NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

25. november 2020

DOKUMENT
AC/35-D/2001-REV3

JULGEOLEKUKOMITEE

FÜÜSILISE JULGEOLEKU DIREKTIIV

Eesistuja kohusetäitja märkus

1. Käesoleva dokumendi lisas avaldatakse kolmas redaktsioon normdokumendi C-M(2002)49-REV1 „Turvalisus Põhja-Atlandi lepingu organisatsioonis“ täiendavast füüsilise julgeoleku direktiivist. Redaktsioon on olemuselt siduv ja kohustuslik. Käesolev dokument asendab dokumendi AC/35-D/2001-REV2, mis kuulub hävitamisele.

2. Käesolev redaktsioon kajastab NATO Security Policy tervikliku läbivaatuse AC/35-N(2015)0025-AS1, vastu võetud 21. detsembril 2015) tulemusi.

3. Käesoleva normdokumendi on heaks kiitnud julgeolekukomitee (AC/35-N(2020)0004-AS1, vastu võetud 4. novembril 2020) ning dokumendile rakendatakse korralist ülevaatamist.

(Allkiri) Marco Criscuolo

Lisasid: 1

nõunik: R. Grumberg, NOS
(sisetel. 9182)
Algteksti keel: Inglise

FÜÜSILISE JULGEOLEKU DIREKTIIV
SISUKORD

FÜÜSILISE JULGEOLEKU DIREKTIIV

SISSEJUHATUS

1. Julgeolekukomitee (AC/35) avaldab käesoleva füüsilise julgeoleku direktiivi NATO Security Policy (dokument C-M(2002)49) lisa D täiendusena. Käesolev direktiiv sisaldab kohustuslikke sätteid ja samuti nimetatud sätteid selgitavat teavet. Direktiivi käsitleb järgnevaid küsimusi:

a) aluspõhimõtted;

b) füüsilise julgeoleku üldised nõuded;

c) konkreetsed füüsilise julgeoleku meetmed;

d) NATO salastatud teabe säilitamisnõuded;

e) side- ja infosüsteemide füüsiline kaitse ja

f) kaitse tehniliste rünnakute vastu.

ALUSPÕHIMÕTTED

2. Territoorium, hooned, kontorid, ruumid ja teised alad, kus NATO salastatud teavet säilitatakse, käideldakse ja/või arutatakse, peavad olema kaitstud asjakohaste füüsilise julgeoleku meetmetega. Vajalike füüsilise julgeoleku meetmete üle otsustamisel tuleb võtta arvesse kõiki asjassepuutuvaid tegureid, sealhulgas:

a) teabe salastatuse tase ja liik;

b) säilitatava ja/või käideldava salastatud teabe kogus ja vorm (paberkandjal ja/või elektrooniline);

c) läbipääsukontroll ja teadmisvajaduse põhimõtte jõustamine;

d) vaenulikest luureteenistustest lähtuv oht NATO ja/või NATO liikmesriikide vastu ja kohalikul tasandil hinnatud terrorismi, spionaaži, õõnestustegevuse, sabotaaži ja (organiseeritud) kuritegevuse oht ja

e) salastatud teabe säilitamise viis (näiteks paberkandjal või elektrooniliselt või krüpteeritult).

3. Füüsilise julgeoleku meetmed kavandatakse, et:

a) tõkestada varjatud või jõuga sissetungi;

b) heidutada, takistada ja avastada sisemistest ohtudest tulenevaid tegevusi;

c) võimaldada töötajate eristamist NATO salastatud teabele juurdepääsu andmisel nende juurdepääsuloa (PSC) taseme ja teadmisvajaduse alusel ja

d) avastada turvaintsidente ja reageerida neile niipea kui võimalik.

4. Riigi julgeoleku volitatud esindajad (inglise keeles *National Security Authorities* (NSA)) / volitatud julgeolekuasutused (inglise keeles *Designated Security Authorities*) ja muud pädevad julgeolekuasutused ning NATO tsiviil- ja sõjalised organid vastutavad julgeoleku tagamise kavade koostamise eest viisil, mis väldib ohuolukorras NATO salastatud teabe sattumist volitamata või vaenulikesse kätesse. Kavad peavad sisaldama salastatud teabe ohuolukorras evakueerimist ja/või hävitamist. Minimaalselt peab kava sisaldama:

a) konkreetsete ohuolukordade kirjeldusi, mille puhul salastatud teave evakueeritakse ja/või hävitatakse;

b) ohuolukorras evakueerimise/hävitamise protseduure, milles määratakse täideviimise algatamise eest vastutavad isikud (peamine ja asendaja);

c) sidepidamismeetodeid;

d) hävitamisseadmeid või evakueerimismeetodeid;

e) kindlaksmääratud alternatiivseid evakueerimiseks mõeldud säilituskohti ja

f) ohuolukorras hävitatavate või evakueeritavate esemete prioritiseerimist.

ÜLDISED FÜÜSILISE JULGEOLEKU NÕUDED

5. Füüsilised meetmed on ainult üks osa kaitsemeetmetest ja seda toetatakse usaldusväärse personali julgeoleku ja teabe julgeoleku ning side- ja infosüsteemide turvalisuse meetmetega, mille üksikasjad on toodud dokumendi C-M(2002)49 lisades C, E ja F, samuti neid täiendavates direktiivides. Julgeolekuriskide mõistlik juhtimine hõlmab proportsionaalsete, tõhusate ja kulutõhusate meetodite kehtestamist ohtudega võitlemiseks ja haavatavuste kompenseerimiseks nende valdkondade kaitsemeetmete kombineerimise abil. Tõhusus ja kulutõhusus saavutatakse, määratledes füüsilise julgeoleku nõuded rajatiste planeerimise ja kavandamise osana ning konsulteerides julgeolekuasutustega, vähendades seeläbi vajadust kulukate renoveerimistööde järele.

6. Füüsilise julgeoleku programmid põhinevad „sügavuti kaitse“ põhimõttel, mis koosneb asjakohaste füüsilise julgeoleku meetmete kombinatsioonist, tagades kaitsetaseme, mis vastab organisatsiooni ja selle teabe kriitilisuse ja haavatavusele. Kuigi füüsilise julgeoleku meetmed on asukohaspetsiifilised ja sõltuvad mitmetest teguritest (näiteks kohaliku tasandi oht, hoone struktuur ja arhitektuur, keskkonnakaalutlused, asukoht), kohaldatakse järgmiseid põhimõtteid:

a) esmalt on vajalik tuvastada kaitset vajav vara. Seejärel luuakse mitmekihilised julgeoleku meetmed, mis tagavad sügavuti kaitse ja ründaja viivituse;

b) esimese kihi füüsilise turvalisuse meetmetega piiritletakse kaitstud ala ja heidutatakse loata sissetungijat;

c) järgmise kihi meetmetega avastatakse loata sissetungimised või selle katsed ning hoiatatakse valvemeeskonda;

d) sisemine meetmete kiht takistab sissetungijaid nii kaua, kuni valvemeeskond suudab nad kinni pidada. Seega on valvemeeskonna reageerimisaeg ja sissetungijate takistamiseks kavandatud füüsilise julgeoleku meetmed omavahelises seoses.

7. Füüsilist julgeolekut tagavat varustust (näiteks videovalvesüsteem, valveseadmestik, seifid/turvakapid) peab regulaarselt hooldama, et tagada selle optimaalne toimimine. Samuti on vajalik perioodiliselt hinnata nii üksikute julgeolekumeetmete kui ka kogu julgeolekusüsteemi tõhusust. See on eriti oluline, kui objekti kasutusotstarbes või julgeolekusüsteemi konkreetsetes elementides on toimunud muutus. Selleks harjutatakse regulaarselt intsidentidele reageerimise kavasid (tavatingimustes kord aastas).

8. Kohalik julgeolekut korraldav teenistuja peab hoolikalt hindama salvestamist ja/või edastamist võimaldavate elektrooniliste süsteemide või mobiilsete seadmete (näiteks mobiiltelefonid, nutitelefonid ja/või -kellad, tahvelarvutid, sülearvutid, esemevõrku kasutavad seadmed (IoT)) lubamist aladele, kus säilitatakse, töödeldakse või arutatakse NATO salastatud teavet. NATO valdustes mobiilsete seadmete kasutamise lisadokumenti (AC/35-D/1042, *Supporting Document on the Use of Mobile Devices on NATO Premises*) on võimalik kasutada mobiilseid seadmeid puudutavate kohalike julgeolekumeetmete ja regulatsioonide väljatöötamiseks.

Turvaalad

9. Turvaalad on alad, millel säilitatakse, käideldakse või arutatakse NATO CONFIDENTIAL (NC) või kõrgemal tasemel salastatud teavet. Järgmised lõiked kohalduvad võrdselt nii alalistele kui ajutistele turvaaladele. Sellised alad peavad olema korraldatud ja struktureeritud nii, et need vastaksid ühele järgmistest nõuetest:

a) NATO klass I turvaala: eriti tundlik ala, kus NC ja kõrgemal tasemel salastatud teavet säilitatakse, käideldakse või arutatakse sellisel viisil, et sisenemine alale tähendab põhimõtteliselt juurdepääsu NATO salastatud teabele ja seega tähendaks volitamata sissepääs turvanõuete rikkumist. Selliste alade hulka võivad kuuluda operatsioonide juhtimise ruumid, serveriruumid või arhiivihoidlad ja nende puhul on nõutav:

   i. selgelt määratletud ja kaitstud perimeeter, mille abil kontrollitakse kõiki sisenemisi ja väljumisi;

   ii. sissepääsukontrollisüsteem, mille alusel saavad läbipääsu vaid isikud, kellel on nõuetekohane ja spetsiaalse volitusega[1] õigus alale sisenemiseks;

   iii. alal tavapäraselt säilitatava teabe, see tähendab teabe, millele alale sisenedes juurdepääs saadakse, salastatuse taseme ja kategooria (näiteks ATOMAL, BOHEMIA) määramine; ja

   iv. selge viide sellele, et alale sisenemiseks on nõutav kohaliku julgeolekut korraldava teenistuja luba. Viites võib olla näidatud asjassepuutuv salastatuse tase ja/või ala tundlikkus;

b) NATO klass II turvaala: ala, kus NC ja kõrgemal tasemel salastatud teavet säilitatakse, töödeldakse või arutatakse sellisel viisil, et seda on võimalik kaitsta volitamata isikute juurdepääsu eest, kasutades alasiseselt kehtestatud kontrollimehhanisme. Selliste alade hulka võivad kuuluda kontorid või koosolekuruumid, kus NATO salastatud teavet säilitatakse, käideldakse või arutatakse. Nende alade puhul on nõutav:

   i. selgelt määratletud ja kaitstud perimeeter, mille abil kontrollitakse kõiki

[1] Spetsiaalne volitus on personalil, kellel on formaalselt tuvastatud teadmisvajadus, kelle juurdepääs põhineb nende töökohustuste iseloomul ning kes on sissepääsukontrolli nimekirjas, samuti isikud, keda on eraldi korraldusega (*ad hoc)* volitanud asjassepuutuva organisatsiooni juht konkreetse rolli või kohustuse täitmiseks.

sisenemisi ja väljumisi;

ii. sissepääsukontrollisüsteem, mis võimaldab saatjata läbipääsu vaid isikutele, kes on läbinud julgeolekukontrolli ja kes on volitatud alale sisenema; ja

iii. isikutele, kes ei vasta eespool punkti b alapunktis ii toodud kriteeriumitele, tuleb rakendada isiku saatmine või võrdväärne kontrollimehhanism, et ära hoida nende volitamata juurdepääs NATO salastatud teabele ja kontrollimatu sissepääs aladele, millele on spetsiaalselt määratud kaitse tehniliste rünnakute, tahtliku ja tahtmatu pealtkuulamise eest.

10. Kõiki turvaalasid (näiteks kontoreid, koosolekuruume ja -saale, tehniliselt turvalisi turvaalasid, jne), kus arutatakse NATO salastatud teavet, hinnatakse perioodiliselt pealtkuulamise riski suhtes. Kui asjassepuutuv julgeolekuasutus teeb kindlaks niisuguste riskide olemasolu, tuleb salastatud teabe arutelud keelata või rakendada kohaseid protseduurilisi maandamismeetmeid (näiteks määratleda koosolekuruumid, mis on ette nähtud salastatud teabe üle arutlemiseks) või tehnilisi maandamismeetmeid (näiteks seinte, uste ja lagede heliisolatsioon, heli summutamise süsteemide paigaldamine, vms).

11. Turvaalasid, kus töötajad ei viibi ööpäevaringselt, kontrollitakse viivitamatult pärast tavapärase tööpäeva lõppu kindlustamaks, et need on nõuetekohaselt turvatud, välja arvatud juhul kui selleks otstarbeks kasutatav valveseadmestik on aktiveeritud.

12. Koosseisulise personali klass I või klass II turvaalale sissepääs peab olema kontrollitud asjakohase läbipääsusüsteemiga (näiteks lubade või isikutuvastuse süsteem).

Administratiivala

13. NATO klass I või klass II turvaala ümber või ette kehtestatakse administratiivala. Administratiivalal võib säilitada, käidelda või arutada ainult NATO RESTRICTED (NR) tasemel salastatud teavet. Sellisel alal peab olema nähtavalt määratletud perimeeter, mille piires on võimalik isikuid ja sõidukeid kontrollida. Isikute saatmine ei ole nõutav.

Tehniliselt turvalised turvaalad

14. Nii alalised kui ajutised tehniliselt turvalised turvaalad on alad, mis vajavad kaitset tehniliste rünnakute ja tahtliku pealtkuulamise eest.

15. Tehniliselt turvalistele turvaaladele korraldatakse regulaarselt füüsilisi ja tehnilisi[2] julgeoleku kontrolle ning nendesse sissepääs on rangelt kontrollitud. Tehniliste rünnakute ja pealtkuulamise eest kaitsmiseks kohaldatakse järgmiseid meetmeid:

a) asjakohase tasemega füüsilised ja tehnilised julgeolekumeetmed, et jõustada riskipõhiseid läbipääsukontrolle. Riski kindlaksmääramise kohustust jagavad vastavad tehnilised eksperdid ja julgeolekuasutus, kes nõustavad riski omanikku otsuse tegemisel / heakskiidu andmisel;

[2] Tehniline julgeoleku kontroll on ala kontrollimine, et kindlaks määrata, kas seal on potentsiaalselt teabe kogumise seadmeid (mikrofonid, kaamerad, jne) või side pealtkuulamise seadmeid.

b) kui sellised alad pole kasutusel, peavad need olema lukustatud ja/või valve all, ja kõiki võtmeid koheldakse turvavõtmetena[3]. Kooskõlas vastava julgeolekuasutuse nõuetega korraldatakse nendel aladel regulaarseid füüsilisi ja/või tehnilisi julgeolekukontrolle. Nimetatud kontrolle tuleb teha ka pärast igakordset alale volitamata sisenemist või selle kahtlustamisel, samuti pärast igasuguse välise personali sisenemist (näiteks hooldustööde või remondi eesmärgil);

c) sellistele aladele ei lubata ühtki eset, mööblit ega seadet enne, kui vastava väljaõppe saanud julgeolekut korraldav teenistuja on selle põhjalikult läbi vaadanud pealtkuulamisseadmete leidmiseks. Aladele toimetatud ja sealt väljaviidavate esemete, mööbli ja seademete kohta peetakse arvestust;

d) salvestus- ja/või edastamisvõimelised elektroonilised süsteemid ja/või mobiilseadmed (näiteks mobiiltelefonid, nutitelefonid ja/või -kellad, tahvelarvutid, sülearvutid, esemevõrku kasutavad seadmed (IoT)) on keelatud;

e) tavapäraselt ei paigaldata neile aladele telefone ja muid videokonverentsiseadmeid. Kui nende paigaldamine on vältimatu, siis ühendatakse need salastatud arutelude toimumise ajaks füüsiliselt lahti. See ei kehti nõuetekohaselt paigaldatud ja heakskiidetud sidevahendite puhul (näiteks salastatud telefoniliinid, videokonverentsitehnika).

KONKREETSED FÜÜSILISE JULGEOLEKU MEETMED

16. Selles osas antakse teavet erinevate konkreetsete füüsiliste (näiteks perimeeter, uksed, lukud) ja tehniliste (näiteks valveseadmestik, videovalvesüsteem) julgeolekumeetmete ja protseduuride (näiteks külastajate kontroll, võtmete kontroll, kontoriruumide eraldamine) ning selle kohta, kuidas need panustavad organisatsiooni või objekti julgeolekuraamistikku.

Perimeeter

17. Perimeeter moodustab füüsilise barjääri ja määratleb ala, mille turvalisus vajab kaitset.

18. Perimeetrit kasutatakse:

a) alale tahtmatult sisenemise tõkestamisel füüsilise ja psühholoogilise heidutuse loomiseks;

b) varjamatult või varjatult volitamata sisenemise tõkestamiseks;

c) alale sissetungimisel viivituse tekitamiseks, et anda valvuritele või valvemeeskonnale aega reageerida; ja

d) tuvastus- ja kontrolliprotseduuride hõlbustamiseks, suunates volitatud isikute ja sõidukite voo läbi kindlaksmääratud sissepääsude.

[3] Turvavõtmed on võtmed, mis sobituvad järgmistele esemetele paigaldatud lukkudega: salastatud teabe säilitamiseks mõeldud seifid/turvakapid; turvaala ruumid või turvaalad; turvaala ruumid, kus on tehtud tehniline julgeoleku kontroll; seifid/turvakapid, mida kasutatakse salastatud dokumentide ringluseks. Turvavõtmeid käideldakse ja kaitstakse samamoodi nagu salastatud teavet, millele need juurdepääsu annavad.

19. Perimeetril paikneva piirdeaia pakutav kaitsetase oleneb selle konstruktsioonist, ehitusmaterjalist, kõrgusest, vundamendi tüübist ja sügavusest ning täiendavatest turvaelementidest, mida kasutatakse selle jõudluse ja tõhususe parandamiseks (näiteks ülaosas ronimistõke, perimeetri valveseadmestik, valgustus, videovalvesüsteem). Mõnedel hoonetel ei ole piirdeaeda, kuid neil võivad olla muud tõkked ja taristu, mis toimivad füüsilise tõkkena.

20. Perimeetril paiknev tõke tekitab otsusekindla sissetungija tegevuses üksnes lühikese viivituse ja seda peaks seega täiendama valveseadmestiku, videovalvesüsteemi, turvavalgustuse ja perioodilise, aga juhusliku intervalliga ringkäikudega, mida sooritavad vastava väljaõppega valvurid või valvemeeskond.

21. Perimeetri tõhusus sõltub samuti sissepääsude turvalisuse tasemest. Seega peavad väravad olema ehitatud, lähtudes samadest turvalisuse standarditest, mis perimeetri puhul ja toimima peab teatud vormis läbipääsukontroll.

Valveseadmestik

22. Perimeetri valveseadmestikku võib kasutada piirdeaia turvalisuse taseme täiendamiseks. Perimeetri valveseadmestiku võib paigaldada varjatult (kuigi seda tehakse tavapäraselt esteetilistel põhjustel) või nähtavate seadmetena, et neil oleks heidutav toime. Perimeetri valveseadmestik on aldis valehäiretele ja seega tuleb seda tavapäraselt kasutada ainult koos häireteate kontrolli süsteemiga, nagu näiteks videovalvesüsteemiga.

23. Sügavuti kaitse põhimõtte kohaselt võib valveseadmestikku kasutada ruumides ja hoonetes valvurite asemel või nende abistamiseks. Et valveseadmestik oleks tõhusus, peaks lisaks olema reageerimisüksus, mis reageerib alates häire aktiveerimisest mõistliku aja jooksul.

Läbipääsukontroll

24. Läbipääsukontroll hõlmab sissepääsulubade ja isikutuvastuse süsteemi, sealhulgas teenusepakkujate ja külastajate kontrollimise ja saatmise korda.

25. Läbipääsukontrolli võib rakendada objektile, hoonele või objektil olevatele hoonetele või aladele, tsoonidele või ruumidele hoones sees. Kontrollimehhanism võib olla elektrooniline, elektromehaaniline või füüsiline. Samuti võib seda kontrolli teostada valvur või vastuvõtutöötaja. Klass I või klass II turvaalale sissepääsu kontrollitakse sissepääsulubade või isikutuvastuse süsteemi alusel, mis kehtib koosseisulise personali suhtes.

26. Kui asutuses on kehtestatud sissepääsulubade süsteem, peab luba kandma kogu aeg nähtaval kohal, et võimaldada äratundmise ja isikusamasuse tuvastamist.

Kontoriruumide eraldamine

27. Selleks, et ära hoida NATO salastatud teabele kas füüsilise juurdepääsu või jälgimise abil volitamata isikute juurdepääs, võetakse kasutusele asjakohaseid meetmeid. Arvesse võetakse tegureid nagu alal töötavate või alale sissepääsu omavate töötajate arv, akende paiknemine ja võimalus väljast ruumi sisemust vaadelda, samuti valgustustingimusi (päevavalgus, kunstlik valgus). Samuti rakendatakse ettevaatusabinõusid tahtmatu ja tahtliku pealtkuulamise vastu.

Valvurid

28. Valvurite kaasamine võib pakkuda väärtuslikku heidutust isikute vastu, kes võivad plaanida varjatud sissetungi. Valvurite kohustuste ja ringkäikude sageduse üle otsustatakse riskitaseme ja teiste olemasolevate turvasüsteemide või varustuse põhjal. Valvuritele antakse piisavad kirjalikud juhised, et tagada konkreetselt määratud ülesannete nõuetekohane täitmine. Valvuritele on vaja sidevahendeid juhtimiskeskusega suhtlemiseks.

29. Kui valvureid kasutatakse turvaalade ja NATO salastatud teabe terviklikkuse tagamiseks, peavad nad olema läbinud asjakohase julgeolekukontrolli, kvalifitseeritud väljaõppe ja neile peab olema rakendatud järelevalve.

30. Kui objektil toimub turvaintsident, on reageerimisüksus kohustatud reageerima. Reageerimisüksus koosneb vastava julgeolekuasutuse poolt kindlaksmääratud arvust vajalikust valvepersonalist (tavapäraselt vähemalt kaks valvurit). Mis tahes reageerimine intsidendile ei tohi kahjustada või nõrgestada kaitset mujal objektil. Valvemeeskonna reageerimist häireteadetele või hädaolukorra signaalidele katsetatakse ja see peab mahtuma ajalimiiti, mis on hinnanguliselt piisav NATO salastatud teabele sissetungijale juurdepääsu ära hoidmiseks.

Videovalvesüsteem

31. Videovalvesüsteemi kasutamine on valvuritele väärtuslik abivahend intsidentide ja valveseadmestiku häireteadete tuvastamisel suurtel objektidel või suurte perimeetrite puhul. Süsteemi tõhusus sõltub aga sobiliku varustuse valimisest ja paigaldamisest ning valitud süsteemi jälgimisest juhtimiskeskuses. Parima videovalvesüsteemi komponentide valikul, näiteks kaamerate tehniliste omaduste, kaamerate paigaldamise asukohtade, videovalvesüsteemi ülekatvuse ja videovalvesüsteemi juhtimiskeskuse jälgimissektsiooni monitoride paigutuse ja ergonoomika asjus konsulteeritakse ekspertidega. Heli ja pildi salvestamine videovalvesüsteemis ei tohi ohustada NATO salastatud teavet jälgimisriski tõttu.

Turvavalgustus

32. Lisaks sellele, et turvavalgustus tekitab valgust, mis on vajalik valvurile tõhusaks jälgimiseks kas otseselt või videovalvesüsteemi kaudu, võib sellel olla ka äärmiselt heidutav mõju võimalikele sissetungijatele. Valgustusstandard peab vastama vähemalt videovalvesüsteemi miinimumnõuetele ja see tuleb paigaldada objekti tingimustega sobival viisil.

Seifid/turvakapid ja kontorimööbel

33. Seifid/turvakapid ja kontorimööbel, mida kasutatakse NATO salastatud teabe säilitamiseks, on sügavuti kaitse viimane kaitseliin turvalisuse tagamiseks. Nende ajalise viivituse tagamise võimekust hinnatakse igakülgsete katsetega, et teha kindlaks nende vastupidavus avastamata sissepääsukatsetele ja sellistele rünnaku vormidele, mida nende suhtes tõenäoliselt rakendada võidakse. Kõnealune varustus peab saama kohase heakskiidu, mis vastab selles säilitatavale salastatud teabe tasemele (nagu on sätestatud direktiivi lõigetes 50–54). NATO salastatud teabe säilitamise jaoks varustuse valimisel tuleb arvesse võtta järgmisi kriteeriume:

a) julgeolekuoht alal, kus teavet säilitatakse;

b) säilitatava teabe salastatuse tase;

c) seifi/turvakapi või mööblieseme ning selle luku poolt tagatava kaitse tase;

d) seifi/turvakapi või mööblieseme paiknemise keskkonna kaitseks rakendatavate lisakaitsemeetmete kombinatsioon.

Lukud

34. Luku ja võtme süsteemid valitakse niisugused, mis tagavad võrdväärse kaitse läbipääsukontrolli tasemega, sobituvad kaitstava teabega ning konstruktsioonitüübi ja materjaliga, millesse need paigaldatakse.

35. Mehaanilised lukusilindrid peavad pakkuma kaitset luku muukimise (*key bumping*), füüsilise rünnaku (näiteks puurimine, peitliga löömise, väänamise, väljatõmbamise) ja võtme volitamata kopeerimise eest. Objekti võtmehaldussüsteemides peab olema mõistlik arv peavõtmete rühmi. Välitingimustes kasutatavad lukud valitakse kohalikku keskkonda arvesse võttes piisava korrosioonikindlusega.

36. Elektroonilised lukud peavad pakkuma piisavat kaitset elektrooniliste võtmete (magnetriba, kiip, token) volitamata kopeerimise eest ning neil peavad olema aktiivsed näidikud, mis annavad märku aku tühjenemisest ja süsteemiriketest. Objekti elektrooniliste võtmete haldussüsteemis peab olema piiratud arv elektroonilisi peavõtmeid, mis tagavad juurdepääsu paljudele elektroonilistele lukkudele ning elektrooniliste võtmete kehtivusaeg peab olema piiratud. Elektroonilised lukud peavad salvestama elektroonilise võtmeluku läbipääsuõiguste logi.

Võtmete ja koodide kontroll

37. Seifide/turvakappide võtmeid ei tohi objektilt välja viia. Üldreeglina ei tohi seifi/turvakapi võtmeid välja viia kontorihoonest, kus seif/turvakapp paikneb. Isik, kes peab seife/turvakappe avama ning valveseadmestiku sisse- ja välja lülitama, peab neid koode peast teadma. Koode tohib teada väikseim võimalik arv isikuid. Koode peab muutma vähemalt siis:

a) kui need esimest korda kasutusele võetakse;

b) kui muutub personal, kelle valduses koodid on;

c) kui on põhjust arvata, et kood on saanud teatavaks kõrvalistele isikutele ja

d) vähemalt iga 12 kuu tagant, välja arvatud juhul, kui asjaomane julgeolekuasutus annab riskihinnangu alusel teistsugused juhised.

38. Ohuolukorras kasutatavaid varuvõtmeid ja iga varukoodi kirjalikku üleskirjutust hoitakse kohaliku julgeolekut korraldava teenistuja juures pitseeritud läbipaistmatus ümbrikus.

39. Kasutusel olevaid ja varuvõtmeid hoitakse eraldi kappides. Iga varukoodi hoitakse eraldi ümbrikus.

40. Võtmeid, koode ja ümbrikke kaitstakse samaväärselt kui teavet, millele need juurdepääsu annavad.

Heakskiidetud varustus

41. Klass I ja klass II turvaaladele ehitatud turvakambrite ja avatud hoiualade, kus säilitatakse NC ja kõrgemal tasemel salastatud teavet avariiulitel või nähtaval kohal (näiteks skeemidel, kaartidel) seinad, põrandad ja uksed peab heaks kiitma vastav julgeolekuasutus.

42. NATO liikmesriigid kasutavad üksnes seda varustust, mille vastav julgeolekuasutus on NATO salastatud teabe kaitsmiseks heaks kiitnud.

43. NATO tsiviil- ja sõjalised organid tagavad, et soetatud varustus on mõnes NATO liikmesriikidest sarnastes tingimustes kasutamiseks heakskiidetud. NATO tsiviil- ja sõjalised organid võivad samuti soetada varustust, mille on kasutamiseks heaks kiitnud vastav julgeolekuasutus täieliku riskianalüüsi põhjal, mille kohaselt tuleb tuvastatud riski (riske) vähendada või leevendada.

Külastajate kontroll

44. Kehtestada tuleb asjakohane külastajate kontrollisüsteem, et määratleda, kas külastajal on lubatud siseneda objektile, hoonesse või alale, kus säilitatakse, töödeldakse ja/või arutatakse NATO salastatud teavet.

45. Ametlikest külastustest teavitab tavapäraselt ette külastaja lähetajaorganisatsioon. Ametlik teade sisaldab vähemalt isikut tõendava dokumendi, näiteks passi või isikutunnistuse kirjeldust.

46. Külastajad võivad liikuda kas saatjaga või saatjata, kuid külastajate üle peab säilima asjakohase tasemega kontroll, nagu on sätestatud järgmises lõikes.

47. Külastajate kontrolli kord võib varieeruda olenevalt kohalikest julgeolekunõuetest. Igal juhul kehtivad saatjaga või saatjata külastajatele järgmised miinimumnõuded:

a) saatjaga:
külastajaid saadab kogu aeg asjakohasel tasemel juurdepääsuluba (PSC) omav teenistuja või valvur. Neilt võib nõuda sellise külastusloa kandmist, mille alusel on võimalik tuvastada, et tegu on külastajaga. Külastajate täielikud andmed tuleb registreerida.

b) saatjata:
isikud, kellel on asjakohane juurdepääsuluba (PSC) ja teadmisvajadus, võivad saada alale või selle osadele ajutiselt saatjata sissepääsu. Neilt nõutakse siiski sellise loa kandmist, mille alusel on võimalik tuvastada, et tegu on külastajaga ja nad on kohustatud tagastama ajutise loa niipea, kui nad on organisatsioonis tegevuse lõpetanud. Külastajate täielikud andmed, sealhulgas sisenemise ja väljumise aeg, tuleb registreerida. Saatjata külastajatel ei ole lubatud teisi külalisi saata.

Läbiotsimine sisenemisel ja väljumisel

48. Objektidel või hoonetes, kus NATO teavet säilitatakse või käideldakse, võib korraldada sisenemisel ja väljumisel pistelisi läbiotsimisi, mille eesmärk on tõkestada volitamata materjalide sissetoomist või salastatud või salastamata materjali volitamata kaasavõtmist.

49. Sisenemisel ja väljumisel läbiotsimise võib seada objektile või hoonesse sisenemise eeltingimuseks. Nähtavale kohale paigutatakse hoiatussilt sisenemisel ja väljumisel toimuda võivate pisteliste läbiotsimiste kohta.

NATO SALASTATUD TEABE SÄILITAMISE MIINIMUMSTANDARDID

50. NATO salastatud teavet säilitatakse aladel, seifides/turvakappides ja/või kontorimööblis, mis on kavandatud teabele volitamata juurdepääsu tõkestama ja tuvastama.

51. COSMIC TOP SECRET (CTS)

CTS tasemel salastatud teavet säilitatakse klass I või klass II turvaalal nii, et täidetud on üks järgnevatest tingimustest:

a) heakskiidetud seifis/turvakapis, millel on üks järgnevatest lisakontrollimehhanismidest:

i. juurdepääsuõigusega valvuri või vahetuses töötava personali pideva kaitse all;

ii. seifi/turvakappi kontrollib vähemalt iga kahe tunni tagant juhuslike ajavahemike järel kas juurdepääsuõigusega valvur või vahetuses töötav personal; või

iii. heakskiidetud valveseadmestik kombineerituna reageerimisüksusega, mis saabub pärast häire teavitust asukohta hinnanguliselt ajavahemiku jooksul, mis kuluks seifi/turvakapi eemaldamiseks või lahti murdmiseks või kehtestatud füüsiliste julgeoleku meetmete ületamiseks.

b) direktiivi liite 1 kohaselt ehitatud avatud hoiualal, millel on heakskiidetud valveseadmestik kombineerituna reageerimisüksusega, mis saabub asukohta pärast häire teavitust sissetungiks kuluva hinnangulise ajavahemiku jooksul; või

c) valveseadmestikuga turvakambris, kombineerituna reageerimisüksusega, mis saabub asukohta pärast häire teavitust sissetungiks kuluva hinnangulise ajavahemiku jooksul.

52. NATO SECRET (NS)

NS tasemel salastatud teavet säilitatakse klass I või klass II turvaalal nii, et täidetud on üks järgnevatest tingimustest:

a) samamoodi, nagu on ette nähtud CTS tasemel salastatud teabe puhul;

b) heakskiidetud seifis/turvakapis või turvakambris, ilma täiendavate kontrollimeetmeteta; või

c) avatud hoiualal, mille puhul on nõutud üks järgnevatest täiendavatest kontrollimeetmetest:

i. asukoht, kus avatud hoiuala paikneb, peab olema juurdepääsuõigusega valvuri või vahetuses töötava personali pideva kaitse all;

ii. juurdepääsuõigusega valvur või vahetuses töötav personal peab avatud hoiuala kontrollima vähemalt kord iga nelja tunni jooksul; või

iii. valveseadmestik kombineerituna reageerimisüksusega, mis saabub asukohta pärast häire teavitust sissetungiks kuluva hinnangulise ajavahemiku jooksul.

53. NATO CONFIDENTIAL (NC)

NC tasemel salastatud teavet säilitatakse klass I või klass II turvaalal heakskiidetud seifis/turvakapis.

54. NATO RESTRICTED (NR)

NR tasemel salastatud teavet säilitatakse lukustatud kapis või kontorimööblis (näiteks töölaua sahtlis) administratiivalal, klass I või klass II turvaalal. NR tasemel salastatud teavet võib säilitada ka lukustatud kapis, turvakambris või avatud hoiualal, mis on heaks kiidetud NC või kõrgemal tasemel salastatud teabe säilitamiseks.

SIDE- JA INFOSÜSTEEMIDE FÜÜSILINE KAITSE

55. Aladele, kus kuvatakse või käideldakse infotehnoloogia abil NATO salastatud teavet või kus sellisele teabele on potentsiaalselt võimalik juurde pääseda, luuakse reeglistik, mis tagab konfidentsiaalsuse, terviklikkuse ja käideldavuse.

56. Alad, kus side- ja infosüsteemide abil kuvatakse, säilitatakse, töödeldakse või edastatakse NC ja kõrgemal tasemel salastatud teavet või kus sellisele teabele on potentsiaalselt võimalik juurde pääseda, peavad olema NATO klass I või klass II turvaalad või nende riigisisene vaste.

57. Alad, kus side- ja infosüsteemide abil kuvatakse, säilitatakse, töödeldakse või edastatakse NR tasemel salastatud teavet või kus sellisele teabele on potentsiaalselt võimalik juurde pääseda, võivad olla administratiivalad.

58. Juurdepääsu aladele, kuhu on paigutatud kriitilise tähtsusega side- ja infosüsteemide elemendid (serverid, võrgu-, varundamise- ja krüptoseadmed) või kus neid hallatakse, kontrollitakse eesmärgipäraselt ja neile juurdepääs on ainult volitatud personalil, kes on seotud julgeolekuga ja süsteemi/võrgu/krüpto administreerimisega.

59. Side- ja infosüsteemidele, millega käideldakse NATO salastatud teavet, kasutatakse asjakohase kaitsetaseme määramiseks dokumendi C-M(2002)49 lisasid E–F ja seda täiendavaid direktiive.

Printerite, koopiamasinate ja purustajate füüsiline kaitse

60. Printereid, koopiamasinaid, purustajaid ja muud varustust, mida kasutatakse NATO salastatud teabe reprodutseerimiseks või hävitamiseks, kaitstakse füüsiliselt sellisel määral, mis tagab, et neid saavad kasutada ainult volitatud isikud ja et NATO salastatud teavet kontrollitakse NATO julgeolekupoliitika (NATO Security Policy) ja seda täiendavate direktiivide kohaselt.

KAITSE TEHNILISTE RÜNNAKUTE VASTU

61. Kontorid või alad, kus regulaarselt arutatakse NS ja kõrgemal tasemel salastatud teavet, peavad olema kaitstud passiivsete ja aktiivsete pealtkuulamisrünnakute eest usaldusväärsete füüsilise julgeoleku meetmetega ja läbipääsukontrolliga, kui risk selleks põhjust annab. Riski kindlaksmääratlemise vastutust koordineeritakse tehniliste ekspertidega ja selle üle otsustab vastav julgeolekuasutus.

62. Kaitse passiivsete pealtkuulamisrünnakute vastu (näiteks NATO salastatud teabe leke ebaturvaliste sidevahendite või soovimatult kiirguva elektromagnetilise signaali kaudu) võib hõlmata tehniliste turvasoovituste küsimist.

63. Kaitse aktiivse pealtkuulamise vastu (näiteks NATO salastatud teabe leke mikrofonide, raadiomikrofonide või muude paigaldatud seademete kaudu) nõuab ruumi tarindite, mööbli ja tarvikute ning kontoritehnika, sealhulgas (mehaaniliste ja elektriliste) kontoriseadmete ja sidevahendite tehnilist ja/või füüsilist julgeoleku kontrolli. Neid kontrolle peavad läbi viima vastava julgeolekuasutuse poolt volitatud ja asjakohase väljaõppega teenistujad.

Elektriliste/elektrooniliste seadmete kontroll

64. Enne mistahes sidevahendite ja elektriliste või elektrooniliste seadmete kasutatamist aladel, kus peetakse koosolekuid või tehakse tööd, mis hõlmavad NS ja kõrgemal tasemel salastatud teavet ja asjaoludel, kus turvariskide hindamise põhjal osutub ohutase kõrgeks, peavad tehnilise julgeoleku kontrolli või sideturvalisuse eksperdid need üle vaatama ja veenduma, et nimetatud seadmetega ei edastataks tahtmatult või ebaseaduslikult arusaadavat teavet väljapoole klass I või klass II turvaala.

AVATUD HOIUALAD

1. Avatud hoiualad on alad, mille puhul vastav julgeolekuasutus on andnud loa NATO salastatud teabe avatud säilitamiseks. Alad peavad olema ehitatud järgmiste standardite kohaselt.

(a) **Konstruktsioon**
perimeetri seinad, põrandad ja lagi peavad olema püsiva konstruktsiooniga ja üksteise külge kinnitatud. Kogu konstruktsioon peab olema teostatud nii, et loata sissetungimine oleks visuaalselt tuvastatav.

(b) **Uksed**
uksed peavad olema puidust, metallist või muust tugevast materjalist. Välisuksed peavad olema kindlustatud sisseehitatud heakskiidetud kolmekohalise kombinatsioonlukuga. Eriliste asjaolude puhul võib vastav julgeolekuasutus anda loa NS ja NC tasemel salastatud teabe hoidla välisustele teiste lukkude paigaldamiseks. Uksi, mida ei kindlustata eespool mainitud lukkudega, kindlustatakse seestpoolt kas avariiväljapääsu riivlukuga, riivlukuga või terve ukse laiuse jäiga puit- või metall-latiga või muude vahenditega, mille vastav julgeolekuasutus on heaks kiitnud.

(c) **Ventilatsiooniavad, kaablikanalisatsioonid ja erinevad avaused**
kõik avatud hoiualasse sisenevad või seda läbivad ventilatsiooniavad, kaablikanalisatsioonid ja sarnased avaused, mille pindala on suurem kui 96 ruuttolli / 620 ruutsentimeetrit (ja mille kõige väiksem mõõt on suurem kui 6 tolli / 15 sentimeetrit) peavad olema kaitstud kas trellide, venitatud metallist restide, kaubandusvõrgust pärinevate tugevate metallplaatide või valveseadmestikuga.

(d) **Aknad**

(i) kõik aknad, mis võivad mõistlikkuse piires võimaldada rajatises salastatud tegevuste jälgimist, tuleb muuta läbipaistmatuks või varustada ruloo, kardinate või muude katetega; ja

(ii) esimese korruse tasemel paiknevad või muul viisil lihtsasti ligipääsetavad aknad (näiteks katuselt, verandalt ja juurdeehitustelt) tuleb ehitada materjalidest või katta materjalidega, mis tagavad kaitse sissetungi eest. Akende kaitse ei pea olema tugevam kui piirnevad seinad. Avatud hoiualade puhul, mis paiknevad kontrollitavas rajatises või võrdväärses kohas, võib sissetungivastase kaitse nõude kõrvale jätta, kui aknad on muudetud mitteavatavaks kas alalise sulgemise või sissepoole paigaldatud lukustusmehhanismiga ning nad on kaetud valveseadmestikuga (kas aknale eraldi paigaldatud andurite või alal paiknevate liikumisanduritega).