31992D0242

1992 5 8 EUROPOS BENDRIJŲ OFICIALUSIS LEIDINYS L 123/19

TARYBOS SPRENDIMAS
1992 m. kovo 31 d.
dėl informacinių sistemų apsaugos

(92/242/EEB)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Europos ekonominės bendrijos steigimo sutartį ir ypač į jos 235 straipsnį,

atsižvelgdama į Komisijos pasiūlymą [1],

atsižvelgdama į Europos Parlamento nuomonę [2],

atsižvelgdama į Ekonomikos ir socialinių reikalų komiteto nuomonę [3],

kadangi Bendrijos užduotis, kuriant bendrąją rinką ir palaipsniui suderinant valstybių narių ekonomines politikas, yra visoje Bendrijoje skatinti darnią ekonominę veiklą, nuolatinį ir apgalvotą plėtimąsi, didėjantį stabilumą, greitai augantį gyvenimo lygį, glaudesnius valstybių narių tarpusavio ryšius;

kadangi saugoma, apdorojama ir elektroniniu būdu perduodama informacija tampa vis svarbesnė ekonominėje ir socialinėje veikloje;

kadangi veiksmingų tarptautinių ryšių priemonių atsiradimas ir plintantis elektroninių informacijos tvarkymo priemonių įsigalėjimas pabrėžia tinkamos apsaugos poreikį;

kadangi Europos Parlamentas savo debatuose ir sprendimuose nuolat pabrėžia informacinių sistemų apsaugos svarbą;

kadangi Ekonomikos ir socialinių reikalų komitetas pabrėžia būtinybę spręsti su informacinių sistemų apsauga susijusias Bendrijos veiklos priemones, ypač sėkmingai pabaigus kurti vidaus rinką;

kadangi veiklos formos nacionaliniu, tarptautiniu ir Bendrijos lygmeniu yra tinkamas pagrindas pradžiai;

kadangi telekomunikacijos, informacinės technologijos, standartizavimas, informacijos rinka, tyrimų, plėtros ir technologijų politikos, o taip pat ir veikla, Bendrijos pradėta šiose srityse, yra glaudžiai susiję;

kadangi tikslinga užtikrinti, kad bendromis pastangomis būtų tęsiamas nacionaliniu ir tarptautiniu lygmeniu pradėtas darbas ir būtų siekiama, kad pagrindinės dalyvaujančios šalys bendradarbiautų; kadangi reikėtų šią veiklą tęsti pagal nuoseklų bendrų veiksmų planą;

kadangi dėl jų sudėtingumo informacinių sistemų apsaugai būtina sukurti strategijas, kurios leistų informacijai laisvai judėti bendrojoje rinkoje ir taip pat užtikrintų informacijos naudojimo saugumą visoje Bendrijoje;

kadangi kiekviena valstybė narė pati atsako už tai, kad būtų atsižvelgta į saugumo ir viešosios tvarkos sąlygojamus apribojimus;

kadangi valstybių narių įsipareigojimai šioje srityje apima suderintas pastangas, paremtas glaudžiu bendradarbiavimu su aukštesniais valstybių narių pareigūnais;

kadangi turi būti numatytas veiksmų plano sudarymas pradiniam 24 mėnesių laikotarpiui ir Aukštesniųjų pareigūnų komiteto su ilgalaikiu įgaliojimu patarti Komisijai dėl veiksmų, diegiant informacijos apsaugos sistemas, įsteigimas;

kadangi manoma, jog pradiniam 24 mėnesių veiksmų planui įgyvendinti prireiks 12 mln. ekiu sumos; kadangi, atsižvelgiant į dabartinę finansinę situaciją, numatyta, kad 1992 metams reikalinga suma bus lygi 2 mln. ekiu;

kadangi sumos, skirtos programai finansuoti laikotarpiui po 1992 biudžetinių metų, sudarys dabartinės Bendrijos finansų sistemos dalį,

NUSPRENDĖ:

1 straipsnis

Priimamas veiksmų planas informacinių sistemų apsaugos srityje. Jį sudaro:

— informacinių sistemų apsaugos bendrosios strategijos (veiksmų plano) sukūrimas pradiniam 24 mėnesių laikotarpiui ir

— Aukštesniųjų pareigūnų grupės (toliau – Komitetas) su ilgalaikiu įgaliojimu patarti Komisijai dėl veiksmų, diegiant informacinių sistemų apsaugą, įsteigimas.

(1) OL C 277, 1990 11 5, p. 18.
(2) OL C 94, 1992 3 13.
(3) OL C 159, 1991 6 17, p. 38.

2 straipsnis

1. Komisija sistemingai konsultuojasi su Komitetui dėl klausimų, susijusių su informacinių sistemų apsauga įvairiose Bendrijos vykdomose veiklose, ypač apibrėžiant darbo strategijas ir programas.

2. Kaip nurodyta priede, veiksmų planas apima parengiamąjį darbą tokiomis temomis:

I. Informacinių sistemų apsaugos strateginės programos formavimas.

II. Vartotojo ir paslaugos teikėjo reikalavimų informacinių sistemų apsaugai nustatymas.

III. Vartotojų, tiekėjų ir paslaugos teikėjų skubių ir laikinų poreikių tenkinimas.

IV. Informacinių sistemų apsaugos techninių charakteristikų, standartizavimo, įvertinimo ir sertifikavimo tvarkos nustatymas.

V. Informacinių sistemų apsaugos technologijų ir jų veikimo plėtojimas.

VI. Informacinių sistemų apsaugos teikimas.

3 straipsnis

1. Veiksmų plano vykdymui pradiniu laikotarpiu apskaičiuotas būtinas Bendrijos lėšas sudaro 12 mln. ekiu, iš kurių 2 mln. ekiu yra numatyti 1992 metams, atsižvelgiant į 1988–1992 m. finansinę perspektyvą.

Vėlesniu programos taikymo laikotarpiu reikalinga suma turės būti įtraukta į galiojančią Bendrijos finansinės veiklos struktūrą.

2. Už biudžetą atsakingos institucijos nustato kiekvieniems finansiniams metams skiriamus asignavimus, atsižvelgdamos į gero valdymo principus, minimus Finansinio reglamento, taikytino Europos Bendrijų bendram biudžetui, 2 straipsnyje.

4 straipsnis

Per pradinį laikotarpį pasiektus rezultatus Komisijos prašymu vertina nepriklausomų ekspertų grupė. Šios grupės parengta ataskaita kartu su Komisijos pastabomis pateikiama Europos Parlamentui ir Tarybai.

5 straipsnis

1. Komisija atsako už veiksmų įgyvendinimą. Jai padeda patariamasis komitetas, kurį sudaro valstybių narių atstovai ir kuriam pirmininkauja Komisijos atstovas.

2. Veiksmų planas įgyvendinamas laikantis 2 straipsnyje nurodytų tikslų ir prireikus papildomas. Plane nurodomi detalūs tikslai ir būsimų veiksmų pobūdis, taip pat finansiniai susitarimai šių veiksmų atžvilgiu. Komisija kreipiasi pasiūlymų dėl veiksmų plano apimties.

3. Veiksmų planas įgyvendinamas tos srities veikėjams glaudžiai bendradarbiaujant. Jame atsižvelgiama į šioje srityje vykdomą Europos ir tarptautinę standartizavimo veiklą, ji skatinama ir plečiama.

6 straipsnis

1. 7 straipsnyje numatyta procedūra taikoma:

— priemonėms, susijusioms su Bendrijos politika informacinių sistemų apsaugos srityje.

2. 8 straipsnyje numatyta procedūra taikoma:

— 5 straipsnyje minimam veiksmų planui parengti ir papildyti,

— kreipimosi pasiūlymų turiniui, pasiūlymų vertinimui ir Bendrijos tam tikroms priemonėms numatomai skirti sumai, jei ji viršija 200 000 ekiu,

— bendradarbiavimo veiklai, kurią pagal šį sprendimą vykdo Bendrijai nepriklausančios organizacijos,

— susitarimams dėl šių priemonių rezultatų platinimo, apsaugos ir naudojimo,

— priemonėms, kurių reikia imtis veiksmams įvertinti.

3. Jeigu Bendrijos skirta tam tikroms priemonėms suma yra mažesnė arba lygi 200 000 ekiu, Komisija konsultuoja Komitetą dėl diegtinų priemonių ir informuoja jį apie vertinimo rezultatus.

7 straipsnis

Komisijos atstovas įteikia Komitetui diegtinų priemonių projektą. Komitetas pateikia savo nuomonę apie šį projektą per laikotarpį, kurį gali nustatyti pirmininkas, atsižvelgdamas į svarstomos problemos skubumą, jei reikia, balsuodamas.

Išvada įrašoma protokole. Be to, kiekviena valstybė narė turi teisę prašyti, kad jos išvada būtų užregistruota protokole.

Komisija ypač atsižvelgia į Komiteto pareikštą išvadą ir informuoja Komitetą apie tai, kokiu būdu į ją buvo atsižvelgta.

8 straipsnis

Komisijos atstovas pateikia Komitetui diegtinų priemonių projektą. Komitetas pateikia savo išvadą apie šį projektą per laikotarpį, kurį gali nustatyti pirmininkas, atsižvelgdamas į svarstomos problemos skubumą. Nuomonė pareiškiama balsų

dauguma, numatyta Sutarties 148 straipsnio 2 dalyje, reglamentuojančioje sprendimus, kuriuos Taryba privalo priimti Komisijai pasiūlius. Valstybių narių atstovų Komitete balsai paskirstomi tame straipsnyje numatytu būdu. Pirmininkas nebalsuoja.

Komisija patvirtina pasiūlytas priemones, jei jos atitinka Komiteto nuomonę.

Jei pasiūlytos priemonės neatitinka Komiteto nuomonės arba nuomonė nepareiškiama, Komisija nedelsdama perduoda Tarybai savo pasiūlymą dėl diegtinų priemonių. Taryba priima sprendimus kvalifikuota dauguma.

Jeigu gavusi pasiūlymą Taryba per tris mėnesius nepriima jokio sprendimo, Komisija patvirtina pasiūlytas priemones, išskyrus tas, kurioms Taryba nepritarė paprastąja dauguma.

Priimta Briuselyje, 1992 m. kovo 31 d.

Tarybos vardu

Pirmininkas

Vitor MARTINS

PRIEDAS

Veiklos krypčių santrauka

VEIKSMŲ PLANO KRYPTYS INFORMACINIŲ SISTEMŲ APSAUGOS SRITYJE

ĮVADAS

Veiksmų plano tikslas – sukurti bendras strategijas, kurios leistų suteikti elektroniniu būdu kaupiamos, apdorojamos ir perduodamos informacijos vartotojams ir gamintojams tinkamą informacinių sistemų apsaugą nuo atsitiktinių ir tyčinių grėsmių.

Veiksmų planas atsižvelgia į pasaulyje vykstantį šios srities standartizavimo procesą ir jį papildo.

Jis apima tokias veiklos kryptis:

— informacinių sistemų apsaugos strategijos kūrimą,

— vartotojo ir paslaugos teikėjo reikalavimų informacinių sistemų apsaugai nustatymą,

— vartotojų, tiekėjų ir paslaugos teikėjų skubių ir laikinų poreikių tenkinimą,

— informacinių sistemų apsaugos techninių charakteristikų, standartizavimo, įvertinimo ir sertifikavimo tvarkos nustatymą,

— informacinių sistemų apsaugos technologijų ir jų veikimo plėtojimą,

— informacinių sistemų apsaugos teikimą.

Veiksmų planą vykdo Komisija, atsižvelgdama į valstybių narių šioje srityje vykdomus veiksmus ir į Bendrijos tyrimų ir darbo rezultatus.

1. **I veiklos kryptis – Informacinių sistemų apsaugos strategijos kūrimas**

1.1. *Esmė*

Informacinių sistemų apsauga pripažįstama kaip sparčiai plintanti ypatybė, neatsiejama nuo šiuolaikinės visuomenės. Elektroniniu būdu teikiamoms informacijos paslaugoms reikia saugios telekomunikacijų infrastruktūros, saugios kompiuterinės ir programinės įrangos, taip pat saugios informacijos naudojimo ir valdymo sistemos. Būtina sukurti bendrą strategiją, apimančią visus informacinių sistemų apsaugos aspektus, kad būtų išvengta dalinio problemų sprendimo. Bet kokia elektroniniu būdu apdorojamos informacijos apsaugos strategija privalo atspindėti bet kurios visuomenės siekį efektyviai veikti ir tuo pat metu apsisaugoti greitai besikeičiančiame pasaulyje.

1.2. *Tikslas*

Strategija turi būti kuriama, derinant socialinius, ekonominius ir politinius tikslus su techninėmis, veiklos ir teisinėmis Bendrijos galimybėmis tarptautiniu mastu. Visa apimančią įvairių aspektų, tikslų ir apribojimų pusiausvyrą turi išlaikyti šioje srityje veikiantys asmenys, kurie bendromis pastangomis kuria vieningą požiūrį ir suderintą strategiją. Toks požiūris yra išankstinė interesų ir poreikių derinimo sąlyga tiek nustatant politikas, tiek plėtojant pramoninį pritaikymą.

1.3. *Statusas ir tendencijos*

Dabartinei situacijai būdingas stiprėjantis suvokimas, jog būtina veikti. Tačiau be iniciatyvos derinti pastangas pavienės pastangos įvairiose srityse gali sukurti tokią situaciją, kai veiksmai faktiškai vienas kitam prieštaraus ir taps dar rimtesnių teisinių, socialinių ir ekonominių problemų priežastimi.

1.4. *Reikalavimai, galimybės ir prioritetai*

Tokia bendra strategija turėtų apimti nagrinėjamus ir apibrėžtus rizikos faktorių analizės ir rizikos valdymo klausimus, susijusius su informacinių ir panašių paslaugų pažeidžiamumu, su įstatymų ir jų lydimųjų aktų dėl kompiuterinių ir telefoninių ryšių neleistino arba netinkamo naudojimo suvienodinimu, su administracine infrastruktūra, apimančia ir apsaugos politikas, ir su veiksmingu jų diegimu įvairiose pramonės ir mokslo šakose, taip pat su socialiniais ir privatumo reikalais (pvz.: identifikavimo, patvirtinimo, neatsisakymo ir, jei įmanoma, įgaliojimo programų taikymas demokratinėje aplinkoje).

Turi būti pateikti aiškūs saugaus platinamų informacinių paslaugų fizinių ir loginių modelių, vystymo nurodymai, taip pat apsaugos užtikrinimo produktų ir paslaugų, bandinių ir prototipų standartai, taisyklės ir apibrėžimai, kad būtų sukurtos gyvybingos administracinės struktūros, modeliai ir standartai specifiniams atskirų sektorių poreikiams tenkinti.

Būtina ugdyti sąmoningumą apsaugos atžvilgiu ir tokiu būdu keisti vartotojų požiūrį į vis didėjantį susirūpinimą dėl informacinių technologijų (IT) saugumo.

2. **II veiklos kryptis — Vartotojų ir paslaugos teikėjų reikalavimų informacinių sistemų apsaugai nustatymas**

2.1. *Esmė*

Informacinių sistemų saugumas yra būtina išankstinė sąlyga verslo operacijų, intelektinės nuosavybės ir konfidencialumo vientisumui ir patikimumui užtikrinti. Dėl šios priežasties kartais sunku rasti pusiausvyrą arba net pasirinkti tarp laisvos prekybos ir įsipareigojimo saugoti privatumą ir intelektinę nuosavybę. Tokie pasirinkimai ir kompromisai turi būti grindžiami galutiniu reikalavimų įvertinimu ir informacinių sistemų apsaugos galimybėmis prie jų derintis.

Vartotojo reikalavimai apima informacinių sistemų apsaugos funkcionalumą, priklausantį nuo technologinių, veiklos ir valdymo aspektų. Todėl informacinių sistemų saugumo reikalavimų nuoseklus nagrinėjimas yra esminis kuriant tinkamas ir veiksmingas priemones.

2.2. *Tikslas*

Nustatyti vartotojų ir paslaugos teikėjų reikalavimų pobūdį bei ypatybes ir jų ryšį su informacinių sistemų apsaugos priemonėmis.

2.3. *Statusas ir tendencijos*

Iki šiol nebuvo dedamos suderintos pastangos greitai besirutuliojantiems ir besikeičiantiems šios srities pagrindinių veikiančių asmenų reikalavimams nustatyti. Bendrijos valstybės narės iškėlė poreikį suvienodinti nacionalines priemones šioje srityje (ypač kalbant apie „IT apsaugos vertinimo kriterijus“). Vienodi vertinimo kriterijai ir abipusis vertinimo sertifikatų pripažinimas yra ypatingai svarbūs.

2.4. *Reikalavimai, galimybės ir prioritetai*

Manoma, kad siekiant nuoseklaus ir skaidraus šioje srityje veikiančių asmenų pagrįstų poreikių traktavimo, yra būtina susitarti ir sudaryti bendrą vartotojų reikalavimų klasifikaciją ir numatyti jos ryšį su informacinių sistemų apsaugos teikimu.

Taip pat manoma, kad yra svarbu nustatyti reikalavimus įstatymams, jų lydimiesiems aktams ir veiklos nuostatams, atsižvelgiant į paslaugų pobūdžio ir technologijos tendencijų vertinimus, numatyti alternatyvias strategijas, kaip administracinėmis, paslaugų, veiklos ir technologinėmis priemonėmis pasiekti tikslus, ir įvertinti alternatyvių apsaugos priemonių bei strategijų veiksmingumą, jų pritaikymą poreikiams ir kaštus vartotojams, paslaugų teikėjams ir operatoriams.

3. **III veiklos kryptis — Vartotojų, tiekėjų ir paslaugos teikėjų skubių ir laikinų poreikių tenkinimas**

3.1. *Esmė*

Šiuo metu yra įmanoma tinkamai apsaugoti kompiuterius nuo neteisėto įsibrovimo iš šalies juos izoliuojant, t. y. taikant tradicines organizacines ir fizines priemones. Tos pačios priemonės yra veiksmingos ir apsaugant elektroninius ryšius tarp uždaros vartotojų grupės narių, dirbančių specializuoto tinklo pagrindu. Tačiau situacija keičiasi, jeigu informacija naudojasi keletas grupių, ja mainomasi viešais arba visiems prieinamais tinklais. Nei technologija, nei terminalai ar paslaugos, nei su jais susiję standartai ir procedūros nėra viešai prieinami, kad prireikus būtų galima pakankamai gerai apsaugoti informacines sistemas.

3.2. *Tikslas*

Reikia siekti sugebėti nedelsiant priimti sprendimus patiems skubiausiems vartotojų, paslaugų teikėjų ir gamintojų poreikiams tenkinti. Tai apima ir IT apsaugos vertinimo kriterijų taikymą. Jie turi būti atviri būsimiems reikalavimams ir sprendimams.

3.3. *Statusas ir tendencijos*

Kai kurios vartotojų grupės yra susikūrusios priemones ir procedūras pagal savo specifinius poreikius, ypač patvirtinimo, sąžiningumo ir neatsisakymo poreikius. Dažniausiai naudojamos magnetinės ir integroscheminės kortelės. Atskiri asmenys naudoja daugiau ar mažiau sudėtingas kriptografines priemones. Tokiu būdu institucijos buvo dažnai skirstomos pagal vartotojų grupes. Tačiau sunku apibendrinti šias priemones ir metodus ir pritaikyti atviros aplinkos poreikiams.

TSO (Tarptautinė standartų organizacija) naudoja OSI (*Open System Interconnection*) Informacinių sistemų apsaugą (ISO DIS – 7498-2) ir CCITT (Tarptautinis konsultacinis komitetas telekomunikacijų klausimais) programas X400 kontekste. Be to, įmanoma apsaugos elementus įterpti į žinutes. Patvirtinimo, sąžiningumo ir neatsisakymo komandos pasiekiamos tokių žinučių (EDIFACT) arba X400 MHS pagalba.

Šiuo metu Elektroninio duomenų perdavimo (EDI – *Electronic Data Interchange*) sistemos teisinis pagrindas egzistuoja tik kaip koncepcija. Tarptautiniai prekybos rūmai (*International Chamber of Commerce*) yra paskelbę vieningas taisykles, kaip keistis komerciniais duomenimis telekomunikacijų tinklais.

Keletas šalių (pvz.: Vokietija, Prancūzija, Didžioji Britanija ir Jungtinės Amerikos Valstijos) yra susikūrusios ar tebekuria kriterijus IT ir telekomunikacijos produktų ir sistemų patikimumui vertinti ir atitinkamas vertinimo procedūras. Šie kriterijai buvo derinami su vietiniais gamintojais, ir tai užtikrins patikimų produktų ir sistemų, pradedant nuo paprastų produktų, skaičiaus didėjimą. Įkūrus nacionalines organizacijas, kurios vertins ir teiks sertifikatus, ši tendencija dar labiau sustiprės.

Slaptumo reikalavimas daugumai vartotojų nėra pats svarbiausias. Tačiau ateityje situacija keisis, nes pažangios ryšių paslaugos, o ypač mobiliojo ryšio paslaugos, vyraus visur.

3.4. *Reikalavimai, galimybės ir prioritetai*

Būtina kuo greičiau sukurti procedūras, standartus, produktus ir įrankius, reikalingus užtikrinti ir informacinių sistemų (kompiuterių ir jų įrangos), ir viešų ryšio tinklų apsaugą. Patvirtinimo, sąžiningumo ir neatsisakymo programoms turėtų būti teikiama pirmenybė. Bandomieji projektai turėtų būti vykdomi, siekiant patikrinti siūlomų sprendimų patikimumą. Pirmumo teisę turintys Elektroninės duomenų perdavimo (EDI) sistemos poreikiai apžvelgiami TEDIS programoje, kur nagrinėjamas šio veiksmų plano turinys.

4. IV veiklos kryptis — Informacinių sistemų apsaugos techninių charakteristikų, standartizavimo, vertinimo ir sertifikavimo tvarkos nustatymas

4.1. *Esmė*

Reikalavimai informacinių sistemų apsaugai auga, ir tokios techninės charakteristikos bei standartai darosi būtini. Be IT apsaugos suderintų standartų ir techninių charakteristikų informacijos pasikeitimu pagrįstiems procesams ir paslaugoms visame ūkyje ir visuomenėje gali atsirasti esminių kliūčių. Taip pat būtina imtis veiksmų siekiant pagreitinti technologijos ir standartų kūrimą ir jų naudojimą su ryšiais ir kompiuteriniais tinklais susijusiose srityse, kurios yra ypač svarbios vartotojams, pramonei ir administravimui.

4.2. *Tikslas*

Būtina numatyti priemones specifinėms apsaugos funkcijoms, kurios padėtų tvarkyti OSI (*Open System Interconnection*), ONP (*Object N Programming*), ISDN/IBC (*Integrated Services Digital Network*) bendrąsias sistemas ir tinklus, paremti ir įgyvendinti. Neatsiejamos nuo techninių charakteristikų ir standartų kūrimo yra patikrinimo priemonės ir būdai, kurie apima sertifikavimą kaip abipusio pripažinimo pagrindą. Jei įmanoma, remtini tarptautiniai sprendimai. Būtina skatinti kompiuterinių sistemų su apsaugos funkcijomis kūrimą ir naudojimą.

4.3. *Statusas ir tendencijos*

Pavyzdžiui, Jungtinės Amerikos Valstijos deda esmines pastangas informacinių sistemų saugumui užtikrinti. Europoje problema sprendžiama IT ir telekomunikacijų standartizavimu ETSI ir CEN/ CENELEC sistemomis, rengiantis CCITT (Tarptautinis konsultacinis komitetas telekomunikacijų klausimais) ir TSO (Tarptautinė standartų organizacija) veiklai šioje srityje.

Atsižvelgdamos į augantį poreikį, Jungtinės Amerikos Valstijos sparčiai didina darbų apimtis, ir paslaugų gamintojai ir teikėjai sparčiai plečia savo veiklą. Europoje, Didžiojoje Britanijoje, Prancūzijoje ir Vokietijoje panašių veiksmų buvo imtasi individualiai, tačiau bendros pastangos, palyginus su Jungtinėmis Amerikos Valstijomis, plėtojasi labai lėtai.

4.4. *Reikalavimai, galimybės ir prioritetai*

Informacinių sistemų apsaugos valdymo, operaciniai, administraciniai ir techniniai aspektai yra glaudžiai tarpusavyje susiję. Taisyklės turi atsispindėti standartuose, ir nuostatos dėl informacinių sistemų apsaugos turi patikrinamu būdu atitikti standartus ir taisykles. Atskirais aspektais taisyklėse turi būti numatytos tokios techninės charakteristikos, kurių paprastai standartai neapima, pavyzdžiui, veiklos nuostatai. Reikalavimai standartams ir veiklos nuostatams egzistuoja visose informacinių sistemų apsaugos srityse, tačiau būtina skirti apsaugos reikalavimus, sutampančius su informacinių sistemų apsaugos tikslais, ir kai kuriuos techninius reikalavimus, kuriuos galima būtų priskirti kompetentingoms Europos standartų institucijoms (CEN/ CENELEC/ ETSI).

Techninės charakteristikos ir standartai turi apimti informacinių sistemų apsaugos objektus (asmens ir įmonės patvirtinimas, neatsisakymo protokolai, teisiškai galiojantis elektroninis įrodymas, leidimų kontrolė), jų ryšių paslaugas (atvaizdo perdavimo slaptumas, balso ir informacijos perdavimo mobiliuoju ryšiu slaptumas, informacijos ir atvaizdų duomenų bazės apsauga, integruotų paslaugų apsauga), jų perdavimo ir apsaugos valdymą (kolektyviniai arba asmeniniai raktai, naudojant viešą tinklą, tinklo valdymo apsauga, paslaugos teikėjo apsauga) ir jų sertifikavimą (garantijų kriterijai ir lygmenys, apsaugos užtikrinimo procedūros apsaugotoms informacinėms sistemoms).

5. V veiklos kryptis — Informacinių sistemų apsaugos technologijų ir veiklos plėtojimas

5.1. *Esmė*

Sistemingas technologijų tyrimas ir plėtojimas, kuris leistų priimti ekonomiškai pagrįstus ir įgyvendinamus sprendimus, atitinkančius esamus ir būsimus informacinių sistemų apsaugos reikalavimus, yra esminė sąlyga paslaugų rinkos plėtotei ir viso Europos ūkio konkurencingumui.

Bet kokie informacinių sistemų apsaugos technologiniai pokyčiai turės apimti ir kompiuterių saugumo, ir kompiuterinių ryšių saugumo aspektus, nes dauguma šiuolaikinių sistemų yra perdavimo sistemos ir gali būti pasiekiamos tik ryšių paslaugų pagalba.

5.2. *Tikslas*

Sistemingas technologijų tyrimas ir plėtojimas, kuris leistų priimti ekonomiškai pagrįstus ir įgyvendinamus sprendimus, atitinkančius esamus ir būsimus informacinių sistemų apsaugos reikalavimus.

5.3. *Reikalavimai, galimybės ir prioritetai*

Su informacinių sistemų apsauga susijęs darbas turėtų apimti plėtros ir įgyvendinimo strategijas, technologijas ir integraciją bei patikrinimą.

Su tyrimais ir plėtra (R&D) susijęs strateginis darbas turėtų apimti saugių sistemų (apsaugotų nuo įsibrovimo, neteisėto modifikavimo ir užsikirtimo) teorinius modelius, funkcinius reikalavimus atitinkančius modelius, rizikos modelius ir apsaugos struktūras.

Technologijų tyrimai ir plėtra turėtų įtraukti vartotojo ir persiųstos informacijos patvirtinimo (pvz.: balso analizės ir elektroninio parašo) sistemas, technines jungtis ir kodavimo protokolus, priėjimo kontrolės mechanizmus ir pasiteisinusių saugių sistemų diegimo būdus.

Techninės sistemos saugumo tikrinimo ir tvirtinimo bei jos taikymo galimybės turėtų būti ištirtos integravimo ir tikrinimo projektais.

Be apsaugos technologijos konsolidavimo ir kūrimo būtina imtis papildomų priemonių, kurios būtų susijusios su standartų kūrimu, išlaikymu ir nuosekliu taikymu, IT ir telekomunikacinių produktų apsauginių savybių tvirtinimu ir sertifikavimu, apimant sistemų kūrimo ir įgyvendinimo būdų tvirtinimą ir sertifikavimą.

Trečioji Tyrimų, plėtros ir technologijų sistemos Bendrijos mastu programa galėtų būti naudojama kolektyviniams projektams pradiniais lygmenimis, t. y. dar neveikiant konkurencijos sąlygoms ir negaliojant normatyviniams dokumentams, skatinti.

6. VI veiklos kryptis – Informacinių sistemų apsaugos paslaugų teikimas

6.1. *Esmė*

Priklausomai nuo informacinių sistemų apsaugos savybių pobūdžio, reikalingos funkcijos turės būti įdiegtos atskirose informacinės sistemos dalyse, pavyzdžiui, terminaluose arba kompiuteriuose, paslaugose, tinklo valdymo kodavimo įrenginiuose, integroscheminėse kortelėse, kolektyviniuose ir asmeniniuose raktuose ir t. t. Kai kurios iš jų gali būti įdiegtos kompiuterinėje arba programinėje įrangoje, kurią pristato gamintojas, tuo tarpu kitos gali būti platinamos kartu su tam tikromis sistemomis (pvz., tinklo valdymo sistema), vartotojams individualiai (pvz., integroscheminėmis kortelėmis) arba specialios paskirties organizacijos pastangomis (pvz., kolektyviniais arba asmeniniais raktais).

Daugumą apsaugos produktų ir paslaugų gali teikti patys gamintojai, paslaugų teikėjai arba operatoriai. Specifinėms funkcijoms vykdyti (pvz., išduoti kolektyvinius arba asmeninius raktus, audito įgaliojimus) gali prireikti įvardyti ir įgalioti atitinkamas organizacijas.

Tas pats taikytina, kai paslaugų kokybę sertifikuoti, vertinti ir tikrinti turi nuo gamintojų, paslaugų teikėjų ir operatorių interesų nepriklausomos organizacijos. Šios organizacijos gali būti privačios, valstybinės arba valstybės įgaliotos vykdyti pavestas funkcijas.

6.2. *Tikslas*

Norint palengvinti informacinių sistemų apsaugos vieningą kūrimą Bendrijoje, saugant ir visuomeninius, ir verslo interesus, reikės sukurti nuoseklų požiūrį apsaugos teikimo atžvilgiu. Jeigu bus įgaliojamos nepriklausomos organizacijos, jų funkcijas ir įgaliojimo sąlygas reikės apibrėžti ir suderinti, o prireikus ir įtraukti į taisykles. Tokiu būdu būtų siekiama Bendrijos lygiu susitarti dėl aiškiai apibrėžtos ir tarp įvairių šios rinkos veikėjų padalintos atsakomybės, kuri būtų abipusio pripažinimo išankstinė sąlyga.

6.3. *Statusas ir tendencijos*

Šiuo metu informacinių sistemų apsauga yra deramai organizuota tik atskirose srityse ir yra sukurta tenkinti tik tos srities poreikius. Visos Europos mastu apsauga teikiama neformaliai, ir tikrinimo bei sertifikavimo procedūrų abipusis pripažinimas kol kas neperžengia uždarų grupių ribų. Dėl augančios informacinių sistemų apsaugos svarbos poreikis apibrėžti nuoseklų požiūrį informacinių sistemų apsaugos teikimo Europoje atžvilgiu ir tarptautiniu mastu tampa ypatingai skubus.

6.4. *Reikalavimai, galimybės ir prioritetai*

Dėl veikiančiųjų asmenų skaičiaus ir glaudžių sąsajų su valdymo ir įstatyminėmis problemomis ypač svarbu iš anksto susitarti dėl informacinių sistemų apsaugos teikimo principų.

Vystant nuoseklų požiūrį šiuo klausimu, bus būtina atsižvelgti į funkcijų, savaime reikalaujančių nepriklausomų (arba bendrai dirbančių) organizacijų dalyvavimo, nustatymo ir jų techninių charakteristikų sudarymo aspektus. Viena tokių funkcijų – tai kolektyvinių arba asmeninių raktų tvarkymas.

Be to, reikia kuo anksčiau nustatyti funkcijas ir apibrėžti, kurias visuomenės interesų labui reikėtų patikėti nepriklausomoms (arba bendrai dirbančioms) organizacijoms. Tokios funkcijos galėtų apimti auditą, kokybės užtikrinimą, tikrinimą, sertifikavimą ir kitas panašias funkcijas.