinkoje.
- Naudoti duomenų praradimo prevencijos (angl. *Data Loss Prevention*) priemones.
- Stebėti ir registruoti (daryti prieigos audito įrašus) jautrių duomenų prieigą, modifikavimą ir pašalinimą.

04 Saugios konfigūracijos nustatymas ir taikymas organizacijos techninėje ir PĮ (angl. *Secure Configuration of Enterprise Assets and Software*)

Sukurti ir veiksmingai valdyti (stebėti, tikslinti ir rengti ataskaitas) nešiojamųjų įrenginių, darbo vietų, tarnybinių stočių ar tinklo įrenginių techninės ir PĮ saugią konfigūraciją (saugumo nustatymus). Konfigūracijų pokyčiai turi būti griežtai stebimi ir valdomi.

- Sukurti ir veiksmingai valdyti saugios konfigūracijos procesą.
- Sukurti ir veiksmingai valdyti tinklo infrastruktūros saugią konfigūraciją.
- Neatliekant jokių veiksmų įrenginiuose, nustatyti automatinį sesijos nutraukimą.
- Įdiegti ir valdyti ugniasienes tarnybinėse stotyse.
- Įdiegti ir valdyti ugniasienes naudotojų įrenginiuose.
- Naudoti saugius duomenų perdavimo protokolus (HTTPS ir SSH).
- Išjungti arba apriboti gamyklines paskyras (angl. *default account*).
- Pašalinti arba išjungti darbo funkcijoms atlikti nereikalingas paslaugas, PĮ, taikomųjų programų modulius.
- Naudoti patikimas domenų vardų sistemas (angl. Domain Name System) (toliau – DNS).
- Mobiliuosiuose įrenginiuose naudoti nesėkmingų bandymų prisijungti limitą, kurį viršijus įrenginys būtų automatiškai blokuojamas.
- Mobiliuosiuose įrenginiuose įdiegti priemones, leisiančias nuotoliniu būdu neatkuriamai ištrinti duomenis.
- Mobiliuosiuose įrenginiuose atskirti organizacijos darbinę aplinką nuo asmeninės.

05 Paskyrų valdymas (angl. *Account Management*)

Taikyti procesus ir priemones, skirtus naudotojų, administratorių ir sistemų paskyroms stebėti ir kontroliuoti. Prieigos teisių suteikimo procesas turi būti griežtai kontroliuojamas.

- Inventorizuoti ir prižiūrėti organizacijos valdomas paskyras.
- Organizacijoje naudoti tik unikalius slaptažodžius (14 arba 8 simbolių slaptažodį, jeigu naudojamas dviejų veiksnių autentikavimas (toliau — MFA)).
- Deaktyvuoti paskyras, jei jomis nesinaudojama daugiau nei 45 dienas.
- Užtikrinti, kad administratoriaus paskyros būtų naudojamos tik administravimo darbams atlikti. Bendrojo pobūdžio darbai turi būti atliekami iš administratoriaus teisių neturinčių paskyrų.
- Inventorizuoti ir prižiūrėti sistemų paskyras (angl. service accounts), kurios naudojamos sistemoms veikti tarpusavyje.
- Centralizuoti paskyrų valdymą

06 Prieigos teisių valdymas (angl. *Access Control Management*)

Taikyti procesus ir priemones, skirtas stebėti ir kontroliuoti, kad prieiga prie organizacijos išteklių būtų suteikiama tik tiems naudotojams, kuriems tai yra būtina. Suteikiant prieigą, vadovautis iš anksto numatyta politika darbo vietoms, PĮ, bei žmogiškiesiems resursams.

- Sukurti prieigos suteikimo procesą.
- Sukurti prieigos panaikinimo procesą.
- Naudoti MFA išorės paslaugose.
- Naudoti MFA nuotoliniams prisijungimams.
- Naudoti MFA administratoriaus paskyrose.
- Inventorizuoti ir prižiūrėti autentifikavimo ir autorizavimo sistemas.
- Centralizuoti visų įrenginių prieigos kontrolę.
- Naudoti rolėmis pagrįstą prieigos kontrolę (angl. *Role-Based Access Control*).

07 Nuolatinis pažeidžiamumų vertinimas (angl. *Continuous Vulnerability Management*)

Nuolat rinkti ir vertinti informaciją, susijusią su PĮ pažeidžiamumais ir saugumo spragų išnaudojimu. Sužinojus apie PĮ pažeidžiamumus veikti nedelsiant, taip sumažinant galimybes piktavaliams pasinaudoti saugumo spragomis.

- Sukurti ir nuolat atnaujinti pažeidžiamumų valdymo procesą.
- Sukurti ir nuolat atnaujinti pažeidžiamumų šalinimo procesą.
- Taikyti automatizuotą operacinių sistemų atnaujinimo valdymą.
- Taikyti automatizuotą taikomųjų programų atnaujinimo valdymą.
- Vadovaujantis nustatytu pažeidžiamumų valdymo procesu, atlikti automatizuotus vidinių sistemų pažeidžiamumų skenavimus.
- Vadovaujantis nustatytu pažeidžiamumų valdymo procesu, atlikti automatizuotus išorinių sistemų pažeidžiamumų skenavimus.
- Vadovaujantis nustatytu pažeidžiamumų valdymo procesu, pašalinti nustatytus pažeidžiamumus.

08 Audito žurnalinių įrašų valdymas (angl. *Audit Log Management*)

Fiksuoti ir valdyti audito įrašus, galinčius padėti nustatyti, ištirti ir užkardyti kibernetines atakas.

- Sukurti ir nuolat atnaujinti audito įrašų valdymo procesą.
- Rinkti audito įrašus.
- Tinkamai saugoti audito įrašus.
- Standartizuoti laiko sinchronizaciją visuose įrenginiuose ir naudoti bent du laiko sinchronizavimo šaltinius.
- Rinkti detalesnius audito įrašus su jautriais duomenimis veikiančiuose įrenginiuose.
- Rinkti organizacijos DNS užklausų audito įrašus.
- Rinkti organizacijos unikalaus interneto svetainės ar tinklalapio adreso (angl. Uniform Resource Locator) (toliau –URL) užklausų audito įrašus.
- Rinkti komandinės eilutės audito įrašus.
- Užtikrinti centralizuotą audito įrašų rinkimą ir saugojimą.
- Audito įrašus saugoti ne mažiau kaip 90 dienų.
- Užtikrinti nuolatinę audito įrašų peržiūrą.
- Rinkti trečiųjų šalių ir (ar) paslaugų teikėjų veiksmų audito įrašus.

09 El. pašto ir žiniatinklio naršyklės apsauga (angl. *Email and Web Browser Protections*)

Mažinti galimybes piktavaliams tiesiogiai kontaktuoti ir manipuliuoti el. pašto ir žiniatinklio naudotojais.

- Naudoti tik leistinas ir atnaujintas naršyklės ir el. pašto aplikacijas.
- Naudoti DNS filtravimo funkciją.
- Naudoti tinkle (angl. Network-Based) veikiančius URL filtrus visuose organizacijos įrenginiuose.
- Drausti nereikalingus arba nepatvirtintus naršyklės ir el. pašto plėtinius.
- Siekiant sumažinti suklastotų ar pakeistų el. laiškų tikimybę sukurti DMARC (angl. Domain-based Message Authentication Reporting, and Conformance) politiką.
- Blokuoti neleistinus failų tipus.
- Įdiegti ir nuolat atnaujinti el. pašto serverio apsaugą nuo kenkimo PĮ.

10 Apsauga nuo kenkimo programų (angl. *Malware Defenses*)

Drausti ir kontroliuoti kenkimo programinio kodo diegimą, plitimą ir naudojimą organizacijos įrenginiuose.

- Įdiegti kenkimo PĮ aptikimo PĮ visuose organizacijos įrenginiuose.
- Automatizuoti kenkimo kodo požymių (angl. *signatures*) atnaujinimą.
- Uždrausti automatinio vykdymo (angl. *Autorun*) ir paleidimo (angl. *Autoplay*) iš nešiojamųjų laikmenų funkcionalumą.
- Automatiškai tikrinti nešiojamąsias laikmenas dėl kenkimo programinio kodo.
- Naudoti žalos mažinimo priemones (angl. *Anti-exploitation*).
- Centralizuotai valdyti kenkimo kodo aptikimo PĮ.
- Naudoti elgsena pagrįstą (angl. *Behavior-Based*) kenkimo kodo aptikimo įrangą.

11 Duomenų atkūrimas (angl. *Data Recovery*)

Taikyti procesus ir priemones, padedančias atkurti organizacijos duomenis ir priemones į patikimą, iki incidento buvusią būseną.

- Sukurti ir nuolat atnaujinti duomenų atkūrimo procesą.
- Automatiškai daryti atsargines kopijas.
- Užtikrinti atsarginių kopijų apsaugą.
- Bent vieną duomenų kopiją saugoti izoliuotoje (atskirtoje nuo darbinės) aplinkoje.
- Kas ketvirtį atlikti bandomąjį duomenų atkūrimą.

12 Tinklo infrastruktūros valdymas (angl. *Network Infrastructure Management*)

Siekiant sumažinti galimybes piktavaliams rengti kibernetines atakas, būtina veiksmingai valdyti (sekti, pranešti ir pašalinti trūkumus) tinklo įrenginių naudojimą.

- Užtikrinti, kad tinklo infrastruktūra būtų nuolat atnaujinama.
- Naudoti tinklo segmentavimą, privilegijų ribojimą bei prieinamumo didinimą ir užtikrinti saugią tinklo architektūrą.
- Saugiai valdyti tinklo infrastruktūrą (naudoti SSH, HTTPS ir kitus šifruotus protokolus).
- Sukurti ir nuolat atnaujinti architektūros schemą (-as) ir kitą tinklo dokumentaciją.
- Centralizuoti tinklo autentifikavimą, autorizavimą ir auditą (AAA) (angl. Authentication, Authorization and Auditing).
- Naudoti saugius tinklo komunikacijos protokolus (pvz., 802.1X, WPA2 Enterprise).
- Užtikrinti, kad jungiantis prie organizacijos infrastruktūros iš išorės būtų naudojamas virtualus privatus tinklas (angl. Virtual Private Network, VPN).
- Administravimo darbus atlikti tik iš tam skirtų įrenginių (fizinių arba virtualių), atskirtų nuo pagrindinio organizacijos tinklo ir atjungtų nuo interneto.

13 Tinklo stebėsena ir apsauga (angl. *Network Monitoring and Defense*)

Taikyti procesus ir priemones užtikrinant išsamią tinklo stebėseną ir apsaugą nuo saugumo grėsmių visoje organizacijos tinklo infrastruktūroje.

- Centralizuoti įspėjimus apie saugumo įvykius.
- Įdiegti įsilaužimų aptikimo sprendimą (angl. Intrusion Detection Solution, IDS).
- Naudoti įsilaužimų į tinklą aptikimo sprendimą (angl. Network Intrusion Detection System, NIDS).
- Užtikrinti tinklo srauto filtravimą tarp tinklo segmentų.
- Valdyti nuotolinių įrenginių prieigą.
- Saugoti ir analizuoti tinklo srauto įrašus.
- Įdiegti įsilaužimų prevencijos sprendimą (angl. Intruder Prevention System, IPS).
- Įdiegti įsilaužimų į tinklą prevencijos sprendimą (angl. Network Intrusion Prevention System, NIPS).
- Užtikrinti prievado lygmens prieigos kontrolę.
- Užtikrinti aplikacijos lygmens filtravimą.
- Nuolat tobulinti saugumo įvykių pranešimų kriterijus.

14 Darbuotojų kibernetinio saugumo sąmoningumo ir įgūdžių mokymai (angl. *Security Awareness and Skills Training*)

Užtikrinti, kad organizacijos darbuotojai turėtų reikiamas žinias ir įgūdžius atpažinti kibernetines grėsmes. Nuolat didinti darbuotojų sąmoningumą sudarant ir taikant kibernetinio saugumo mokymo planą.

- Sukurti ir atnaujinti darbuotojų kibernetinio saugumo sąmoningumo programą.
- Nuolat mokyti darbuotojus atpažinti socialinės inžinerijos atakas, kuriomis siekiama išvilioti jautrius duomenis (angl. phishing).
- Supažindinti darbuotojus su gerosiomis autentifikavimo praktikomis, pvz., MFA.
- Supažindinti darbuotojus apie organizacijoje taikomą duomenų tvarkymo politiką, kaip saugoti, perduoti, archyvuoti ir naikinti jautrius duomenis.
- Informuoti darbuotojus apie netyčinio duomenų atskleidimo priežastis.
- Mokyti darbuotojus atpažinti saugumo incidentus ir pranešti apie juos.
- Mokyti darbuotojus, kaip patikrinti ir pranešti apie pasenusią PĮ.
- Informuoti darbuotojus apie grėsmes, kylančias naudojantis nesaugiais tinklais ir perduodant šiais tinklais duomenis.
- Organizuoti tikslinius kibernetinio saugumo mokymus IT administratoriams, naudotojams ir vadovams.

15 Paslaugų teikėjų valdymas (angl. *Service Provider Management*)

Sukurti paslaugų teikėjų, kurie administruoja jūsų organizacijos jautrius duomenis ar yra atsakingi už jūsų organizacijos kritinių sistemų priežiūrą, vertinimo procesą. Tai padės pasirinkti patikimus paslaugų teikėjus.

- Sudaryti ir nuolat atnaujinti trečiųjų šalių paslaugų teikėjų sąrašą.
- Sudaryti ir nuolat atnaujinti trečiųjų šalių paslaugų teikėjų valdymo politiką.
- Klasifikuoti trečiųjų šalių paslaugų teikėjus, atsižvelgiant į organizacijos įautrios informacijos pasiekiamumą, turimas prieigas ir rizikas ir kt.
- Užtikrinti, kad į sutartis su paslaugų teikėjais būtų įtraukti saugumo reikalavimai.
- Vertinti trečiųjų šalių paslaugų teikėjus.
- Kontroliuoti ir stebėti trečiųjų šalių atliekamus veiksmus.
- Užtikrinti, kad pasibaigus sutarties laikotarpiui su trečiųjų šalių paslaugų teikėju nedelsiant būtų apribota prieiga prie organizacijos resursų.

16 Taikomųjų programų saugumas (angl. *Application Software Security*)

Valdyti sukurtos ar įgytos PĮ saugumo elementus per visą jų gyvavimo ciklą. Stebėti ir aptikus ištaisyti saugumo spragas, taip užkertant kelią piktavaliams jomis pasinaudoti.

- Sukurti ir nuolat atnaujinti saugų taikomųjų programų kūrimo procesą.
- Sukurti ir nuolat atnaujinti procesą, skirtą pranešimams apie PĮ pažeidžiamumus (pranešimų priėmimas ir nagrinėjimas) valdyti.
- Atlikti saugumo pažeidžiamumų atsiradimo priežasčių analizę.
- Sukurti, veiksmingai valdyti ir nuolat atnaujinti naudojamų trečiųjų šalių PĮ komponentų sąrašus.
- Naudoti tik saugius ir patikimus trečiųjų šalių paslaugų teikėjų PĮ komponentus.
- Sudaryti taikomųjų programų pažeidžiamumų vertinimo skalę ir numatyti prioritetais paremtą pažeidžiamumų valdymo procesą.
- Naudoti rekomenduojamus saugios konfigūracijos šablonus, kurie padės sustiprinti aplikacijų infrastruktūros komponentų saugumą.
- Atskirti gamybines ir testuojamas sistemos aplinkas.
- Mokyti programuotojus saugaus programinio kodo kūrimo principų.
- Taikyti saugaus projektavimo principus taikomųjų programų architektūroje.
- Naudoti saugius ir išbandytus modulius ar paslaugas aplikacijos komponentuose.
- Naudoti statinės ir dinaminės analizės įrankius, siekiant patikrinti, ar laikomasi saugaus programavimo praktikos.
- Atlikti programos įsilaužimo testavimą.
- Atlikti programos grėsmių modeliavimą.

17 Incidentų valdymas (angl. *Incident Response Management*)

Siekiant užtikrinti organizacijos informacijos ir reputacijos apsaugą ir veikos tęstinumą, parengti incidentų valdymo politiką (kibernetinių incidentų valdymo, veiklos tęstinumo valdymo, atsakingų asmenų ir funkcijų paskirstymo planus ir t. t.). Tai padės greičiau reaguoti į vykstančias atakas, efektyviau suvaldyti žalą, aptikti įsilaužėlius ir panaikinti jų veiklos padarinius, atkurti tinklo ir sistemų veiklą.

- Paskirti už kibernetinių incidentų nagrinėjimą atsakingus asmenis.
- Sudaryti ir nuolat atnaujinti asmenų, su kuriais reikia komunikuoti valdant incidentą, sąrašą (vidiniai darbuotojai, atsakingų institucijų atstovai, trečiųjų šalių tiekėjai ir pan.)
- Sukurti ir nuolat tobulinti pranešimų apie kibernetinius incidentus procesą organizacijoje.
- Sukurti ir nuolat atnaujinti incidentų valdymo procesą.
- Paskirti atsakingą už reagavimą į kibernetinius incidentus personalą, nustatyti jo funkcijas ir atsakomybę reaguojant į kibernetinius incidentus.
- Nustatyti konkrečius komunikavimo mechanizmus reaguoti į kibernetinius incidentus.
- Reguliariai vykdyti incidentų valdymo pratybas.
- Rengti įvykusių kibernetinio incidentų ataskaitas.
- Aiškiai apibrėžti ir atskirti kibernetinių incidentų ir įvykių ribas.

18 Įsilaužimo testavimas (angl. *Penetration Testing*)

Priemonės tikslas – visapusiškai išbandyti organizacijos (personalo, procesų, technologijų) atsparumą įsilaužimams, imituojant galimus piktavalio veiksmus.

- Sukurti ir nuolat tobulinti įsilaužimo testavimo programą.
- Periodiškai atlikti išorinį įsilaužimo testavimą.
- Pašalinti įsilaužimo testavimo metu aptiktas silpnąsias vietas.
- Atlikus įsilaužimo testavimą, koreguoti saugos priemones, kad būtų aptinkamos testavimo metu naudotos įsilaužimo technikos.
- Periodiškai atlikti vidinį įsilaužimo testavimą.

Pagrindinės rekomendacijos:

Inventorizuoti, identifikuoti techninę ir PĮ. Turimų resursų informacija padeda juos valdyti, priimti sprendimus bei pritaikyti kontrolės priemones. Tai yra vienas iš kertinių informacijos šaltinių, kuriais užtikrinamas tolesnis organizacijos kibernetinis saugumas.

Atnaujinti organizacijoje naudojamą PĮ. Kibernetiniai nusikaltėliai, sužinoję apie išleistus programų atnaujinimus, juos ištiria ir stengiasi pasinaudoti programų spragomis, atsirandančiomis dėl asmenų, delsiančių atnaujinti programas, aplaidumo, siųsdami į jų kompiuterius kenkimo programinį kodą.

Užtikrinti organizacijoje prieigų kontrolę ir valdymą. Labai svarbu užtikrinti administratoriaus teises turinčių paskyrų kontrolę. Iš administratoriaus teises turinčių paskyrų turi būti atliekami tik administravimo darbai, kitiems darbams atlikti turi būti naudojamos naudotojo paskyros.

Reguliariai daryti sistemų atsargines kopijas. Atsarginės kopijos užtikrina organizacijos veiklos tęstinumą įvykus kibernetiniam incidentui. Atsarginės kopijos turi būti nuolat testuojamos ir saugomos keliose vietose, atskiroje infrastruktūroje.

Maketavo KAMBRD Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius; 2024. Spausdino LK KKC, Muitinės g. 4, Domeikava, LT-54359 Kauno r.; www.kam.lt