MÕISTED

1) Andmed- informatsiooni taastõlgendatav esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks.
2) Andmekaitse- halduslike, tehniliste või füüsiliste meetmete rakendamine kaitseks volitamatu juurdepääsu eest andmetele.
3) Andmekogu- arvutustehnikas andmete kogumine, salvestus ja korrastamine raaltöötluseks.
4) Andmete töötlemine- andmetega (protsessina) operatsioone sooritama.
5) Autoriseerimine- protsess, mis annab (või keelab) õiguse ligi pääseda võrguressurssidele. Enamik e-kaubanduse turvasüsteeme põhineb kaheastmelisel protsessil. Esiteks toimub autentimine, kus kontrollitakse, et kasutaja on tõesti see, kellena ta esineb, seejärel toimub volitamine, mis lubab kasutajal juurde pääseda temale ette nähtud ressurssidele.
6) Avalik võti- krüptograafias nimetatakse avalikuks võtmeks usaldatava asutuse poolt väljastatud ja krüpteerimisvõtmena kasutamiseks mõeldud väärtust, mida koos avalikust võtmest tuletatud privaatvõtmega saab efektiivselt kasutada sõnumite ja digitaalallkirjade krüpteerimiseks. Avaliku ja privaatvõtme paari kasutamist tuntakse *asümmeetrilise krüptograafia* nimetuse all.
7) Viirus- pahatahtliku häkkeri kirjutatud programmijupike, mis on lülitatud mingi normaalse programmi koosseisu ning põhjustab ootamatuid ja sageli kasutajale äärmiselt ebameeldivaid tagajärgi.
8) Virtuaalne privaatvõrk- privaatvõrk, mis kasutab avalikku telekommunikatsiooni infrastruktuuri, säilitades samal ajal privaatsuse ja turvalisuse.
9) Võrgulüüs- *default gateway* ehk vaikimisi võrgulüüs määratakse ära selleks, et arvuti teaks, kellele paketid saata kui soovitud sihtkoht ei asu samas võrgus.
10) 3DES- krüpteerimisstandard Triple DES (3DES) kasutab kolme täielikult sõltumatu võtmega DES-šifri rakendust EDE (Encipher-Decipher-Encipher ehk "šifreerimine-dešifreerimine-šifreerimine") režiimis.
11) AES- *täiustatud krüpteerimisstandard* NIST'i salajase võtmega krüpteerimismeetodi standard, mis kasutab 128, 192 ja 256-bitiseid võtmeid ning Rijndaeli algoritmi. Tuli

2001.a. Triple DES meetodi asemele. AES võimaldab teostada krüpteerimist ühe tsükliga kolme asemel ning selle võti on pikem kui Triple DES'i 168-bitine võti.

12) ARP- *aadressiteisenduse protokoll* Protokoll IP aadressi vastendamiseks arvuti füüsilisele ehk MAC-aadressile Etherneti kohtvõrgus (Etherneti-aadressile). Näiteks IP praegu kõige levinuma versiooni *IP version 4 (IPv4)* puhul on IP aadressi pikkus 32 bitti, aga Ethernet'i võrgus on seadmete aadresside pikkuseks 48 bitti . Seepärast peetakse ARP-puhvri nime all tuntud tabelit, mis seab omavahel vastavusse IP-aadressid ja MAC-aadressid. ARP annab ette protokollireeglid, mille alusel toimub selle vastavuse tekitamine ja aadresside teisendamine.
13) AV- *täiendatud virtuaalsus* Keskkond, kus enamik inimese vaataväljas paiknevaid objekte on genereeritud arvuti abil ja ainult väike osa neist on reaalsed. Näiteks võib reaalne olla ainult inimene ise, kes on paigutatud täielikult virtuaalsesse keskkonda.
14) BYOD- *tule oma seadmega* Poliitika, mis lubab töötajatel või õpilastel kasutada oma isiklikke sülearvuteid, tahvelarvuteid, nutitelefone jms nii kodus kui ka tööl ja koolis. Vajadus sellist poliitikat rakendada hakkas kasvama koos mobiilseadmete levikuga ja on valdav arengumaades (Brasiilia, Venemaa, India jt). Positiivne on BYOD-i puhul see, et inimestel on mugavam kasutada üht ja sama seadet nii kodus kui tööl ja enamasti on isiklikud seadmed ka uuemad ja moodsamad, sest firmad ei uuenda oma tehnikat nii tihti kui eraisikud. See tõstab töötajate motivatsiooni ja suurendab tööviljakust. Teisalt kaasnevad aga sellega mitmesugused turvariskid.
15) CA- liikluse tuvastuse ja põrke vältimisega multipöördusvõrk.
16) CERT- 1988.a. asutatud Interneti andmeturbe probleemidega tegelev keskus Carnegie Mellon'i Ülikooli Tarkvaraprojekteerimise Instituudis.
17) CHAP- *väljakutse ja kätlusega autentimisprotokoll* Autentimisprotokoll, mille puhul autentimisagent (harilikult võrguserver) saadab klientprogrammile kasutajanime ja parooli krüpteerimiseks ettenähtud võtme. See võimaldab kasutajanime ja parooli edastamist krüpteeritud kujul, et kaitsta neid pealtkuulamise eest.
18) CRC- *tsükkelkoodkontroll.*
19) Avarii (Disaster) - järsk õnnetus, mis põhjustab suurt kahju
20) Avatekst- krüpteerimata tekst.
21) Avatus (Exposure)- võimalikkus, et teatav rünne kasutab ära *andmetöötlussüsteemi* teatava *nõrkuse.*

22) Dark Web- pimeveeb, interneti pahem pool.
23) Deep Web- süvaveeb sisaldab selliseid otsingumootorite poolt indekseerimata ja parooliga või tulemüüriga kaitstud ressursse, mis ei ole üldsuse jaoks ette nähtudki. Sellised andmed pole avalikuks kasutamiseks.
24) Dekrüpteerimine- krüpteeritud andmete või teksti "avamine" ehk teisendamine tagasi originaalkujule.
25) Dešifreerimine- krüpteeritud andmete või teksti "avamine" ehk teisendamine tagasi originaalkujule.
26) Ekstranet- firma intraneti laiendus väljapoole firmat läbi Interneti, et võimaldada valitud klientidele, hankijatele ja oma firma ringiliikuvatele töötajatele juurdepääsu firma konfidentsiaalsetele andmetele ja rakendusprogrammidele. Ekstranet erineb tavalisest firma veebisaidist, millele juurdepääs on kõigile vaba. Vahel võib see erinevus olla mõneti ähmane, kuid üldiselt tähendab ekstranet reaalaja-juurdepääsu läbi mingit tüüpi tulemüüri (firewall). Kuigi selliste süsteemide puhul tuleb pöörata erilist tähelepanu turvameetmetele, muutuvad nad järjest populaarsemateks.
27) Elutähtis teenus- elutähtis teenus on teenus, millel on ülekaalukas mõju ühiskonna toimimisele ja mille katkemine ohustab vahetult inimeste elu või tervist või teiste teenuste toimimist.
28) Foori protokoll (Traffic Light Protocol)- valgusfoori protokoll (TLP) loodi teabe parema jagamise hõlbustamiseks. TLP on tähiste kogum, mida kasutatakse tundliku teabe jagamiseks asjakohase vaatajaskonnaga.
29) Küberkriminalistika (Forensics)- on digitaalse kohtueksperti haru, mis on seotud arvutites ja digitaalsetes andmekandjates leiduvate tõenditega. Elektroonilise kriminalistika eesmärk on uurida digitaalset meediat kohtuprotsessiliselt mõistlikul viisil, eesmärgiga tuvastada, säilitada, taastada, analüüsida ja esitada digitaalse teabe kohta fakte ja arvamusi.
30) Haavatavus (Vulnerability)- vara või vararühma nõrk koht, mida saab ära kasutada üks või mitu ohtu.
31) Hübriidsõda- sõjapidamisviis, milles rakendatakse korraga nii konventsionaalse kui ka mittekonventsionaalse sõjapidamise elemente. Mittekonventsionaalseteks elementideks võivad olla näiteks majandustegevuse abil mõjutamine, propaganda, eri meediakanalite kaasamine, vastase psühholoogiline mõjutamine ja kübersõda.

32) Käideldavus - infosüsteemi põhiline nõue ilma milleta pole kogu infosüsteemil
33) Kaitsetus - ilma kaitseta
34) Konfidentsiaalsus - andmete loetavus üksnes volitatud isikutele
35) Krüpteerimine - muuta failis asuvad andmed võõrastele loetamatuteks ehk info salastada
36) Krüptoalgoritm - algoritm, mis on kavandatud arvutusliku kõvaduse eelduste ümber
37) Krüptograafia - informatsiooni muutmine loetamatuks ilma eriteadmiste ja -vahenditeta
38) Krüptogramm - salakirjas tekst
39) Küberkuritegu - kuriteod, mis on pandud toime elektrooniliste sidevõrkude ja infosüsteemide abil või selliste võrkude või süsteemide vastu
40) Kübersõda - on sõda küberruumis; arvuteid ja võrke (s.h internetti) kasutatakse relvadena.
41) Lunavara - pahavara, mis krüpteerib kasutaja arvutis kas teatud olulised andmed või terve kõvaketta, mille järel kurjategijad nõuavad andmete lahtikrüptimisvõtme eest lunaraha
42) MIME - ehk Multipurpose Internet Mail Extensions on Interneti-standard, mis laiendab e-kirjade vormingut, et toetada teksti tähemärkide komplektides, va ASCII, ning heli-, video-, pildi- ja rakendusprogrammide manuseid
43) NAT - ehk Võrguaadresside teisendus on võrguliikluses ja ruuterites kasutatav tehnika, mis seisneb IP-pakettide päiste muutmises, nii et paistaks, nagu võrguliiklus tuleneks NAT-ruuterist, kuigi ühenduse looja oli mingi seade NAT-ruuteri "taga"
44) NTP - ehk võrguaja protokoll on andmesideprotokoll täpse aja edastamiseks ajaserveritest.
45) OSINT - ehk Open-source intelligence on avalikult kättesaadavatest allikatest kogutud andmed, mida kasutatakse luurekontekstis.
46) PAN - ehk Personaalvõrk on arvutivõrk seadmete ühendamiseks, mille keskmes on üksikisiku tööala.
47) PAP - ehk Parooli autentimisprotokoll on paroolipõhine autentimisprotokoll, mida kasutab PPP (Point to Point Protocol) kasutajate valideerimiseks
48) PCI-DSS - ehk Maksekaarditööstuse andmeturbe standard on infoturve, mis pakub tehnilisi ja operatiivseid nõudeid, mis on mõeldud konto andmete kaitsmiseks.

49) PGP - ehk Pretty Good Privacy on krüpteerimisprogramm, mis pakub krüptograafilist privaatsust ja autentimist andmesideks
50) PKI - ehk Avaliku võtme infrastruktuur on avaliku võtme infrastruktuur võimaldab turvaliselt digitaalselt autentida ja allkirjastada
51) MAC-aadress - ehk meediumipöörduse juhtimise aadress on füüsilise võrguliidese unikaalne identifitseerija
52) Marsruuter - ehk ruuter on elektrooniline seade, mis ühendab omavahel kaht või enamat arvutivõrku, ning võimaldab nendevahelise andmeside
53) Nimeserver - ehk DNS-server (domeeninimede süsteem) andmesidevõrgus töötav server, mis pakub domeeninimede IP-aadressid vastendamise teenust
54) Nõrkus (Vulnerability) - on nõrkus, mida ähvardaja, näiteks ründaja, saab arvutisüsteemis volitamata toiminguteks ära kasutada
55) Nuhkvara - on tarkvara, mis kogub arvuti kasutaja kohta isiklikku infot ilma sellest kasutajat selgesõnaliselt teavitamata
56) Oht (Threat) - on võimalik oht, mis võib ära kasutada turvalisuse rikkumise haavatavust ja põhjustada seega võimalikku kahju
57) Õngitsemine - ehk phishing on inimpsüühikaga manipuleerimise üks viise, lollitamistehnika, millega üritatakse arvutikasutaja viia niikaugele, et ta annab kurjategijaile ise oma juurdepääsuandmed, paroolid, krediitkaardi rekvisiidid ja muu turvakriitilise informatsiooni
58) Pahavara - kahjustab arvutis asuvaid andmefaile ja vähendab arvuti jõudlust
59) Plokkšiffer - on deterministlik algoritm, mis töötab kindla pikkusega bitirühmades, mida nimetatakse plokkideks, muutumatu muutusega, mis on määratletud sümmeetrilise võtmega
60) Probleem (Problem) - on mis tahes olukord, mis ilmneb ootamatult või takistab millegi tekkimist
61) Räsi - on krüptograafias kasutatav ühesuunaline funktsioon tekstistringide kodeerimiseks
62) Risk - on kõik, mis võib negatiivselt mõjutada andmete konfidentsiaalsust, terviklikkust või kättesaadavust

63) Ründeskript - on tarkvara osa, andmemaht või käsurida, mis kasutab ära viga või haavatavust, et põhjustada tarkvara, riistvara või muu elektroonilise (tavaliselt arvutipõhise) tahtmatut või ettenägematut käitumist
64) DDoS- DDoS rünnak seisneb sihtmärgi päringutega nii ülekoormamises, et see muutub kättesaamatuks või kokku jookseb.
65) DES - Andmete krüptimisstandard. See on sümmeetrilise võtmege algoritm andmete krüptimiseks.
66) DoS - Platvormist sõltumatu akronüüm ketta opsüsteemile.
67) EDI - Elektrooniline andmevahetus. Arvutist arvutisse andmete vahetamine.
68) ETO - Engineer-To-Order on tootja nõuded oma klienditoodete ainulaadsete tehniliste projektide jaoks.
69) FTP - FTP on klient-server protokoll, mis tähendab seda, et failide vahetus toimub kahe arvuti vahel, millest üks on serveri, teine kliendi rollis
70) FW - Firmware. Püsivara on spetsiifiline arvutitarkvara klass, mis tagab seadme konkreetse riistvara madala taseme juhtimise
71) GMT - Greenwich Mean Time on keskmine päikeseaeg Londoni Greenwichi kuninglikus observatooriumis alates kesköösт
72) HIPAA - Ravikindlustuse kaasaskantavuse ja vastutuse seadus, USA seadus, mis on loodud pakkuma privaatsusstandardeid, et kaitsta patsientide haigusloosid ja muud terviseteavet, mida edastatakse terviseplaanidele, arstidele, haiglatele ja teistele tervishoiuteenuse pakkujatele.
73) Identiteet - Identiteet on omaduste hulk, mis teevad objekti unikaalseks võrreldes teiste objektidega
74) Identiteedi vargus - Identiteedivargus on isiku identiteedi volituseta kasutamise ehk teise isiku tähtsate isikuandmete (nimi, isikukood, dokument või pangakaart) andmete kuritarvitamine, mille tulemusena tekitatakse isikule materiaalset või moraalset kahju
75) Identifitseerimine - Identifitseerimine – identsust kindlaks tegema, kedagi või midagi kellenagi või millenagi ära tundma
76) Informatsioon - Informatsiooni all on algselt mõistetud ja mõistetakse üldkeeles ka praegu inimesele mõeldud andmeid ja teateid
77) Infosüsteem - Infosüsteem on asutuse, ettevõtte, omavalitsuse, riigi, organisatsiooni jne teabe säilitamiseks ja töötlemiseks mõeldud süsteem

78) Infovara - Näiteks ettevõtluses on andmeid ja andmed on ettevõtte infovara
79) Internet - Internet on mis tahes arvutivõrkude võrgustiku üldnimetus
80) Intranet - firmasisene arvutite lähivõrk, kus kasutatakse Internetiga ühilduvaid protokolle ja programme
81) Intsident - Ebameeldiv vahejuhtum
82) IP aadress - on arvutivõrgus asuva seadme (arvuti või nutiseadme) identifikaator ehk seadmele määratud alaline või ajutine tunnusnumber, mille abil võrku ühendatud seadmed üksteist leiavad
83) Isikuandmed - on teave inimese ehk füüsilise isiku (andmesubjekti) kohta, millega saab teda otse või kaudselt tuvastada
84) HMI - HMI on tarkvararakendus, mis pakub operaatorile või kasutajale teavet protsessi oleku kohta ning võtab vastu ja juhib operaatori juhtimisjuhiseid
85) HTTP - HTTP on aluseks olev protokoll, mida kasutab Internet ja see protokoll määratleb sõnumite vormindamise ja edastamise ning toimingud, mida veebiserverid ja brauserid peaksid erinevatele käskudele reageerimisel võtma.
86) IDEA - on sümmeetrilise võtme ploki šifr
87) IDS - Sissetungimise tuvastamise süsteem on seade või tarkvararakendus, mis jälgib võrku või süsteeme pahatahtliku tegevuse või poliitika rikkumiste suhtes
88) IMAP - on Interneti-põhine protokoll, mida e-posti kliendid kasutavad TCP / IP-ühenduse kaudu meiliserveritest e-kirjade allalaadimiseks
89) IOT - on omavahel seotud arvutusseadmete, mehaaniliste ja digitaalsete masinate, objektide, loomade või inimeste süsteem, mis on varustatud kordumatute identifikaatoritega (UID) ja võimega andmeid võrgu kaudu edastada, ilma et oleks vaja inimeselt inimesele või inimeselt arvutile interaktsiooni
90) IPS - kasutatakse arvutiturvalisuses. See pakub võrguliikluse eeskirju ja reegleid koos sissetungimiste tuvastamise süsteemiga süsteemi või võrguadministraatorite teavitamiseks kahtlasest liiklusest, kuid lubab administraatoril toimingu teha pärast hoiatuse saamist
91) ISKE - ISKE juurutamise eesmärk on tagada IT-süsteemides töödeldavate andmete jaoks piisav turvatase
92) ISO - on arvutifail, mis on olemasoleva failisüsteemi täpne koopia

93) LAN - on arvutivõrk, mis ühendab arvuteid piiratud alal, näiteks elukohas, koolis, laboris, ülikoolilinnas või büroohoones
94) Jadašifer - on sümmeetriline võtmesala, kus tavalise teksti numbrid on kombineeritud pseudo-juhusliku šifri numbrivooga (klaviatuur)
95) PLC- *programmeeritava loogikaga kontroller, programmeeritav kontroller* Juhtseade, mis kasutab programmeeritavat mikroprotsessorit ja on tavaliselt programmeeritud IEC 61131 programmikeeltes. Programmeeritavaid kontrollereid liigitatakse sageli selle järgi, kui palju neil on sisend/väljundporte. Need on sageli RISC-põhised ning neid kasutatakse tööstuslike seadmete ja protsesside juhtimiseks reaalajas
96) POP/POP3- Postkontoriprotokoll (POP) elektronposti vastuvõtmiseks. POP3 on klient/server protokoll, kus elektronposti sõnumeid võetakse vastu ja hoitakse ISP meiliserveris. Kasutaja (või tema arvutis olev klientprogramm) kontrollib perioodiliselt oma postkasti sisu ISP serveris ja laadib alla saabunud sõnumid.
97) RC4- Sümmeetriliste võtmetega voošiffer firmalt RSA Security (1987.a.). Selle loojaks oli Ron Rivest ja kuigi ametlikult on lühendi RC4 tähenduseks "Rivest Cipher 4", tuntakse seda rohkem nimetuse all "Ron’s Code"
98) RSA- USA firma RSA Data Security poolt 1977.a. välja töötatud avaliku võtmega krüpteerimismeetod , mis võimaldab nii andmete krüpteerimist kui autentimist.
99) S/MIME- on avaliku võtme krüptimise ja MIME andmete allkirjastamise standard.
100) SCADA- on arvutisüsteemide ja sidevõrkude abil toimuv tehniliste protsesside jälgimine ja juhtimine.
101) SMTP- *lihtne meiliedastusprotokoll* Üks TCP/IP protokollidest, mis on ette nähtud serveritevaheliseks e-posti sõnumite saatmiseks ja vastuvõtmiseks.
102) SNMP- *lihtne võrguhalduse protokoll* Interneti protokollistandard STD 15, RFC 1157 sõlmede haldamiseks IP võrgus.
103) Salajane võti- *privaatvõti* Krüptograafias nimetatakse privaatvõtmeks ainult salajasi sõnumeid vahetavatele partneritele teadaolevat võtit, mida kasutatakse nii sõnumite krüpteerimiseks kui dekrüpteerimiseks. Sellise süsteemi puhul on risk selles, et kui üks partneritest kaotab võtme või laseb selle ära varastada, kaob kohe süsteemi turvalisus. Et seda riski vältida, on kasutusele võetud avalike ja privaatvõtmete kombinatsioon.

104) Seiresüsteem- sensoorsete ja sidevahendite kooskõlastatud kogum, mis jälgib, tuvastab või registreerib loodusliku või kunstliku süsteemi väljundeid või toiminguid sündmuste ajaloo või tuleviku kujundamiseks.

105) Sertifikaat- tõend, mis kinnitab usaldusprintsiipi SSL-krüpteeritud tehingute puhul. Sertifikaadis on informatsioon selle väljastaja (sertifitseerimisasutuse), sertifikaadiomaniku (organisatsioon, kellele sertifikaat on väljastatud), avaliku võtme ja sertifikaadi kehtivusaja kohta (harilikult 1 aasta)ning selle hosti nimi, millel sertifikaati kasutatakse. Sertifikaadil on sertifitseerimisasutuse digitaalallkiri, nii et sertifikaadi mistahes detaili omavoliline muutmine tühistab sertifikaadi automaatselt.

106) Server- Võrguga ühendatud arvuti või seade, mis haldab võrgu ressursse.

107) Šifreerimine- Andmete krüptograafiline transformeerimine krüptogrammi loomiseks.

108) Signeerimine- nimega märgistama

109) Sündmus (Event)- Programmi poolt avastatav tegevus või toiming.

110) Terviklus- Infosüsteemi või andmete täielikkus ja vastuolude puudumine

111) Trollid- troll on inimene, kes paneb tülitsema või ärgitab inimesi Internetis tähelepanu kõrvale juhtima ja külvama ebakõlasid, postitades veebikogukonnas põletikulisi ja kahanevaid, võõraid või teemaväliseid sõnumeid

112) Tulemüür- Internetti ja kohtvõrku teineteisest eraldav spetsialiseeritud arvuti, nn. lüüsarvuti, mis ise ei sisalda tundlikke andmeid ja kaitseb kohtvõrku volitamata sissetungijate eest väljastpoolt.

113) Turvaauk- Tarkvara nõrk koht, mis võib ründajatele anda võimaluse tungida Internetiga ühendatud arvutisse ning varastada sealt andmeid või teha muud kurja

114) Turvameede- riski kahandav tegevus, protseduur või protsess

115) Uss (Worm)- Teatud tüüpi arvutiviirus, mis võrgukeskkonnas teiste programmide abita ennast paljundab ja levib.

116) Vara (Asset)- miski, millel on organisatsiooni jaoks väärtus.

117) SSH- *turvaline kest, turvakest* UNIX‘i-põhine käsuliides ja protokoll, mis võimaldab turvalist sisselogimist kaugarvutisse. Paljud võrguülemad kasutavad seda veebi- jt serverite kaugjuhtimiseks. SSH kujutab endast tegelikult komplekti kolmest utiliidist *slogin, ssh* ja *scp*, mis on varasemate UNIX’i utiliitide *rlogin, rsh* ja *rcp* turvalised versioonid. SSH käsud on krüpteeritud ja mitmes mõttes turvalised.

118) SSL- *turvasoklite kiht* Infoturbe protokoll üle Interneti edastatavate andmete turvalisuse tagamiseks. Sõna "sokkel" viitab sellele, et andmete edasi-tagasi saatmine klient- ja serverprogrammi vahel toimub läbi soklikihi programmi ja meenutab elektripirni pesasse sisse- ja väljakeeramist. SSL kasutab RSA kahe võtmega (avalik ja privaatvõti) krüpteerimissüsteemi. RSA süsteemi juurde kuulub ka digitaalne sertifikaat e. isikutunnistus. SSL protokolli töötas välja Netscape ja seda kasutatakse laialdaselt näiteks krediitkaardiinfo edastamiseks elektrooniliste äritehingute puhul

119) TCP- *edastusohje protokoll* Levinuim võrgu transpordikihi protokoll, mida kasutatakse Etherneti võrkudes ja Internetis.

120) TLS- *transpordikihi turbeprotokoll* Avatud protokoll, mis võimaldab klient-server rakendustel omavahel turvaliselt suhelda üle Interneti, olles kaitstud pealtkuulamise või sõnumite rikkumise ja võltsimise eest.

121) UDP- *kasutajadatagrammi protokoll* Sideprotokoll, mis pakub suhteliselt piiratud teenust andmete vahetamisel intentetiprotokolli (IP) kasutavasse võrku ühendatud arvutite vahel.

122) UTZ- UTZ programm võimaldab põllumajandustootjatel õppida paremaid põllundusmeetodeid, parandada töötingimusi ning hoolitseda paremini oma laste ja keskkonna eest

123) VPN- *virtuaalne privaatvõrk*

124) WAN- *laivõrk* Arvutivõrk, mis kasutab järjestikliine ja mille ulatus ületab 1 km

125) WEP- IEEE 802.11 andmeturbe protokoll traadita (raadio-) võrkudele (IEEE 802.11x).

126) WPA- Andmeturbe protokoll Wi-Fi alliansilt IEEE 802.11 standardile vastavatele raadiokohtvõrkudele (Wi-Fi võrkudele).