Küberneetika AS
Infotehnoloogia Osakond

*Dok*. DO--X-09-0498

# TURVAKLASSIDE KIRJELDUSED

## TEHNILINE ARUANNE

lk. 14

Töö täitjad:
Ahto Buldas
Monika Oit
Valdo Praust[1]

Tallinn 1998

[1] Osales töös kui Eesti Informaatikakeskuse esindaja

# ANNOTATSIOON

Käesolevas töös esitatakse infosüsteemide, eriti riiklike andmekogude, turvavajaduste ja nõuete spetsifitseerimise metoodika, mis seisneb erinevatele turvaeesmärkidele vastavate turvaklasside määramises.

# SISUKORD

**1.TERMINID....4**

**2.TURVAKLASSID JA NENDE OTSTARVE....5**

**3.ANDMETURBE KOLM ASPEKTI....7**

**4. KONFIDENTSIAALSUS....8**

**5. KÄIDELDAVUS....10**

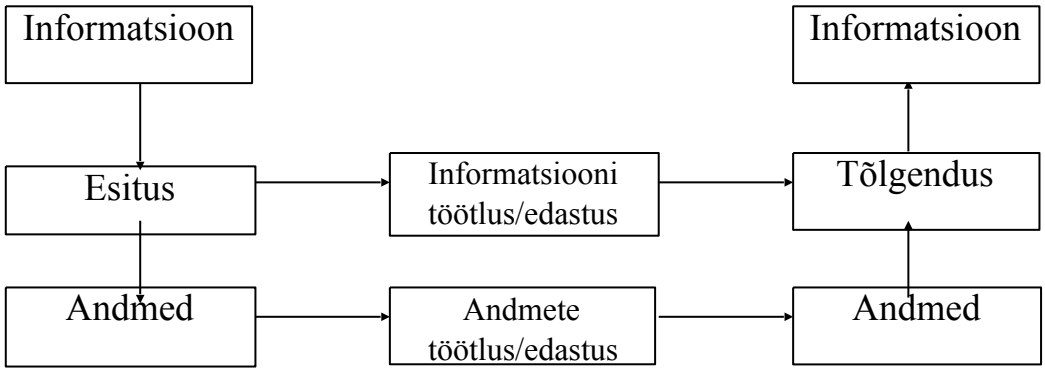
**6. TERVIKLUS....12**

**7. ÜLDISI MÄRKUSI....13**

## 1.TERMINID

*Informatsioon* – teadmus[2], mis puudutab objekte, näiteks fakte, sündmusi, asju, protsesse või ideid, sealhulgas mõisteid, ja millel on teatavas kontekstis eritähendus.

*Andmed* – informatsiooni taastõlgendatav esitus[3] formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks.




*Joonis 1*. Andmete ja informatsiooni vahekorda selgitav skeem.

*Olem* – suvaline konkreetne või abstraktne asi, mis eksisteerib, eksisteeris või võiks eksisteerida, kaasa arvatud nende asjade ühendused.

*Andmebaas* – rakendusvaldkondi toetav andmete kogum, mis on organiseeritud vastavalt mingile kontseptuaalsele struktuurile, kirjeldab nende andmete tunnusomadusi ja neile andmetele vastavate olemite vahelisi seoseid.

*Konfidentsiaalsus* – omadus, mis näitab, et informatsioon ei ole tehtud kättesaadavaks volitamata isikuile, olemitele või protsessidele ega neile avalikustatud (ISO 7498-2:1989).

*Andmeterviklus* – omadus, mis näitab, et andmeid ei ole volitamatul viisil muudetud ega hävitatud (ISO 7498-2:1989).

*Käideldavus* – omadus olla volitatud olemi nõudmisel kättesaadav ja kasutuskõlblik (ISO 7498-2:1989).

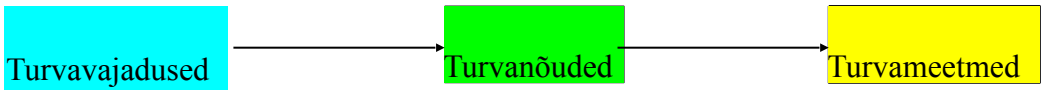
---

[2] informatsiooni mõiste on seotud temast üldisema – teadmuse – mõistega, mille üheks osaks on see mida teatakse, st mingi asjaolu (objekt), ja teiseks osaks see kes teab (subjekt). Informatsioonil iseenesest puudub vorm, mis tekib alles esituse kaudu.

[3] andmed on informatsiooni esitus, st tema kirjapanek mingis eelnevalt kokkulepitud formaliseeritud keeles, mis võimaldab andmetele vastavat teadmust edasi anda subjektilt subjektile. Andmete tõlgendus erinevate subjektide poolt võib aga olla erinev. Näiteks sõna 'hallitus' tähendus sõltub sellest, kas tema lugeja on eestlane või soomlane.

## 2.TURVAKLASSID JA NENDE OTSTARVE

Mistahes infosüsteemi turvaülesande lahendamine seisneb turvameetmete valimises vastavalt turvavajaduste alusel kehtestatud turvanõuetele. Turvavajaduse väljaselgitamisel ja turvanõuete püstitamisel lähtutakse varadele antud hinnangutest, ohu- ja riskianalüüsi tulemustest, kuid samas ka kehtivatest andmeturvet puudutavatest seadusandlikest aktidest. Näiteks isikuandmeid tuleb kaitsta vastavalt Isikuandmete kaitse seaduses ette nähtud korrale, sõltumata sellest, kas on karta otsest finantskahju asutusele või organisatsioonile.




Asutuse või organisatsiooni infosüsteemis vajalikud turvanõudeid tulenevad seega paljudest parameetritest. Tegelikke turvavajadusi arvestava turvameetmete spetsifikatsiooni saamine eeldab põhjalikku analüüsiprotseduuri, mille läbiviija peab olema kursis nii asutuse töö spetsiifika kui ka andmeturbe tehniliste küsimustega. Niivõrd laia teadmusega spetsialistide vähesuse tõttu esineb sageli olukordi, kus asutuse oma töötajate poolt pakutud turvameetmed on tehnilistel põhjustel ebapiisavad[4], või kus andmekaitse spetsialistide poolt valitud tehnilises mõttes täiuslikud turvameetmed ei arvesta asutuse tegelikke turvavajadusi. Seetõttu on vajalik turvaülesande jaotamine kaheks alamülesandeks:

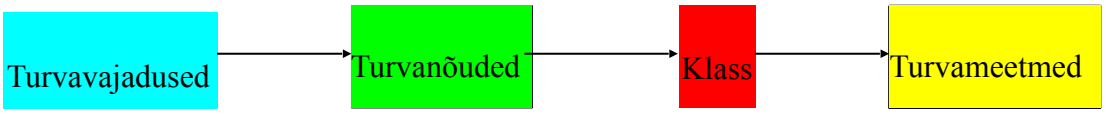
- turvanõuete püstitamine – teostatakse asutuse või organisatsiooni töötajate poolt.
- turvameetmete valik – teostatakse infotehnoloogia ja andmeturbe spetsialistide poolt.

Töö jaotamine eeldab alati vahetulemuste edasiandmist erineva elukutse, haridusliku tausta ja vaadetega inimeste vahel. Sellest tuleneda võivate vääritimõistmiste ärahoidmiseks on vaja formaliseeritud keelt vahetulemusena saadud informatsiooni üleandmiseks.
Asutuses ei leidu sageli töötajat, kellel oleks detailne pilt kogu asutuse infovahetusest, mistõttu ei saa turvavajaduste selgitamisel tavaliselt piirduda üheainsa töötaja arvamusega, vaid tuleb küsitleda kümneid ja vahel ka sadu töötajaid. See asjaolu võib aga muuta turvavajaduste kirjelduse killustatuks ja ebaülevaatlikuks. Infosüsteeme ja seadmeid projekteerivad spetsialistid tahavad,

[4] Meenutagem kasvõi pool aastat tagasi ühes päevalehes avaldatud Nõmme haigla peaarsti väidet, et haiglast varastatud arvutist polevat võimalik sinna salvestatud delikaatseid isikuandmeid kätte saada, kuna need olevat parooliga kaitstud.

et turvanõudeid oleksid esitatud lihtsamalt ja konkreetsemalt. Sellest tuleneb soov omada kokkuleppelisi **turvaklasse,** mis ülesannet lihtsustaks.

Turvaklasse võib (turvaspetsialisti seisukohalt) vaadelda kui teatud turvameetmete komplekside sümboleid, mis ise on sõltumatud turvavajaduste põhjustest, ja teisalt (asutuse töötajate seisukohast) kui teatud turvanõuete komplekside sümboleid. Näiteks ei olene konfidentsiaalsust tagavad turvameetmed sellest, kas kaitstavad andmed on riigisaladus või delikaatsed isikuandmed, vaid üksnes sellest, mil määral neid on vaja kaitsta.




Vanemates klassifikatsioonides (TCSEC, ITSEC) on klassid üheselt määratud komplektid funktsionaalsetest nõuetest. Klasse on võrdlemisi vähe, st parimal juhul kümmekond. See asjaolu seab aga olulised kitsendused turvanõuete kirjeldamise täpsusele ja muudab klassifikatsiooni kasutamise väheefektiivseks. Uusimates (algust tehti juba ITSEC klassides) klassifikaatorites on turvalisus kui eesmärk jagatud erinevateks aspektideks, millele vastavad spetsiifilised turvanõuded ja ka spetsiifilised turvameetmed.

## 3.ANDMETURBE KOLM ASPEKTI

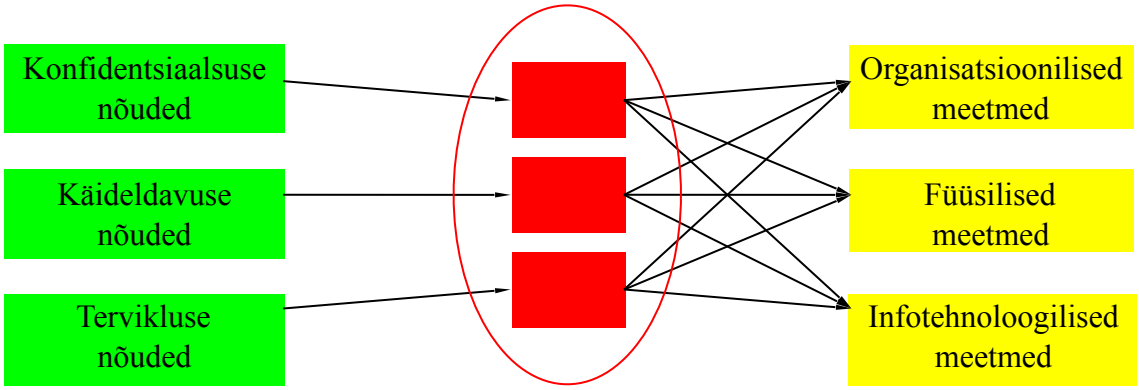
Suurema kirjeldustäpsuse saavutamiseks jagatakse andmeturve kui eesmärk tavaliselt kolmeks alameesmärgiks:

- konfidentsiaalsus – andmete loetavus üksnes volitatud isikutele,
- käideldavus – andmete kiire ja mugav kättesaadavus volitatud isikutele,
- terviklus – andmete kaitstus võltsimise ja volitamata muutmise eest.

Mõned standardid pakuvad eraldi järgmisi omadusi:

- autentsus – pärinevus väidetavast allikast, mida ülaltoodud kolmeses jaotuses võib vaadelda tervikluse osana;
- jälitatavus – võimalus olemi toiminguid üheselt jälitada, mis samuti on vaadeldav tervikluse ja konfidentsiaalsuse osana, sest jälitatavuse vajadus ei oma iseseisvat tähtsust, vaid tuleneb neist kahest, või isegi kõigist kolmest aspektist;[5]
- usaldusväärsus – ettenähtud käitumise ja tulemuste järjekindlus, mida võib vaadelda käideldavuse osana;

Turvaklassi määramist võib eelnenust tulenevalt vaadelda kui üksteisest sõltumatute osaklasside määramist.




Turvaklass

[5] Võimalus olemite toiminguid jälitada ei ole infoturbe seisukohalt omaette hüve. Jälitamisvõimaluse olemasolu võib vaadelda üldise peletus- ja tuvastusmehhanismina, mille rakendamise eesmärk on kas tervikluse, käideldavuse või konfidentsiaalsuse tagamine.

## 4. KONFIDENTSIAALSUS

Andmete konfidentsiaalsus tähendab kvalitatiivselt nende loetavust üksnes volitatud isikutele. Kvantitatiivses tähenduses tuleb konfidentsiaalsust mõista ühest küljest kui vajalike salastusmeetmete ranguse mõõtu, ja teisest küljest kui avalikustamisest tulenevate kahjude ulatuse mõõdupuud. Praktika on näidanud, et konfidentsiaalsuse puhul on just potentsiaalsed kahjud need, mille abil andmeturvet ja krüptograafiat pealiskaudselt tundev inimene saab vajalikku konfidentsiaalsusklassi adekvaatselt määrata. Käesolev klassifikatsioon eristab nelja konfidentsiaalsusklassi[6], mille kahjudest lähtuvad kirjeldused on järgmised.

S3. Teabe avalikustamine on ohtlik riigi, asutuse või inimese julgeolekule või on vastuolus inimõigustega; samuti kui teabe avalikustamine võib põhjustada kontrollimatuid muudatusi riigile või asutusele tähtsates infosüsteemides. Riigile tähendab andmete avalikustamine eelarvega võrreldavaid kahjusid, ettevõttele tema aastakäibega võrreldavaid kahjusid.

Sellesse klassi võib arvata näiteks informatsiooni uute relvade hankimise ja väljatöötluse kohta, mille leke võiks ohustada nende relvade riigikaitse eesmärgil kasutamise efektiivsust ja seeläbi nõrgendada riigi kaitsevõimet. Iga ettevõte võib lugeda klassi S3 kuuluvaks kõik sellised andmed, mille avalikustamine seab ohtu ettevõtte eksistentsi. Samuti võib lugeda sellesse klassi kuuluvaks näiteks kohtuprotsessidesse kaasatud oluliste tunnistajate isikuandmeid, mille avalikustamine seaks ohtu tunnistajate elu. Kõik pääsuandmed, mis võimaldavad piiramatut tegutsemist riiklikult tähtsates andmekogudes (näiteks põhiregistrid) põhjustades sellega kaost riigis, võib samuti lugeda klassi S3 kuuluvateks. Iga ettevõtte võib liigitada näiteks oma süsteemiülema paroolid ja kasutatavad krüpteerimisvõtmed klassi S3 andmeteks, sest nende avalikustamine võib põhjustada andmekogude hävingut ja delikaatsete isikuandmete ulatuslikku leket.

S2. Teabe avalikustamine häirib riigi või asutuse funktsioneerimist või rikub inimese privaatsust. Riigile tähendab andmete avalikustamine miljonitesse ulatuvaid kahjusid, ettevõttele aga kahjusid, mis ulatuvad kümne protsendini aastakäibest.

Sellesse klassi võib arvata näiteks teabe, mille leke võib häirida riigikaitset või diplomaatiat, põhjustada välis- ja sisepoliitilisi kriise, nõrgestada majandust. Kõik delikaatsed isikuandmed võiksid olla S2 konfidentsiaalsusega, samuti ka need isikuandmed, mille avalikustamine on isiku enda poolt ära keelatud. Samuti kuuluvad siia klassi poliitikat ja majandust laias ulatuses puudutavate seadusandlike aktide vahevariandid ja mustandid, mis võivad põhjustada segadusi enne ametliku lõppvariandi valmimist. Eraettevõte võib liigitada klassi S2 näiteks kõik tulevaste äriideedega seotud teabe, mille avalikustamine on kasulik konkurentidele ja võib tunduval määral vähendada ettevõtte tulusid. Riikliku registri pidajad võivad sellesse klassi liigitada kõik paroolid, mille abil on võimalik saada piiratud lugemis- ja modifitseerimisõigusi registri andmetes.

S1. Teabe avalikustamine võib põhjustada materiaalset või moraalset kahju.

Sellesse klassi võib arvata näiteks asutuse või ettevõtte töötajate palgaandmed, mille avalikustamine konkurentidele ja ka teistele töötajatele võib põhjustada asutusele materiaalset kahju, samuti asutuse sisemist töökorraldust puudutavad andmed.

S0. Teave on kõigile soovijaile kasutamiseks.

---

[6] Klassifikaatori eeskujuks on võetud riigisaladuse kaitse korras toodud klassijaotus: täiesti salajane, salajane, konfidentsiaalne, avalik. Antud klassifikaatoris on need nimed sihilikult ära jäetud, et mitte tekitada asjatuid vaidlusi klasside tähenduse üle.

Ehkki sellesse klassi võib liigitada kõik andmed, millele pole otstarbekas muud konfidentsiaalsusklassi omistada, on ka klassi S0 ära märkimine oluline, sest see näitab vähemasti konfidentsiaalsusvajaduse hinnangu olemasolu.

Liiga rangete konfidentsiaalsust tagavate meetmete kasutamine võib halvata infosüsteemi tööd ja olla seega ohuks käideldavusele. Seetõttu on oluline, et erinevate klasside määramise õigus andmetele on rangelt reglementeeritud. Näiteks klassi S3 määramise õigus võiks olla ainult isikul, kes vastutab andmeturbe eest tervikuna, st nii konfidentsiaalsuse kui ka tervikluse eest.

Konfidentsiaalsusklass kui konfidentsiaalsuse kaitsevajaduse määr ei ole absoluutses sõltuvuses potentsiaalsete kahjude rahalise suurusega, vaid sõltub kaitstavate varade omaniku olukorrast. Riigi kui omaniku jaoks võib klassi S3 andmete lekkega seotud kahjude määr olla rahaliselt tunduvalt suurem kui näiteks väikefirma juhi poolt määratud klassiga S3 andmetel.

## 5. KÄIDELDAVUS

Andmete käideldavuse omadus väljendub nende andmete õigeaegses ja hõlpsas kättesaadavuses volitatud isikutele. Käideldavus on infosüsteemi põhiline nõue ilma milleta pole kogu infosüsteemil mõtet. Käideldavuse vajadust saab iseloomustada kahe kvantitatiivse suurusega:

- teabe aegkriitilisus – aeg, mille jooksul peavad andmed peale vajaduse tekkimist olema kättesaadavad, st nende hilisemal kättesaadavusel pole mõtet.
- teabe hilinemise tagajärgede kaalukus – potentsiaalne hinnatud kahju, mis tekkib andmete hilinemisel.

Need parameetreid tuleb vaadelda sõltumatutena. Teave võib olla aegkriitiline, kuid samas tema mittesaamise tagajärjed ei pruugi olla eriti tõsised.

Aegkriitilisuse järgi jagatakse andmed kolme klassi:

K2. Teave, mis tuleb saada sekundite jooksul.
Siia klassi kuuluvad kõik operatiivjuhtimiseks vajalikud andmed, mille edastamine toimub reeglina automatiseeritult ilma inimese vahetu osavõtuta. Näiteks politsei, tolli, piirivalve ja kaitseväe operatiivinfo. Klassi K2 võib liigitada ka börsi- ja finantsoperatsioonide teave, samuti meditsiini- ja päästeteenistuse operatiivinfo, lennu- ja laevajuhtimisel kasutatav seiresüsteemide teave.

K1. Teave, mis peab olema kättesaadav mõne või mõnekümne minuti jooksul.
Siia võib liigitada näiteks uudistes edastatava teabe. Sellesse klassi peaks kuuluma ka valdav enamus riiklikes registrites hoitavast teabest[7]. Näiteks passi- ja autoregistrid.

K0. Teabe hilinemine mitme päeva jooksul ei põhjusta komplikatsioone.
Vaikimisi kuulub siia kogu teave, millele pole aegkriitilisuse nõudeid esitatud.

Hilinemise tagajärgede kaalukuse järgi jagatakse andmed nelja klassi:

R3. Teabe õigeaegne mittesaamine põhjustab kas
- riigi suveräänsuse kadu või ettevõtte pankrotti,
- kahjusid, mis on võrreldavad riigieelarve või ettevõtte aasta-käibega,
- mitmeid hukkunuid või
- ulatuslikku keskkonnasaastet.

Siia kuulub päästeteenistuse ja kaitseväe operatiivinfo. Samuti kuulub sellesse klassi finantsasutuste tehingute info. Sellesse klassi kuuluvad ka ministrite ja kaitseväe juhataja korraldused.

R2. Teabe mittesaamine põhjustab kas
- olulist kahju riigi suveräänsusele või ettevõtte mainele,
- miljonitesse ulatuvaid kahjusid,
- ohtu inimelule või
- keskkonnasaastet.

---

[7] Riiklike registreid on siin käsitletud Andmekogude seaduses määratletud mõistes. Riiklike registrite alla ei kuulu kõik ametkondlikud andmekogud, näiteks huntide register ja säinaste register.

Siia kuulub enamik riigiametnike ja ettevõtte juhatuse korraldusi. Siia klassi kuuluvad ka häired tehnoloogiliste protsesside (kaasaarvatud transpordisüsteemid) juhtimissüsteemides, samuti järelvalve- ja signalisatsioonisüsteemides.

R1. Teabe mittesaamine põhjustab kas

- häireid riigikorralduses või ettevõtte tegevuses,
- sadadesse tuhandetesse ulatuvaid kahjusid,
- ohtu inimeste tervisele või
- keskkonnasaaste ohtu.

Siia võib liigitada mistahes andmed, mille alusel tehakse mingeid (majanduslikke) otsuseid, nt kuulutatakse välja hankekonkursse, esitatakse tellimusi jne.

R0. Teabe mittesaamine ei too kaasa mainimisväärseid tagajärgi.

## 6. TERVIKLUS

Tervikluse omadus väljendab andmete volitamata muutmise võimatust ja andmete allika tuvastatavust ja tõestatavust. Terviklusnõude juures tuleb arvestada järgmiste nõuete tasemetega ranguse järjekorras:

- andmeallika tõestatavus,
- andmeallika tuvastatavus,
- volitamatu muutmise tuvastatavus,
- madal terviklus.

Selle alusel jaotatakse teave nelja klassi:

T3. Teave, mille allikat saab tõestada kolmandale osapoolele. Teave on niivõrd kaaluka tähtsusega, et võib olla vaja kohtus tõestada tegelikku sisestajat või viimase muudatuse tegijat.
Siia kuulub näiteks registris fikseeritud teave välja antud passide kohta, et tuvastada ja vajaduse korral kohtus tõestada valepassi välja andnud töötaja süü. Ettevõtte juht võib liigitada klassi T3 kõik teabe, mille eest vastutamiseks ei piisa vastutusest asutuse juhi ees, kelle maksimaalne võimalik karistus alluvale on tema lahtilaskmine.

T2. Teave, mille allikas on tuvastatav. Teave on piisava tähtsusega, et selle teabe vastutav töötleja peab saama tuvastada, milline tema alluvaist on andmed sisestanud või neis viimati muudatusi teinud.
Vastutusala juht võib tema halduses (vastutusalas) oleva teabe liigitada klassi T2, kui selle teabe terviklus on oluline kogu vastutusalale tervikuna, st kui vastutusala juht peab saama vajaduse korral karistada teabe hooldamisel eksinud alluvat.

T1. Teave, mille volitamatud muutmised on tuvastatavad. Teave, mille kõik volitamata muudatused peavad olema tuvastatavad, isegi kui need on tehtud süsteemiülema poolt tema töö kaigus.
Sellesse klassi võib liigitada teabe, mille terviklust peab olema võimalik kiiresti tuvastada, kuid otsest vajadust selle allika või viimase muutja tuvastuseks ei ole.

T0. Terviklusomadused pole olulised.

## 7. ÜLDISI MÄRKUSI

Klasside tähistuses on kasutatud vastava omaduse nimetusele viitavat tähte, kusjuures on püütud vältida võimalikke väärassotsiatsioone tekitavaid tähistusi (A, B, C, E, F - vastavalt TCSEC ja ITSEC klasside tähistused, I - võib minna segamini number 1-ga)

Kokku tuleb 192 klassi, kuid neid ei vaadelda tervikuna, vaid komponentidena. Erinevaid komponente on kokku 15, millest igaühele pannakse vastavusse konkreetsed turvanõuded.

Näiteks üks konkreetne klass on S2K1R3T2.

Turvaklassi võib omistada kas kogu andmebaasile/andmekogule, tema osale, üksikutele andmeväljadele või ka teatud päringutele andmebaasist.