

# KASPERSKY LAB

---



**EASY-TO-USE**  
SYSTEM PROTECTING  
STORED DATA

**ADVANCED**  
TECHNOLOGIES AGAINST  
ALL TYPES OF HACKER  
ATTACKS

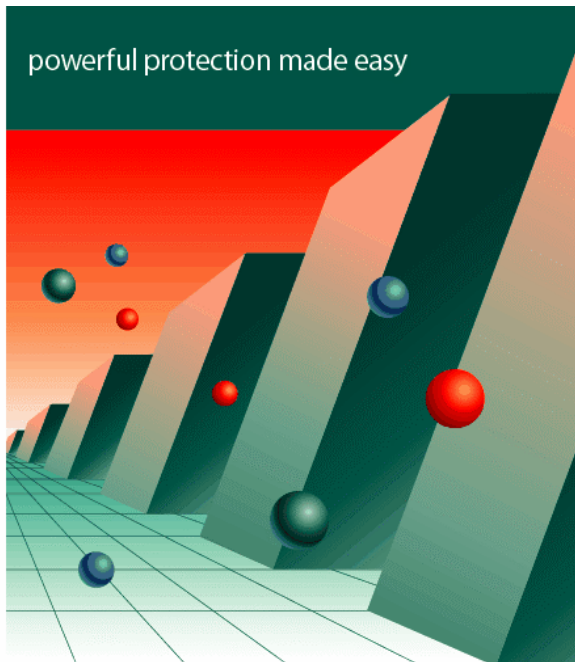
**COMPLETE**  
CONTROL OVER  
INTRUSION ATTEMPTS

**UNIQUE**  
SELF-LEARNING  
ABILITY

**COMPREHENSIVE**  
DATA PACKET  
FILTRATION

**CONTINUOUS**  
CONTROL OVER  
APPLICATION ACTIVITY

**FREE**  
ROUND-THE-CLOCK  
TECHNICAL SUPPORT



# Kaspersky Anti-Hacker

personal  
firewall

[www.kaspersky.com](http://www.kaspersky.com)

The Kaspersky logo, consisting of the word "KASPERSKY" in a stylized, outlined font, with a small red "3" to its right.

---

## Kaspersky Anti-Hacker 1.5

**KASUTUSJUHEND**

KASPERSKY ANTI-HACKER 1.5

---

# Kasutusjuhend

© Kaspersky Lab Ltd.  
Tel. +7 (095) 797-87-00 • Faks +7 (095)948-43-31  
<http://www.kaspersky.ee>

August 2003

# Sisukord

PEATÜKK 1. KASPERSKY ANTI-HACKER .....	5
1.1. Programmi otstarve ja põhifunktsioonid .....	5
1.2. Mida on uut versioonis 1.5.....	6
1.3. Tarnekomplekt .....	7
1.3.1. Mida sisaldab tarnekomplekt.....	7
1.3.2. Litsentsileping.....	7
1.3.3. Registreerimiskaart .....	8
1.4. Milliseid andmeid sisaldab kasutusjuhend .....	8
1.5. Kasutatavad tähistused .....	9
1.6. Teenused registreerunud kasutajatele.....	10
PEATÜKK 2. PROGRAMMI PAIGALDUS JA EEMALDAMINE .....	12
2.1. Nõuded kasutatavale süsteemile .....	12
2.2. Programmi paigaldus.....	13
2.3. Programmi eemaldamine .....	18
PEATÜKK 3. TÖÖ ALGUS.....	19
PEATÜKK 4. KASPERSKY ANTI-HACKER – INTERNETIST JA KOHTVÕRGUST LÄHTUVATE HÄKKERIRÜNNAKUTE VÄLTIMINE .....	22
4.1. Kaspersky Anti-Hackeri tööpõhimõtted.....	22
4.2. Turvatasemed .....	23
4.3. Seadistussoovitusi .....	25
PEATÜKK 5. PROGRAMMI KÄIVITAMINE JA SELLE KASUTAJALIIDES.....	28
5.1. Programmi käivitamine .....	28
5.2. Süsteemmenüü.....	29
5.3. Peaaken .....	30
5.4. Menüü .....	30
5.5. Tööriistariba.....	32

5.6. Tööpiirkond.....	34
5.7. Seisundiriba.....	34
5.8. Kontekstmenüü.....	34
5.9. Reeglite loomise viisard.....	35
5.10. Kasutajaliidese seadistuste muutmise ja säilitamine.....	35
5.11. Töö lõpetamine programmiga.....	37
<b>PEATÜKK 6. KAITSE AKTIVEERIMINE JA SEADISTAMINE.....</b>	<b>38</b>
6.1. Kaitse aktiveerimine ja turvaseme valimine.....	38
6.1.1. Kaitse aktiveerimine.....	38
6.1.2. Turvaseme valimine.....	40
6.1.3. Võrgusündmusest teavitav aken.....	41
6.1.4. Õpetusaken.....	41
6.1.5. Hoiatus täitmisefaili asendusest.....	43
6.2. Programmi toimingud rünnaku puhul.....	44
6.3. Rakenduste reeglite seadistamine.....	45
1.1.1. Töö reeglite loendiga.....	45
6.3.2. Uue reegli lisamine.....	48
6.3.2.1. Samm 1. Reegli seadistamine.....	48
6.3.2.2. Samm 2. Reegli täitmistingimused.....	52
6.3.2.2.1. Aadressi või aadresside vahemiku sisestamine.....	54
6.3.2.2.2. Pordi sisestamine.....	56
6.3.2.3. Samm 3. Täiendavad toimingud.....	58
6.4. Pakettide filtreerimise reeglite seadistamine.....	59
6.4.1. Töö reeglite loendiga.....	59
6.4.2. Uue reegli lisamine.....	62
6.4.2.1. Samm 1. Reegli rakendustingimuste sisestamine.....	62
6.4.2.2. Samm 2. Reegli nimetuse ja täiendavate toimingute sisestamine.....	65
6.5. Rünnakute detektor.....	66
1.1.1. Rünnakute detektori seadistusaken.....	66
6.5.2. Avastatavate häkkerirünnakute loend.....	68

PEATÜKK 7. PROGRAMMI TÖÖTULEMUSTE VAATAMINE .....	70
7.1. Jooksva seisundi vaatamine .....	70
7.1.1. Aktiivsete võrgurakenduste loend .....	70
7.1.2. Aktiivsete ühenduste loend.....	73
7.1.3. Avatud portide loend.....	76
7.2. Töö päevikutega .....	78
7.2.1. Päevikuteakna avamine .....	78
7.2.2. Päevikuteaken .....	79
7.2.2.1. Peamenüü.....	79
7.2.2.2. Aruandetabel.....	79
7.2.2.3. Järjehoidjad.....	80
7.2.3. Päeviku valimine .....	80
7.2.3.1. Võrgurünnakute päevik.....	80
7.2.3.2. Rakenduste aktiivsuse päevik.....	81
7.2.3.3. Pakettide filtreerimise päevik.....	82
7.2.4. Päevikuvalikute seadistamine .....	83
7.2.5. Päeviku säilitamine failis .....	84
LISA A. KASPERSKY LAB LTD.....	85
A.1. Kaspersky Lab'i antivirustooted .....	85
A.2. Meie kontaktandmed .....	88
LISA B. SELETAV SÕNASTIK.....	89
LISA C. KORDUMA KIPPUVAD KÜSIMUSED .....	90

# PEATÜKK 1. KASPERSKY ANTI-HACKER

## 1.1. Programmi otstarve ja põhifunktsioonid

*Mis on Kaspersky Anti-Hacker?*

Programm Kaspersky Anti-Hacker kujutab endast operatsioonisüsteemi Windows juhtimisel töötava arvuti ja sellel olevate andmete sanktsioneerimata juurdepääsu ning internetist ja lokaalvõrgust lähtuvate häkkerirünnakute eest kaitsvat personaalset võrkude vahelist ekraani.

Programm Kaspersky Anti-Hacker täidab alltoetletud funktsioone.

- Jälgib kõigi TCP/IP protokolliga töötavate rakenduste võrgukasutust Teie arvutil. Avastades mõne rakenduse sooritava kahtlase toimingu teavitab programm sellest Teid, blokeerides ühtlasi antud rakendusele juurdepääsu võrgule, mille tulemusena tagatakse Teie arvutil säilitatava informatsiooni konfidentsiaalsus. Näiteks, kui "trooja" programm püüab edastada Teie andmeid interneti vahendusel kurjategijale, blokeerib Kaspersky Anti-Hacker kahjurprogrammi juurdepääsu võrgule.
- SmartStealth™ tehnoloogia raskendab arvuti välist avastamist, mille tulemusena kaotavad häkkerid rünnakuobjekti ning kõik nende katsed arvutile tungida on määratud läbikukkumisele. Samuti aitab see vältida igat tüüpi DoS (Denial of Service) rünnakuid, osutamata samal ajal mitte mingit negatiivset mõju Teie internetikasutusele, tagades standardse läbipaistvuse ja info kättesaadavuse.
- Blokeerib levinuimad võrgust lähtuvad häkkerirünnakud tänu pidevale siseneva ja väljuva liikluse filtreerimisele ning hoiatab neist kasutajat.
- Tuvastab (tavaliselt tõsisematele rünnetele eelnevaid) portide skaneerimiskatseid ja keelab edasise suhtluse ründava arvutiga.
- Võimaldab vaadata kõigi aktiivsete ühenduste, võrgurakenduste ja avatud portide loendeid ning katkestada vajadusel soovimatud ühendused.

- Võimaldab kasutada programmi sooritamata selleks keerulisi seadistusi. Programm toetab lihtsustatud administreerimist viiel turvasemel: Lubada kõik, Madal, Keskmine, Kõrge, Keelata kõik. Vaikimisi on sisse lülitatud Keskmine turvatase, mis seadistab iseõppimisfunktsiooni abil turvasüsteemi vastavalt Teie reaktsioonile ühele või teisele sündmusele.
- Vajadusel võib aga turvasüsteemi seadistada väga paindlikult, sealhulgas ka soovitud ning soovimatute võrguoperatsioonide filtreerimissüsteemi ja rünnakute detektorit.
- Võimaldab registreerida teatud võrguturvalisusega seotud sündmused soovitud detailiseeritusega spetsiaalsetes päevikutes.

Programmi võib kasutada iseseisva tootena või kombineeritult teiste **Kaspersky Lab Ltd.** lahendustega.



**Tähelepanu!** Kaspersky Anti-Hacker ei kaitse Teie arvutit sellel säilitatavaid andmeid rikkuda ja hävitada võivate viiruste ja kahjurprogrammide eest. Selleks soovitame Teil kasutada Kaspersky Anti-Virus Personali.

## 1.2. Mida on uut versioonis 1.5

*Mis muutus versioonis 1.5. Uued võimalused*

Programmi uus versioon:

- toetab ADSL-moodemeid;
- toetab täielikult **Nähtamatuse režiimi** (läbitud testid aadressil [www.pcflank.com](http://www.pcflank.com));
- avastab uusi võrgurünnakuid: SmbDie, Helkern ja Lovesan;
- võimaldab kasutada pakettide filtreerimise ja rakenduste reeglites portide vahemikku;
- lihtsustatud on programmi esialgset seadistamist alandamata sealjuures arvuti kaitsetaset: enamkasutatavatele rakendustele on vaikimisi lubatud nende tüübile vastav võrguaktiivsus;

- parandatud on kasutajaliidest: op-süsteemis Windows XP toetatakse XP-stiili; reeglite tööloendite suurus on muudetav; uue reegli lisamiseks võib kasutada klahvi <Ins>.

## 1.3. Tarnekomplekt

*Mida sisaldab tarnekomplekt.*

*Litsentsileping. Registreerimiskaart*

### 1.3.1. Mida sisaldab tarnekomplekt

Tarkvaratoote tarnekomplekti kuuluvad:

- pitseeritud ümbrik CD plaadiga, millele on salvestatud tarkvaratoote failid;
- kasutusjuhend;
- võtmediskett või paigaldus CD-le salvestatud võtmefail;
- registreerimiskaart (toote seerianumbriga);
- litsentsileping.



Enne CD plaati (või diskette) sisaldava ümbriku avamist tutvuge tähelepanelikult litsentsilepinguga.

### 1.3.2. Litsentsileping

Litsentsileping on Teie ja Kaspersky Lab Ltd. vaheliseks juriidiliseks kokkuleppeks, kus on näidatud, millistel tingimustel võite kasutada Teie poolt soetatud tarkvaratoodet.

Lugege litsentsileping tähelepanelikult läbi!

Litsentsilepingu tingimustega mittedõustumisel võite tagastada karbi Kaspersky Anti-Hackeriga edasimüüjale, kellelt Te selle soetasite ja saada tagasi selle eest makstud summa. Sealjuures ei tohi olla avatud paigaldus CD-d (või diskette) sisaldav ümbrik!

CD-d (või diskette) sisaldava ümbriku avamine tähendab Teie poolset litsentsilepingu allkirjastamist ja nõustumist kõigi selle tingimustega.

### 1.3.3. Registreerimiskaart

Palun täitke registreerimiskaardi ärarebitav konts näidates sellel võimalikult täpselt oma andmed: ees- ja perekonnanime, telefoni, e-posti aadressi (kui on), ja saatke see siis edasimüüjale, kellelt Te antud tarkvaratoote soetasite.

Oma tava või e-posti aadressi või telefoni hilisemal muutumisel teatage sellest kindlasti asutusele, kuhu Te saatsite registreerimiskaardi ärarebitava kontsu.

Registreerimiskaart on dokument, mis teeb Teist meie kompanii registreerunud kasutaja ja annab õiguse toote kasutusvõtme kehtivusaja vältel saada tehnilist tuge ja teavet Kaspersky Lab Ltd. uutest tarkvaratoodetest ja uutest maailmas ilmunud viirustest (antud teenust pakutakse meie kodulehel [www.kaspersky.ee](http://www.kaspersky.ee) uudistelistiga liitunud kasutajatele).

## 1.4. Milliseid andmeid sisaldab kasutusjuhend

*Milliseid küsimusi valgustatakse antud kasutusjuhendis*

Käesolev kasutusjuhend sisaldab programmi Kaspersky Anti-Hacker paigalduseks, seadistamiseks ja ekspluatatsiooniks vajalikke andmeid ning koosneb järgmistest peatükkidest:


Peatüki nimetus	Lühikirjeldus
Kaspersky Anti-Hacker	Toote tutvustus, tarnekomplekti ja kasutusjuhendi struktuuri kirjeldus
Programmi paigaldus ja eemaldamine	Nõuded, millele peab vastama kasutatav arvuti. Paigaldus- ja eemaldusprotseduuride kirjeldus
Töö algus	Kuidas alustada tarkvaratoote kasutamist. Kaitsesüsteemi loomise näidis





Peatüki nimetus	Lühikirjeldus
Kaspersky Anti-Hacker – internetist ja kohtvõrgust lähtuvate häkkerirünnakute vältimine	Tarkvaratoote tööpõhimõtted. Peamiste mõistete ja lahendatavate ülesannete kirjeldus
Programmi käivitamine ja selle kasutajaliides	Programmi peaaakna avamine ja selle kasutajaliides
Kaitse aktiveerimine ja seadistamine	Kaitse aktiveerimine. Kaitsevalikute - pakettide filtreerimise ja rakenduste reeglite seadistamine
Programmi töötulemuste vaatamine	Võrgurünnakute, rakenduste aktiivsuse ja pakettide filtreerimise päevikute ning avatud portide, aktiivsete ühenduste ja võrgurakenduste loenditega tutvumine
Lisa A. Kaspersky Lab Ltd.	Kaspersky Lab Ltd. üldandmed. Kontaktinfo
Lisa B. Seletav sõnastik	Kasutusjuhendis kasutatavate mõistete seletav sõnastik
Lisa C. Korduma kippuvad küsimused	Vastused kasutajate poolt sageli esitatavatele küsimustele

## 1.5. Kasutatavad tähistused

*Kasutusjuhendis kasutatud erinevate tähistuste mõtteline tähendus*

Kasutusjuhendis on kasutatud erinevaid kujunduselemente sõltuvalt mõningate lõikude mõttest ning need on toodud koos selgitustega allolevas tabelis.

Kujundus	Mõtteline tähendus
<b>Rasvane kiri</b>	Menüüde, menüüelementide, akende ja nende elementide nimetused jne.
 Märkus.	Täiendav info, märkused.

Kujundus	Mõtteline tähendus
 Tähelepanu	Info, millele tuleb pöörata erilist tähelepanu.
 Programmi käivitamiseks: <ol style="list-style-type: none"> <li>1. Samm 1.</li> <li>2. ...</li> </ol>	Täidetavate sammude jada ja võimalike toimingute kirjeldus.
 Ülesanne:	Ülesande püstitamine seadistuste, funktsionaalsuse jne. realiseerimise näitena.
 Lahendus	Püstitatud ülesande lahendus.

## 1.6. Teenused registreerunud kasutajatele

### *Registreerunud kasutajatele võimaldatavad teenused*

Kaspersky Lab Ltd. pakub oma legaalsetele kasutajatele laia valikut Kaspersky Anti-Hackeri kasutamiseefektiivsust suurendavaid teenuseid.

Toote soetamisel saate Te selle registreerunud kasutajaks ja võite kasutusvõtme kehtivusaja vältel saada järgmisi teenuseid:

- antud tarkvaratoote uusi versioone;
- konsultatsiooni antud tarkvaratoote paigalduse, seadistamise ja kasutamisega seotud küsimustes e-posti teel;
- teavet Kaspersky Lab Ltd. uutest tarkvaratoodetest ja uutest maailmas ilmunud viirustest (antud teenust pakutakse meie kodulehel [www.kaspersky.ee](http://www.kaspersky.ee) uudistelisticga liitunud kasutajatele).



Operatsioonisüsteemide ja mitmesuguste teiste tehnoloogiate töö ja kasutamisega seotud konsultatsioone me ei teosta.



# PEATÜKK 2. PROGRAMMI PAIGALDUS JA EEMALDAMINE

## 2.1. Nõuded kasutatavale süsteemile

*Kasutatavale raud- ja tarkvarale  
esitatavate nõuete loetelu*

**Kaspersky Anti-Hackeri** tööks on vajalik:

- personaalarvuti sellele paigaldatud operatsioonisüsteemiga Microsoft Windows 98/ME/NT 4.0/2000/XP;
- op-süsteemide Microsoft Windows NT 4.0/2000/XP korral peavad programmi paigaldajal olema antud arvuti administraatori õigused;
- paigaldatud TCP/IP protokolliga tugi;
- võrgu- (Ethernet) või sissehelistamisühenduse olemasolu;
- paigaldatud vähemalt Microsoft Internet Explorer 5.0 või soovitatavalt uuem versioon;
- mitte vähem, kui 50 Mb kõvakettaruumi programmifailidele ja täiendavalt soovitava suurusega päevikufailidele;
- **op-süsteemide Windows® 98/Me/NT 4.0 kasutamisel:**
  - op-süsteemide Windows 98 ja Windows NT 4.0 korral Intel Pentium® 133MHz või kiirem protsessor;
  - op-süsteemi Windows Me korral Intel Pentium® 150MHz või kiirem protsessor;

- 32 Mb operatiivmälu;
- **op-süsteemi Windows NT 4.0 Workstation kasutamisel peab olema paigaldatud Service Pack v. 6.0 või uuem;**
- **op-süsteemi Windows 2000 kasutamisel:**
  - Intel Pentium 133MHz või kiirem protsessor;
  - 64 Mb operatiivmälu;
- **op-süsteemi Windows XP kasutamisel:**
  - Intel Pentium 300MHz või kiirem protsessor;
  - 128 Mb operatiivmälu.

## 2.2. Programmi paigaldus

*Paigaldusprotseduur.*

*Paigaldusviisard*

Tarkvaratoote paigaldamiseks käivitage CD-plaadil olev programm Setup.exe. Paigaldusprogramm töötab dialoogirežiimis. Iga dialoogiaken sisaldab teatud nuppe paigaldusprotsessi juhtimiseks. Alljärgnevalt selgitame peamiste nuppude otstarvet:

- **OK** – toimingu rakendamine;
- **Tühistada** – toimingu tühistamine;
- **Edasi** – üleminek järgmisele sammule;
- **Tagasi** – tagasipöördumine eelmisele sammule.



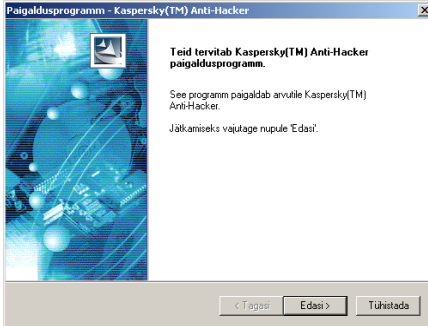
Enne programmi Kaspersky Anti-Hacker paigaldust arvutile on soovitatav sulgeda kõik arvutil töötavad rakendused.

### Samm 1. Üldinfo lugemine

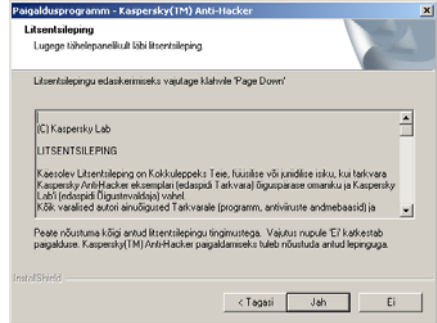
Paigaldusviisardi esimene dialoogiaken (joonis 1) sisaldab tarkvarapaketi Kaspersky Anti-Hacker üldandmeid.

## Samm 2. Litsentsilepingu lugemine

Dialogiaken **Litsentsileping** (joonis 2) sisaldab litsentsilepingu teksti. Lugege see läbi ning lepingutingimustega nõustumisel vajutage nupule **Jah**. Vastupidisel juhul vajutage nupule **Ei** ning katkestage paigaldus.

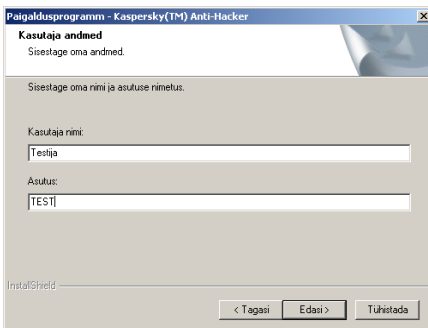


Joonis 1. Paigaldusviisardi esimene dialogiaken



Joonis 2. Dialogiaken **Litsentsileping**

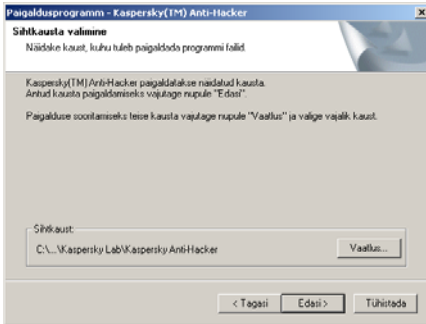
## Samm 3. Kasutaja andmete sisestamine



Joonis 3. Dialogiaken **Kasutaja andmed**

Dialogiaknas **Kasutaja andmed** (joonis 3) sisestage antud tarkvaratoote kasutaja andmed. Väljas **Kasutaja nimi** - oma nimi ja väljas **Organisatsioon** - asutuse nimetus. Vaikimisi asub neis väljades Windowsi registrist võetud info.

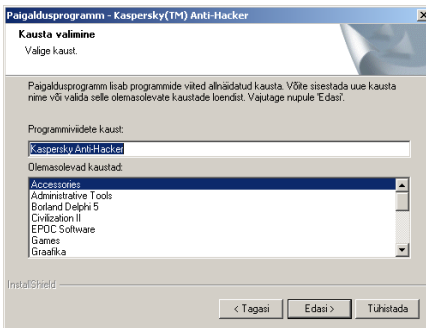
## Samm 4. Paigalduskausta valimine



Joonis 4. Dialoogiaken **Sihtkausta valimine**

Dialoogiaknas **Sihtkausta valimine** (joonis 4) sisestage väljas **Sihtkaust** Kaspersky Anti-Hackeri komponentide paigalduseks sobiv kaust, milleks kasutage nuppu **Vaatus**.

## Samm 5. Programmigrupi nimetuse sisestamine

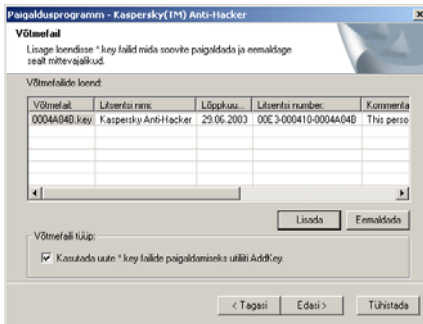


Joonis 5. Dialoogiaken **Kausta valimine**

Dialoogiaknas **Kausta valimine** (joonis 5) sisestage standardsesse programmimenüüsse **Programs** loodava paketi Kaspersky Anti-Hacker käivitamiseks mõeldud programmigrupi nimi ja vajutage seejärel nupule **Edasi**.

## Samm 6. Võtmefailide näitamine

Dialoogiaknas **Võtmefail** (joonis 6) tuleb näidata võtmefaili (\*.key faili) nimi ja asukoht.



Joonis 6. Dialoogiaken **Võtmefail**

Kui antud fail asub kaustas, kust toimub paigaldus, kuvatakse see automaatselt **Võtmefailide loendis**.

Kui võtmefail asub mingis teises kaustas, siis vajutage nupule **Lisada** ning näidake avanevas standardses dialoogiaknas **Võtmefaili valimine** vajalik nimi ja tee. Vajadusel võib kasutada korruga mitut võtmefaili.

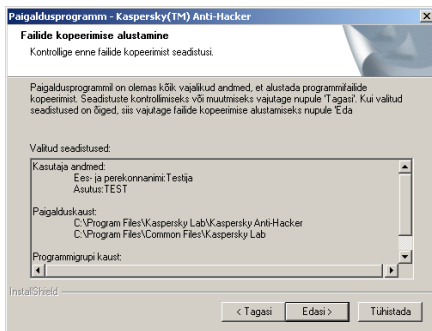
Soovitame Teil lülitada sisse märkeruudu **Kasutage võtmefailide (\*.key) paigaldamiseks utiliiti AddKey, mis võimaldab paigaldada uued võtmefailid topeklõpsuga nende nimedel**. Vastasel juhul tuleb Teil uus paigaldatav võtmefail käsitsi üldfailide kausta kopeerida.

Võtmefail on Teie isiklikuks "võtmeks", milles asub kogu *Kaspersky Anti-Hackeri* tööks vajalik teenistuslik informatsioon ja nimelt:

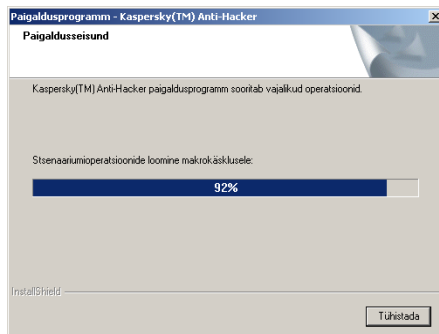
- antud versiooni müüja andmed (firma nimetus, adressid, telefonid);
- tehnilise toe andmed (kes teostab ja kust seda võib saada);
- toote väljalaske kuupäev;
- litsentsi nimetus ja number;
- antud litsentsi kehtivusaeg.

## Samm 7. Failide kopeerimine kõvakettale

Dialoogiaknas **Failide kopeerimise algus** (joonis 7) lugege läbi paigaldusinfo ja vajadusel selles midagi muuta pöörduge nupu **Tagasi** abil tagasi vajalikku dialoogiaknasse. Juhul, kui kogu informatsioon on sisestatud õieti, vajutage nupule **Edasi** ning algab failide kopeerimine arvuti kõvakettale, mida iseloomustavat teavet kuvatakse dialoogiaknas **Paigaldusseisund** (joonis 8).



Joonis 7. Dialoogiaken **Failide kopeerimise algus**



Joonis 8. Dialoogiaken **Paigaldusseisund**

## Samm 8. Paigalduse lõpetamine

Peale paketi Kaspersky Anti-Hacker paigalduse lõppu ilmub ekraanile dialoogiaken **Paigalduse lõpetamine** (joonis 9).



Joonis 9. Dialoogiaken **Paigalduse lõpetamine**

Paigaldusprotsessi korrektseks lõpetamiseks tuleb arvuti restartida. Valige variant **Jah, restartida arvuti kohe praegu** arvuti koheseks restartimiseks või **Ei, restartida arvuti hiljem**, kui soovite arvuti hiljem restartida. Seejärel vajutage nupule **Valmis**.

## 2.3. Programmi eemaldamine

### *Programmi eemaldamine arvutilt*



Programmi Kaspersky Anti-Hacker arvutilt eemaldamiseks sooritage järgmised toimingud:

1. Vajutage **Windowsi** tegumiribal olevale **Start** nupule ja avanevas menüüs valige alammenüü **Programms**.
2. Seejärel avage programmi Kaspersky Anti-Hacker alammenüü, mida vaikinisi nimetatakse **Kaspersky Anti-Hacker**, kuid mis võis olla programmi paigaldamisel ka muudetud. Antud menüüs valige korraldus **Kaspersky Anti-Hacker Uninstall**.
3. Kui soovite Kaspersky Anti-Hackeri tõesti eemaldada, siis vajutage dialoogiaknas olevale nupule **Jah**. Vastupidisel juhul nupule **Ei**.




Programmi võite eemaldada ka standardsest **Control Panelilt** avatavast aknast **Add or Remove Programs**.

# PEATÜKK 3. TÖÖ ALGUS

*Töö algus programmiga.  
Turvasüsteemi loomise näidis*

Peale programmi paigaldust ja arvuti restarti turvasüsteem rakendub ja faktiliselt juba alates sellest hetkest tõkestab Kaspersky Anti-Hacker Teie arvuti vastu sooritatavaid ründeid ja sellele paigaldatud rakenduste lubamatut suhtlust interneti või kohtvõrguga.

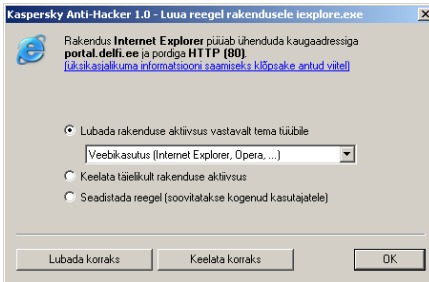
Sisenenud süsteemi, teete oma tööd nagu tavaliselt. Võrgusuhtluse puudumisel teavitab programmi olemasolust Teie arvutil üksnes tegumiribal asuv ikoon . Klõpsates sellel hiirega võite avada programmi peaakna ja vaadata informatsiooni aktiivsest turvasemest ning seda muuta (peaakna üksikasjalik kirjeldus on toodud punktis 5.3 lk. 30). Vaikimisi töötab programm **Keskmisel** turvasemel, mis loob kaitsesüsteemi seadistamiseks kõige lihtsamad võimalused. Enamikel juhtudel ei tule teil seda ise seadistada: enamkasutatavamatele rakendustele on vaikimisi lubatud nende tüübile vastav võrguaktiivsus. Kuid mõningates olukordades tuleb kaitsesüsteem seadistada käsitsi. Alljärgnevalt vaatleme seda protsessi üksikasjalikumalt.



**Ülesanne.** Oletame, et Teie arvuti on ühendatud internetiga ning Te käivitasite programmi Microsoft Internet Explorer ja sisestasite veebilehe [www.kaspersky.com](http://www.kaspersky.com) aadressi. Seejärel ilmub Teie arvuti ekraanile teade **Luua reegel rakendusele IEXPLORER.EXE** (joonis 10).

Akna ülaosas on kuvatud programmi Microsoft Internet Explorer ikoon ja nimi, veebilehe [www.kaspersky.com](http://www.kaspersky.com) aadress ja ühenduse loomiseks kasutatava pordi number. Üksikasjalikumalt informatsiooni ühenduse kohta võite vaadata klõpsates hiirega allajoonitud viitel (joonis 11).

Seni, kuni Te ei ole programmile näidanud, kuidas toimida, võrguühendust ei looda. Teil tuleb reageerida programmi poolt väljastatud teatele.



Joonis 10. Turvasüsteemi õpetusaken



Joonis 11. Ühenduse andmed



Selleks sooritage järgmised toimingud.

1. Valige nupp **Lubada rakenduse aktiivsus vastavalt tema tüübile** ja selle all olevast ripploendist rida **Veebikasutus**.
2. Vajutage nupule **OK**.

Seejärel lubab Kaspersky Anti-Hacker programmil Microsoft Internet Explorer ühenduda ning ühtlasi lubatakse talle ka kõik järgnevad veebibrauserile iseloomulikud võrguühendused.


Nagu Te ülesande täitmise käigus võisite märgata, sisaldab aken **Luu reegel rakendusele IEXPLORER.EXE** kolme alloletatud toiminguvarianti.

- **Lubada rakenduse aktiivsus vastavalt tema tüübile** (Teie poolt antud juhul valitud variant) – lubab sündmuse initsieerinud rakendusele selle tüübile vastava iseloomuga võrgusuhtluse. Tüüp valitakse valikunupu all olevast ripploendist. Võite lubada rakendusele ka igasuguse aktiivsuse, kui valite väärtuse **Kõik lubatud**.
- **Keelata täielikult rakenduse aktiivsus** – keelab sündmuse initsieerinud rakendusele sooritada nii antud, kui ka kõiki tulevasi võrguoperatsioone.

- **Seadistada reegel** – lubab rakendusel sooritada nii antud operatsiooni, kui ka kõik tulevased analoogsed võrguoperatsioonid. Võrguoperatsiooni tingimused tuleb kinnitada peale vajutust nupule **OK** avanevas reeglite viisardis (viisardist vt. p. 6.3.2 lk. 48).


Kui Te ei tea, millist varianti valida, võite vajutada nupule **Lubada korra**ks või **Keelata korra**ks ja jälgida võrgupääsu taotleva rakenduse edasist käitumist.



Õpetusakna sulgemisel vajutusega selle paremas ülannurgas olevale nupule , keelatakse vaidlusalune operatsioon ühekordselt.

Nii toimides võite seadistada töö käigus oma arvuti turvasüsteemi just täpselt vastavaks oma vajadustele.



Sisestatud reeglite loendit võite näha, kui valite menüüs **Teenindus** korralduse **Rakenduste reeglid** või vajutate tööriistaribal olevale nupule .

Soovitame töötada programmi esimestel kasutusnädalatel **Keskmisel** turvasemel, et õpetada programmi Teie poolt standardsete võrguoperatsioonide sooritamise käigus neile õieti reageerima ja luua neile lubavad reeglid.

Peale õppeperioodi lõppu võite viia programmi üle **Kõrgele** turvasemele, kindlustades end nii igasuguste sanktsioneerimata võrgusündmuste ja häkkerirünnakute eest. Kuid pidage meeles, et seejärel paigaldatavatele rakendustele on juurdepääs võrgule vaikimisi suletud ning Teil tuleb Kaspersky Anti-Hackeri täiendavaks õpetamiseks see ajutiselt **Keskmisele** turvasemele tagasi viia või luua uutele rakendustele vajalikud reeglid käsitsi.

# PEATÜKK 4. KASPERSKY ANTI-HACKER – INTERNETIST JA KOHTVÕRGUST LÄHTUVATE HÄKKERIRÜNNAKUTE VÄLTIMINE

## 4.1. Kaspersky Anti-Hackeri tööpõhimõtted

*Kuidas töötab Kaspersky Anti-Hacker? Rakenduste reeglid.  
Pakettide filtreerimise reeglid.  
Rünnakute detektor*

Kaspersky Anti-Hacker kaitseb Teie arvutit võrgust tulevate rünnakute eest ning tagab Teie andmete konfidentsiaalsuse, kontrollides selleks kõiki Teie arvutil sooritataavaid võrguoperatsioone. Võrguoperatsioone on kahte liiki:

- operatsioonid rakenduste tasandil (kõrgtasandilised). Antud tasandil analüüsib Kaspersky Anti-Hacker selliste rakenduste nagu veebibrauserid, postiprogrammid, failvahetusprogrammid jne. aktiivsust;
- operatsioonid pakettide tasandil (madalatasandilised). Antud tasandil analüüsib Kaspersky Anti-Hacker vahetult Teie võrgukaarti või modemi läbivaid andmepakette.

Kaspersky Anti-Hackeri seadistamine seisneb võrguoperatsioonide filtreerimisreeglite kirjeldamises. Osa filtreerimisalasesest tööst teostatakse automaatrežiimis rünnakute detektoriga, mis avastab portide skaneerimise, DoS

rünnakud jne. ning võib vajadusel ründaja blokeerida. Lisaks sellele võite kirjeldada ka oma individuaalsed filtreerimisreeglid tagamaks oma arvuti tugevdatud kaitset.

Kumbagi võrguoperatsioonide liigi jaoks on Kaspersky Anti-Hackeris ette nähtud oma spetsiaalne reeglite loend.

- *Rakenduste reeglid* võimaldavad lubada igale konkreetsele rakendusele üksnes sellele spetsiifilise aktiivsuse. Vajadusel võite luua igale rakendusele suvalise hulga reegleid. Teie poolt antud reeglitele mittevastavate võrguoperatsioonide avastamisel programm hoiatab Teid ning võimaldab vajadusel soovimatud toimingud blokeerida (**Keskmisel** turvatasemel). Kõige lihtsamalt saab sellise reegli kirjeldada tuvastades, mis tüüpi rakendusega on tegemist ja kohaldades talle antud tüüpi rakenduste üldreegleid (tüüpide loend ja kirjeldus on toodud p. 6.3.2.1 lk. 48). Teine viis on määratleda antud rakendusele suhtluseks lubatud kaugteenistuste aadressid ja selleks kasutatavad pordid.
- *Pakettide filtreerimise reeglid* võimaldavad lasta läbi või blokeerida Teie arvutile saabuvaid või sellelt saadetavaid andmepakette. Otsus tehakse paketi pealdise: kasutatava protokoll, pordinumbrite, IP-aadresside jne. analüüsi alusel. Pakettide filtreerimise reegleid kohaldatakse eranditult kõigile rakendustele. Näiteks, kui blokeerisite pakettide filtreerimise reeglites mõne IP-aadressi, siis on suhtlus antud aadressiga täielikult keelatud.



Pakettide filtreerimise reeglid on kõrgema prioriteediga, kui rakenduste reeglid ning programm täidab need esmajärjekorras. Näiteks, kui blokeerisite pakettide filtreerimise reegluga kõik sisenevad ja väljuvad paketid, siis ei arvestata võrguoperatsioonide filtreerimisel ühtegi rakenduste reeglit.

## 4.2. Turvatasemed

*Milliseid turvatasemed saab kasutada Kaspersky Anti-Hackeris?*

Programm võimaldab valida ühe viiest turvatasemest.

- **Kõik lubatud** – Teie arvuti kaitse on välja lülitatud. Antud tasemel on lubatud igasugune võrguaktiivsus.
- **Madal** – lubatud on kõigi rakenduste võrguaktiivsus, peale nende, mis ei ole keelatud otseselt rakenduste reeglitega.

- **Keskmine** – programm teavitab Teid rakenduste võrguaktiivsusest võimaldades seadistada turvasüsteemi vastavalt Teie vajadustele, kasutades selleks iseõppimismehhanismi. Ekraanile väljastatakse rakenduse ja selle poolt sooritatava võrguoperatsiooni andmed ning palutakse Teil otsustada, kas antud operatsioon ühekordselt blokeerida või lubada, keelata täielikult rakenduse aktiivsus, lubada see vastavalt rakenduse tüübile või seadistada võrgusuhtluse täiendavad valikud. Teie vastuse alusel võib programm formeerida antud rakendusele edaspidi automaatselt kohaldatava reegli.
- **Kõrge** – programm lubab kasutada võrku ainult rakendustel, millistele see on otseselt reeglites lubatud. Antud turvasemel õpetusaken ekraanile ei ilmu ja kõik reeglites sanktsioneerimata ühendused on keelatud.



**Pidage meeles, et peale Kõrge turvaseme valimist paigaldatud võgurakendused vaikimisi interneti ei pääse.**

- **Kõik keelatud** – Teie arvuti juurdepääs võrgule on täielikult blokeeritud. Antud turvatase on analoogne arvuti füüsilisele lahutamisele internetist ja/või kohtvõrgust.



Turvasemetel **Kõrge**, **Keskmine** ja **Madal** võite muuta oma arvuti ka **Väljast nähtamatuks** (vt. p. 5.6 lk. 34). Antud režiimis on lubatud vaid kasutaja algatatud võrguliiklus ja kogu ülejäänud võrguaktiivsus (kaugühendumine Teie arvutiga, kontrollimine utiliidiga ping jne.) on keelatud, kui seda ei luba otseselt kehtestatud filtreerimisreeglid.

Faktiliselt tähendab see seda, et Teie arvuti muutub väliskeskonna jaoks "nähtamatuks" ning häkkerid kaotavad rünnakuobjekti ja kõik nende katsed saada juurdepääsu Teie arvutile on määratud läbikukkumisele. Lisaks sellele aitab antud režiim hoida ära ka igasugust tüüpi DoS (Denial of Service) rünnakuid.

Samas ei kahjusta nähtamatuse režiim vähimalgi määral Teie internetikasutust: Kaspersky Anti-Hacker lubab Teie arvuti poolt algatatud võrguaktiivsuse.



Rünnakute detektor on aktiivne kõigil turvasemetel peale taseme **Kõik lubatud**, kuid vajadusel võite selle ka välja lülitada (vt. p. 6.5.1 lk. 66).

## 4.3. Seadistussoovitusi

*Kuidas valida turvatase ja seadistada reeglid erinevates situatsioonides?*

Milliseid Kaspersky Anti-Hackeri komponente on soovitatav kasutada ja milline turvatase valida? Vastus antud küsimusele sõltub Teie ees seisvast ülesandest.



## Ülesanne 1. Andmete kaitsmine internetist tuleva kuritegeliku ründe eest.



On olemas kaks peamist moodust, kuidas kurjategijad pääsevad kahjustama või röövima kasutaja arvutit salvestatavaid andmeid – tungides arvutile tarkvaravigu kasutades või nakatades arvuti trooja programmidega.

Juhul, kui saate teada veast mõnes Teie arvutile paigaldatud programmis, looge selle jaoks keelav reegel. Soovitame Teil seadistada iseseisvalt selle vea iseärasusi arvestava keelava reegli (vt. p. 6.3.2.1 lk. 48).

Kui Teie arvutile on disketi või e-posti vahendusel sattunud trooja programm, mis püüab Teie andmeid interneti kaudu kurjategijale edastada, siis tagab Kaspersky Anti-Hacker raskusteta Teie andmete säilivuse kas keelustades antud operatsiooni (**Kõrgel** turvatasemel) või väljastades sellekohase hoiatuse (**Keskmisel** turvatasemel).



**Tähelepanu!!!** Kaspersky Anti-Hacker ei kaitse Teie arvutit viiruste ja kahjurprogrammide eest.

Näiteks võib trooja programm kasutada Teie andmete kurjategijale edastamiseks standardset postiprogrammi ning sellist tegevust ei suuda Kaspersky Anti-Hacker takistada. Lisaks võivad Teie arvutile sattunud viirused ja kahjurprogrammid hävitada sellel säilitatavad andmed ning muuta Teie arvuti viiruste edasise leviku allikaks. Ka sel juhul suudab Kaspersky Anti-Hacker nakatumise tagajärgi vaid osaliselt vältida. Efektiveks viiruste ja kahjurprogrammide vastaseks kaitseks soovitame kasutada Kaspersky Anti-Hackerit koos antiviiusprogrammiga Kaspersky Anti-Virus Personal / Personal Pro. Lisaks sellele soovitame rakenduste reeglite loendis lubada rakendustel sooritada üksnes rangelt neile omaseid ja vajalikke võrguoperatsioone, et minimeerida sanktsioneerimata võrguoperatsioonide täitmise riski Teie arvutit.

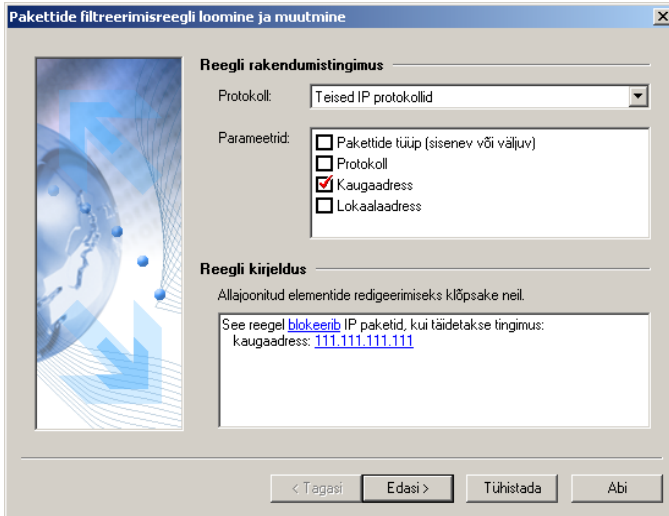


## Ülesanne 2. Kahtlaste internetiaadresside blokeerimine, kui on alust arvata, et neilt aadressidelt sooritatakse ründeid Teie arvutile.



Oma arvuti suhtluse keelustamiseks kahtlaste kaugaadressidega looge vastavad pakettide filtreerimise reeglid. Näiteks on joonisel 12 antud reegel, mis võimaldab täielikult blokeerida aadressi "111.111.111.111".

Ründesituatsioonide profülaktikaks on soovitatav hoida sõltumata valitud turvatasemest pidevalt sisse lülitatuna rünnakute detektor.



Joonis 12. Kahtlase aadressi blokeerimise reeglid



Programmi Kaspersky Anti-Hacker kasutamise huvitava näitena võib nimetada veebilehtedel kuvatavate bannerite blokeerimist. Sisestage pakettide filtreerimise reeglitesse keeld ühenduda bannerite laadimiseks kasutatavate veebilehtedega (näiteks [linkexchange.ru](http://linkexchange.ru)).



**Ülesanne 3. Kohtvõrgu operatsioonide kontrollimine, et kaitsta arvutit ja isiklikku infot võimalike rünnete eest kohtvõrgust.**



Arvuti suhtlus kohtvõrguga toimub operatsioonisüsteemi tasandil, mis ei võimalda nimetada alati seda teostavat rakendust. Sel juhul peate vajaliku kaitse tagamiseks looma vastavad pakettide filtreerimise reeglid.

Programmis Kaspersky Anti-Hacker on turvasüsteemi seadistamise hõlbustamiseks kehtestatud mõningad eelseadistatud lubavad pakettide filtreerimise reeglid ning sealhulgas on vaikumisi lubatud ka kohtvõrguoperatsioonid. Vajadusel võite muuta vaikumisi kehtestatud pakettide filtreerimise reegleid, et kas siis täielikult sulgeda juurdepääs oma arvutile kohtvõrgust või siis lubada seda ainult mõningatele arvutitele.

# PEATÜKK 5. PROGRAMMI KÄIVITAMINE JA SELLE KASUTAJALIIDES


*Programmi käivitusviisid. Peaaken,  
kasutajaliides ja selle seadistamine.  
Programmist väljumine*

## 5.1. Programmi käivitamine

Kaspersky Anti-Hacker käivitub automaatselt kasutaja süsteemi sisenemisel. Programmi mälust välja laadimisel võite selle uuesti käsitsi käivitada.



*Programmi Kaspersky Anti-Hacker käsitsi käivitamiseks,*

1. Vajutage Windowsi tegumiribal olevale **Start** nupule ja valige avanevas menüüs alammenüü **Programs**.
2. Seejärel valige selles programmigrupp Kaspersky Anti-Hacker, mis võib kanda ka mõnda teist programmi paigaldamisel antud nime. Avanevast alammenüüst valige korraldus **Kaspersky Anti-Hacker**.
3. Klõpsake vasaku hiireklahviga tegumiribale ilmunud ikoonil  või tehke seda parempoolse hiireklahviga ja valige avanevast süsteemmenüüst korraldus **Avada Kaspersky Anti-Hacker....**


Seejärel avaneb ekraanil programmi Kaspersky Anti-Hacker peaaken(vt. p. 5.3 lk. 30).



Programmi võib käivitada ka vahetult kaustast, kuhu see on paigaldatud. Selleks avage failihalduris (näiteks Windows Exploreris) programmi Kaspersky Anti-Hacker kaust (vaikimisi **C:\Program Files\Kaspersky Lab\Kaspersky Anti-Hacker**) ja leidnud seal faili **KAVPF.exe** klõpsake sellel kaks korda hiirega.

## 5.2. Süsteemmenüü

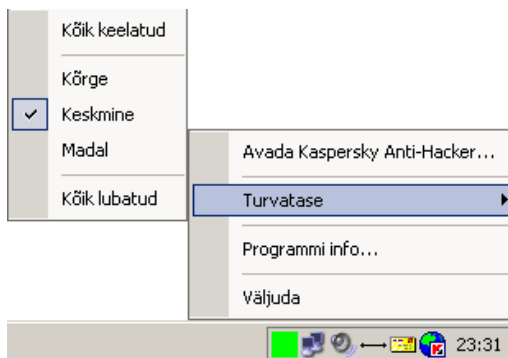
*Tegumiriba ikoon. Süsteemmenüü*

Peale programmi käivitamist ilmub tegumiriba parempoolsesse serva ikoon .

Klõpsates sellel parempoolse hiireklahviga võite avada järgmistest elementidest koosneva süsteemmenüü (joonis 13):

Tabel 1

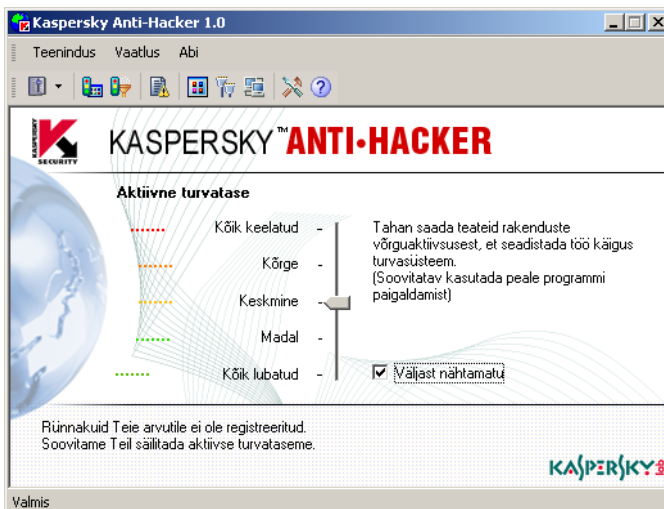
Menüüelement	Otstarve
Avada Kaspersky Anti-Hacker...	Avada programmi peaaken.
Turvatase	Turvataseme valimine: <b>Kõik keelatud, Kõrge, Keskmise, Madal, Kõik lubatud.</b> Turvatasemetest üksikasjalikumalt vt. p. 4.2 lk. 23.
Programmi info	Avada aken programmi ja kasutatavate võtmete üldandmetega.
Väljuda	Programmi mälust välja laadimine.



Joonis 13. Süsteemmenüü

## 5.3. Peaaken

Peale programmi käivitamist avaneb ekraanil selle peaaken (joonis 14). Programmi Kaspersky Anti-Hacker peaaken on mõeldud aktiivse turvatase valimiseks, jooksva kaitseseisundi vaatamiseks, võrguoperatsioonide filtreerimisreeglite muutmiseks ja päevikutega tutvumiseks.



Joonis 14. Kaspersky Anti-Hackeri peaaken

Programmi Kaspersky Anti-Hacker peaknas asuvad:

- menüü;
- tööriistariba;
- tööpiirkond;
- seisundiriba.

## 5.4. Menüü

Peakna ülasaosas asub *menüü*. Hiire abil võib seda teisaldada nii peaknas, kui väljaspool peakent.

Mõningad menüüelemendid on dubleeritud tööriistaribal olevate nuppudega. Tööriistariba nuppude vastavus menüüelementidega on toodud punktis 5.5 leheküljel 32.

Tabel 2

Menüüelement	Otstarve
Teenindus → Rakenduste reeglid	Avada rakenduste reeglite seadistamise aken.
Teenindus → Pakettide filtreerimise reeglid	Avada pakettide filtreerimise reeglite seadistamise aken.
Teenindus → Turvatase	<p>Valida turvatase:</p> <ul style="list-style-type: none"> <li>• Kõik keelatud;</li> <li>• Kõrge;</li> <li>• Keskmine;</li> <li>• Madal;</li> <li>• Kõik lubatud.</li> </ul> <p>Turvaseme võite valida ka programmi tööpiirkonnas. Üksikasjalikumalt vt. p. 4.2 lk. 23.</p>
Teenindus → Valikud	Avada päevikute, kaitse aktiveerimise ja rünnakute detektori seadistusaken.
Teenindus → Väljuda	Laadida programm mälust välja.
Vaatlus → Tööriistaribad	<p>Programmi kasutajaliidese seadistused:</p> <ul style="list-style-type: none"> <li>• <b>Üldine tööriistariba</b> – avada/sulgeda tööriistariba;</li> <li>• <b>Seadistada</b> – avada dialoogiaken kasutajaliidese seadistustega.</li> </ul>
Vaatlus → Seisundiriba	Avada/sulgeda seisundiriba.










Menüüelement	Otstarve
Vaatlus → Päevikud	Avada päevikuteaken ühega järgmistest päevikutest: <ul style="list-style-type: none"> <li>• <b>Võrgurünnakute päevik</b>;</li> <li>• <b>Rakenduste võrguaktiivsuse päevik</b>;</li> <li>• <b>Pakettide filtreerimise päevik</b>.</li> </ul>
Vaatlus → Näidata	Näidata: <ul style="list-style-type: none"> <li>• <b>Aktiivseid võgurakendusi</b> – käivitatud võgurakenduste loendit;</li> <li>• <b>Avatud porte</b> – avatud portide loendit;</li> <li>• <b>Aktiivseid ühendusi</b> – aktiivsete ühenduste loendit.</li> </ul>
Abi → Sisukord	Avada abisüsteem.
Abi → Programmi info...	Avada dialoogiaken programmi ja kasutatavate võtmete lühiaandmetega.
Abi → Kaspersky Anti-Hacker Internetis	Avada Kaspersky Lab'i veebileht

## 5.5. Tööriistariba

Menüüriba all asub *tööriistariba*. Soovi korral võite seda hiirega tirides teisaldada nii peaaknas, kui väljaspool peaakent.

Tööriistaribale on koondatud nupud, millele vajutades võite initsieerida ühtesid või teisi toiminguid. Tööriistariba võite ka ekraanilt eemaldada või taas avada, valides selleks menüüs **Vaatlus** alammenüü **Tööriistaribad** ja klõpsates seal korraldusel **Üldine tööriistariba**.

Tööriistal olevaid nuppe võite ka lisada või eemaldada (vt. p. 5.10 lk. 35).

Nupp	Menüüelement	Otstarve
	Teenindus → Turvatase	Valida turvatase: <ul style="list-style-type: none"><li>• Kõik keelatud;</li><li>• Kõrge;</li><li>• Keskmise;</li><li>• Madal;</li><li>• Kõik lubatud.</li></ul> Üksikasjalikumalt vt. p. 4.2 lk. 23.
	Teenindus → Rakenduste reeglid	Avada rakenduste reeglite seadistusaken.
	Teenindus → Filtreerimise reeglid	Avada pakettide filtreerimise reeglite seadistusaken.
	Vaatlus → Päevikud → Võrgurünnakute päevik	Avada aken võrgurünnakute päevikuga.
	Vaatlus → Näidata → Aktiivseid võgurakendusi	Näidata käivitatud võgurakenduste loendit.
	Vaatlus → Näidata → Avatud porte	Näidata avatud portide loendit.
	Vaatlus → Näidata → Aktiivseid ühendusi	Näidata aktiivsete ühenduste loendit.
	Teenindus → Valikud	Avada aken päevikute, kaitse aktiveerimise ja rünnakute detektori valikutega.
	Abi → Sisukord	Avada abisüsteem.

## 5.6. Tööpiirkond

Programmi tööpiirkonnas asub *turvatasemete skaala* ning süsteemi jooksva seisundi info.

Turvatasemete skaala võimaldab valida ühe viiest järgnevast tasemest:

- Kõik keelatud;
- Kõrge;
- Keskmine;
- Madal;
- Kõik lubatud.

Aktiivse turvataseme muutmiseks teisaldage skaalal olevat liugur, misjärel ilmub sellest paremale uue valitud turvataseme kirjeldus. Uus turvatase jõustub koheselt.

Tasemetel **Kõrge**, **Keskmine** ja **Madal** võite aktiveerida täiendava režiimi – **Väljast nähtamatu** (üksikasjalikumalt vt. p. 4.2 lk. 23).

Tööpiirkonna alaosas kuvatakse informatsiooni süsteemi jooksvast seisundist ja seal on toodud viimati registreeritud häkkerirünnaku andmed: selle toimumise kuupäev, kellaage, tüüp ja rünnanud arvuti aadress, kui see õnnestus tuvastada.

## 5.7. Seisundiriba

Peaakna alaosas asub *seisundiriba*, millel kuvatakse antud hetkel valitud peaakna elemendi spikrit. Võite seisundiriba sulgeda või taas avada valides selleks menüüs **Vaatlus** korralduse **Seisundiriba**.

## 5.8. Kontekstmenüü

Dialogiaknad omavad *kontekstmenüüd*, mille abil võib sooritada just neis akendes ja valitud elementidega sooritataavaid toiminguid.



*Kontekstmenüü avamiseks klõpsake paremat hiireklahvi.*

## 5.9. Reeglite loomise viisard

Reeglite loomise/redigeerimise viisard koosneb järjestikustest dialoogiakendest. Iga dialoogiaken sisaldab nuppe reegli lisamis- või redigeerimisprotsessi juhtimiseks. Alljärgnevalt selgitame nende otstarvet:

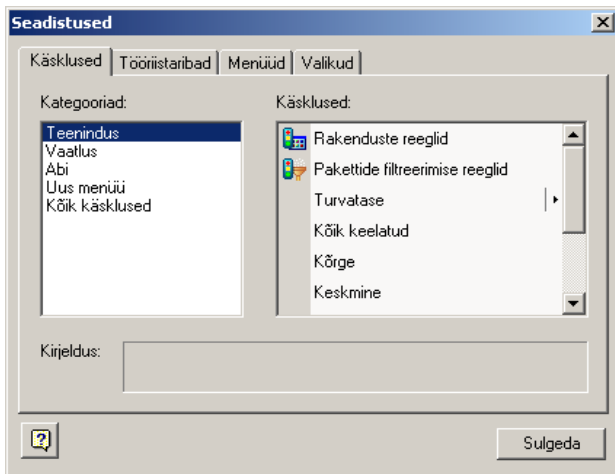
- **Valmis** – reegli loomine;
- **Tühistada** – reegli loomise tühistamine;
- **Edasi** – üleminek järgmisele sammule;
- **Tagasi** – tagasipöördumine eelmisele sammule.
- **Abi** – avada abisüsteem.

## 5.10. Kasutajaliidese seadistuste muutmine ja säilitamine



*Kasutajaliidese seadistuste muutmiseks valige menüüs **Vaatlus** alammenüü **Tööriistad** ja selles korraldus **Seadistada**.*

Ekraanil avaneb dialoogiaken **Seadistused** (joonis 15).

Joonis 15. Dialoogiaken **Seadistused**

Kasutajaliidese seadistuste muutmiseks on soovitatav paigutada aken **Seadistused** nii, et oleksid nähtavad nii tööriistariba, kui programmi peamenüü.

Lehel **Käsklused** võite muuta peamenüü ja tööriistariba konfiguratsiooni. Uue käskluse lisamiseks peate tirima selle hiirega loendist menüüle või tööriistaribale ning selle eemaldamiseks vastupidi toimima.

Lehtedel **Tööriistaribad** ja **Menüüd** võite taastada nende esialgse kuju.

Lehel **Valikud** võite aktiveerida või deaktiveerida tööriistariba nuppude spikrid, muuta nuppude suurust ning muuta menüüelementide järjestust.

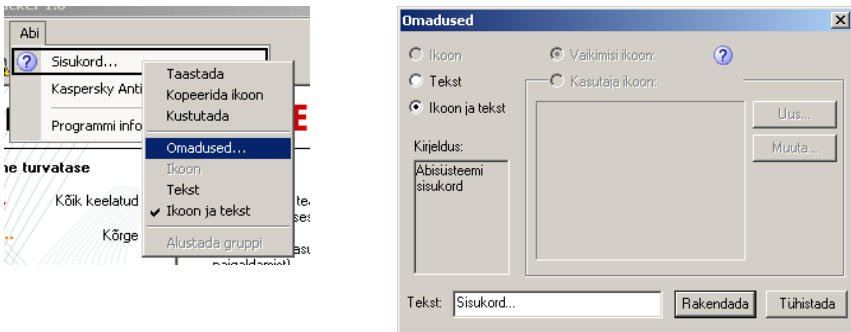
Soovi korral võite muuta ka peamenüü elementide ja nuppude nimetusi, näidata nuppe teksti- või ikoonidena.



*Peamenüü elemendi või tööriistariba nupu nimetuse ja/või teiste omaduste muutmiseks,*

1. Valige akent **Seadistused** sulgemata vajalik peamenüü element või tööriistariba nupp.
2. Vajutage parempoolsele hiireklahvile ning valige avanevas kontekstmenüüs soovitatav toiming:
  - **Kustutada** – kustutada element või nupp;


- **Omadused** – muuta nimetus. Avanevas samanimelises dialoogiaknas muutke väljas **Tekst** elemendi nimetus (joonis 16) ja vajutage nupule **Rakendada**.
- **Icoon** – kuvada ainult ikoon;
- **Tekst** – kuvada ainult tekst;
- **Icoon ja tekst** – kuvada nii ikoon, kui tekst;
- **Alustada gruppi** – lisada eraldaja.



Joonis 16. Käskluste omaduste redigeerimine

Kasutajaliidese seadistused säilitatakse automaatselt ja jõustuvad kohe peale nende muutmist.

## 5.11. Töö lõpetamine programmiga

Programmi mälust välja laadimiseks valige süstemmenüüs või programmi peakna menüüs **Teenindus** korraldus **Väljuda**. Programmi peakna võite sulgeda ka selle paremas ülanurgas oleva nupuga .




Kui märkeruut **Minimeerida** peakna sulgemisel tegumiribale on sisse lülitatud, siis programmi peakna sulgemisel mälust välja ei laeta. Vaikimisi on antud märkeruut sisse lülitatud, kuid vajadusel võite selle välja lülitada (vt. p. 6.1.1 lk. 38). Arvuti mälus töötavale programmile viitab selle tegumiribal asuv ikoon.

# PEATÜKK 6. KAITSE AKTIVEERIMINE JA SEADISTAMINE

## 6.1. Kaitse aktiveerimine ja turvataseme valimine

*Kuidas aktiveerida arvuti kaitset  
Kaspersky Anti-Hackeri abil? Kuidas  
valida turvataset?*

### 6.1.1. Kaitse aktiveerimine

Arvuti häkkerirünnakute vastane kaitse aktiveerub kohe peale programmi Kaspersky Anti-Hackeri paigaldamist ja arvuti restarti. Peale programmi käivitamist ilmub tegumiribale ikoon . Vaikimisi töötab programm **Keskmisel** turvatasemel. Juhul, kui mõni rakendus püüab suhelda kohtvõrgu või internetiga ilmub ekraanile programmi õpetusaken rakenduse ja selle loodava ühenduse andmetega ning päringuga kasutajale, kuidas toimida: kas lubada või blokeerida antud ühendus, keelata alatiseks rakenduse võrguaktiivsus, lubada see vastavalt rakenduse tüübile või seadistada analoogsetele juhtumitele spetsiifiline reegel. Teie vastuse alusel võib programm formeerida antud rakendusele edaspidi automaatselt kasutatava reegli.

Vaikimisi aktiveerub Kaspersky Anti-Hacker peale kasutaja sisenemist süsteemi, kuid võite selle aktiveerida ka kohe peale op-süsteemi Windows algaadimist.



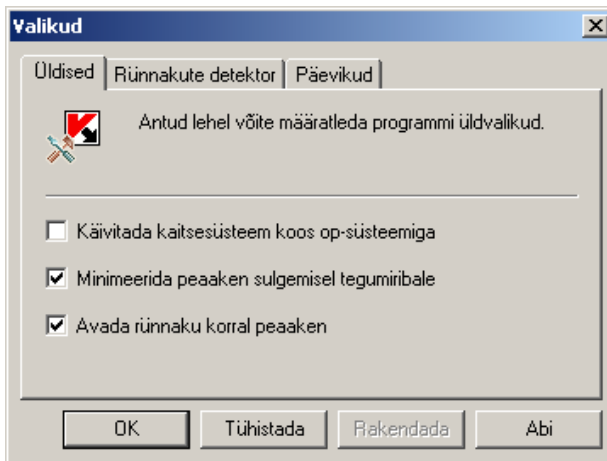
*Kaspersky Anti-Hackeri käivitamise keelamiseks või lubamiseks kohe peale op-süsteemi algaadimist:*

1. Valige menüüs **Teenindus** korraldus **Valikud**.
2. Avanevas dialoogiaknas **Valikud** (joonis 17) lülitage sisse või välja lehel **Üldised** asuv märkeruut  **Käivitada kaitsesüsteem koos op-süsteemiga**. Sisse lülitatud märkeruudu korral käivitatakse programm


kohe peale op-süsteemi algladimist. Kui programm oli seadistatud käivitamiseks **Keskmisel** turvasemel, siis kuna kuni kasutaja süsteemi sisenemiseni ei ole võimalik kuvada ekraanil õpetusakent, lubatakse kõik tundmatud võrguühendused. Samuti on tundmatu võrguaktiivsus lubatud turvasemel **Madal** ja **Kõik lubatud**. Ülejäänud tasemetel see blokeeritakse.



Oletame, et Teie arvuti on ühendatud kohtvõrku ning selle kaitse on seadistatud aktiveeruma kohe peale op-süsteemi algladimist ja Kaspersky Anti-Hackeri turvasemeks on valitud **Kõik keelatud**, või on teistel tasemetel (peale **Kõik lubatud**) kehtestatud kogu võrguliikluse blokeeriv reegel. Sel juhul kestab süsteemi sisenemine tavalisest kauem ja sisenemise järel ei ole kohtvõrk kättesaadav.



Joonis 17. Dialoogiaken **Valikud**

Võite muuta programmi reageeringut vajutusele peaakna paremas ülanurgas olevale nupule . Vaikimisi antud nupule vajutades programmi peaaken suletakse, kuid programmi ennast mälust välja ei laeta.



*Selleks, et koos peaakna sulgemisega ka programm mälust välja laetaks,*

1. Valige menüüs **Teenindus** korraldus **Valikud**.
2. Avanevas dialoogiaknas **Valikud** (joonis 17) lülitage lehel **Üldised** välja märkeruut  **Minimeerida peaaken sulgemisel tegumiribale**.

Vaikimisi avaneb rünnaku avastamisel ekraanil sellest informeeriv peaaken.



Selleks, et peaaaken ei avaneks iga kord rünnaku avastamisel,

1. Valige menüüs **Teenindus** korraldus **Valikud**.
2. Avanevas dialoogiaknas **Valikud** (joonis 17) lülitage välja lehel **Üldised** olev märkeruut  **Avada rünnaku korral peaaaken**.

## 6.1.2. Turvataseme valimine

Turvataseme valitakse turvatasemete skaalal oleva liuguriga programmi peaaeknas või menüüst **Teenindus** korraldusega **Turvataseme**. Samuti võite kasutada selleks samanimelist süsteemmenüü korraldust.

Võite valida ühe järgnevast viiest turvatasemest:

- **Kõik keelatud**;
- **Kõrge**;
- **Keskmine**;
- **Madal**;
- **Kõik lubatud**.

Tasemetel **Kõrge**, **Keskmine** ja **Madal** võite lülitada täiendavalt sisse ka märkeruudu **Väljast nähtamatu**.



Turvataseme jõustub kohe peale selle valikut.

Üksikasjalikud soovitused turvatasemete kasutamiseks on toodud p. 4.2 lk. 23.

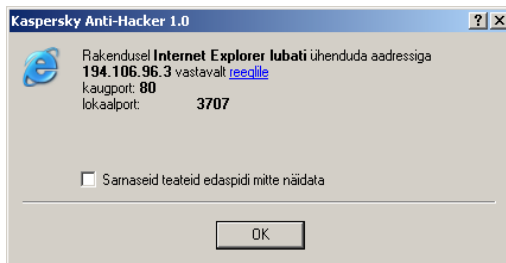
## 6.1.3. Võrgusündmusest teavitav aken

Kui lülitasite reegli loomisel sisse märkeruudu **Teavitada kasutajat** (vt. p. 0 lk. 57, p. 6.4.2.2 lk. 65), siis kuvatakse selle reegli rakendumisel ekraanil teavitusaken (joonis 18).

Joonisel 18 on toodud teate näidis, mis ilmub pakettide filtreerimise reegli rakendamisel. Teate tekstis on antud lokaal- ja kaugaadressid, aga samuti ühenduse pordid.

Rakendunud reeglit võite vaadata vastavas viisardis, vajutades selleks allajoonitud viitele.

Teadete edasise näitamise võite ka ära muuta, lülitades sisse märkeruudu **Sarnaseid teateid edaspidi mitte näidata**.



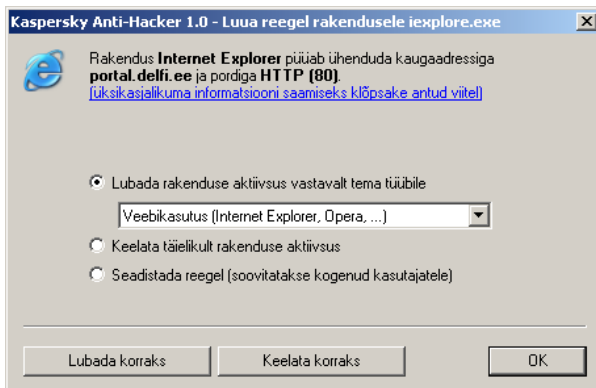
Joonis 18. Teade toimunud sündmusest



Reegli loomisel võite selle reegli rakendamisjuhtude protokollimiseks lülitada sisse märkeruudu **Registreerida sündmus päevikus**.

## 6.1.4. Õpetusaken


**Keskmisel** turvasemel väljastab programm katsel sooritada reeglites kirjeldamata võrguoperatsioone *õpetusakna* (joonis 19).

Joonis 19. Dialoogiaken **Luua reegel rakendusele ...**

Akna ülaosas on kuvatud kaugarvutiga ühenduda püüdvä rakenduse nimi ja ikoon, selle arvuti aadress ja portide numbrid. Üksikasjalikuma informatsiooni vaatamiseks klõpsake allajoonitud viitel.

Konkreetselt operatsiooni ühekordseks lubamiseks või keelamiseks võite vajutada nuppudele **Lubada korraks** või **Keelata korraks**.



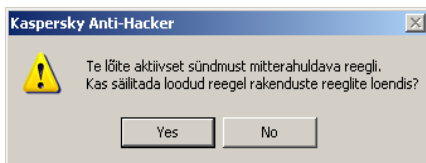
Õpetusakna sulgemine vajutusega selle paremas ülanurgas olevale nupule  keelab ühekordselt vaidlusaluse operatsiooni.

Reegli loomiseks analoogsete antud rakenduse initsieeritud sündmuste edasiseks automaatseks töötlemiseks valige üks alloletatud toimingutest ja vajutage nupule **OK**. Seejärel lisatakse rakenduste reeglite loendisse uus reegel.

- **Lubada rakenduse aktiivsus vastavalt tema tüübile** – lubada sündmuse initsieerinud rakendusele kõik selle ripploendist valitud tüübile vastavad võrguoperatsioonid (üksikasjalikumalt vt. p. 6.3.2.1 lk. 48).
- **Keelata täielikult rakenduse aktiivsus** – keelata sündmuse initsieerinud rakendusele kõik võrguoperatsioonid.
- **Seadistada reegel** – lubada või keelata rakendusele mõningaid peale vajutust nupule **OK** avanevas viisardis (viisardist üksikasjalikumalt vt. p. 6.3.2 lk. 48) antud tingimusi rahuldavad võrguoperatsioonid.



Kui seadistasite reegli, mis ei luba programmil reageerida tekkinud situatsioonile, ilmub vastav hoiatus (joonis 20). Kui soovite loodud reegli säilitada, siis vajutage nupule **Jah**, kui koostasite reegli ekslikult, siis nupule **Ei**. Mõlemal juhul tehakse Teile ettepanek jätkata toimingut valimist õpetusaknas.



Joonis 20. Hoiatus loodud reegli ja situatsiooni mittevastavusest



Pöörake tähelepanu, et juhul, kui mitu programmi püüavad lühikese ajavahemiku vältel täita Teie arvutil võrguoperatsioone, reaktsioon millistele ei ole veel määratletud reeglitega, tekib uute reeglite loomisel *päringute järjekord* ning päringud väljastatakse õpetusaknasse üksteise järel: esmalt peate määratlema reaktsiooni esimese võrguprogrammi tegevusele, siis teise programmi tegevusele jne. Kõik programmid, millisteni järjekord ei ole veel jõudnud, jäävad ootama Teie reaktsiooni.

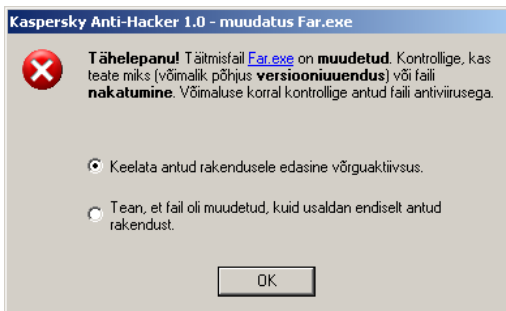
## 6.1.5. Hoiatus täitmisfaili asendusest

Kaspersky Anti-Hacker kaitseb võrgurakendusi nende algupäraste täitmisfailide asenduse eest. Avastades asendatud faili, väljastab Kaspersky Anti-Hacker hoiatuse (joonis 21).

Võite valida ühe järgmistest variantidest:

- **Keelata antud rakendusele edasine võrguaktiivsus** – kõik rakenduse järgnevad võrguoperatsioonid keelatakse: rakenduse reeglite loendi algusesse lisatakse keelav reegel ja kõik varem rakendusele loodud reeglid lülitatakse välja. Soovitame Teil kontrollida antud rakendust antivirusega, taastada see arhiivist või paigaldada uuesti. Peale rakenduse taastamist eemaldage antud rakenduse reeglite loendist keelav reegel ning lülitage sisse kõik talle loodud reeglid. Kaspersky Anti-Hacker võib taas väljastada hoiatuse täitmisfaili asendusest, kuid sel juhul valige allkirjeldatud variant ja jätkake tööd.
- **Tean, et fail oli muudetud, kuid usaldan endiselt antud rakendust** – failimuutus aktsepteeritakse ja kõik antud rakenduse jaoks loodud reeglid jätkavad toimimist.

Vajutage nupule **OK**.



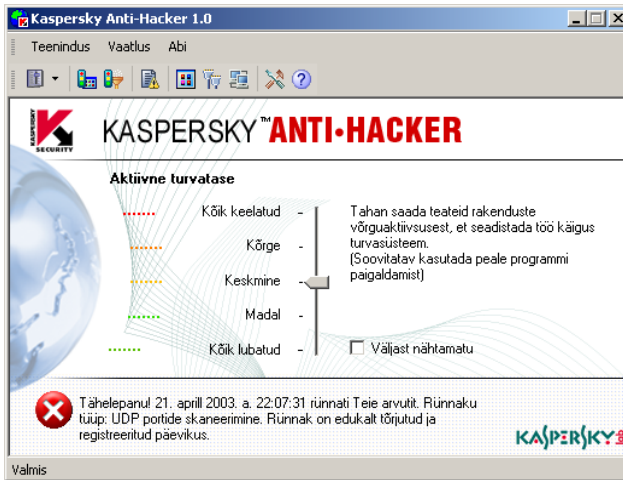
Joonis 21. Hoiatus rakenduse täitmisfaili asendusest

## 6.2. Programmi toimingud rünnaku puhul

*Mis toimub häkkerirünnaku avastamisel?*

Häkkerirünnaku avastamisel avaneb programmi peaaken (kui on lülitatud sisse märkeruut **Avada rünnaku korral peaaken** – vt. p. 6.1.1 lk. 38). Pöörake tähelepanu toimunud häkkerirünnakut kirjeldavale infole tööpiirkonna alaosas, kus on kuvatud rünnaku kuupäev, kellaeg ja tüüp (joonis 24).

Rünnak tõkestatakse ja ründav arvuti blokeeritakse seadistustes määratud ajaks (vt. p. 6.5 lk. 66).



Joonis 22. Teade avastatud häkkerirünnakust

Oletame, et märkasite, kuidas mõningatelt kaugarvutitelt üritatakse pidevalt Teie arvutisse tungida. Võite keelata selle suhtluse kaugarvutitega, luues vastava pakettide filtreerimise reegli (vt. p. 6.4 lk. 59).

Sagedaste korduvate rünnakute puhul soovitame Teil valida turvasemeks **Kõik keelatud** ning pöörduda võrguadministraatori või internetiteenuse pakkuja poole.

## 6.3. Rakenduste reeglite seadistamine

*Kuidas seadistada rakenduste reegleid? Rakenduste reeglite loomise viisard*

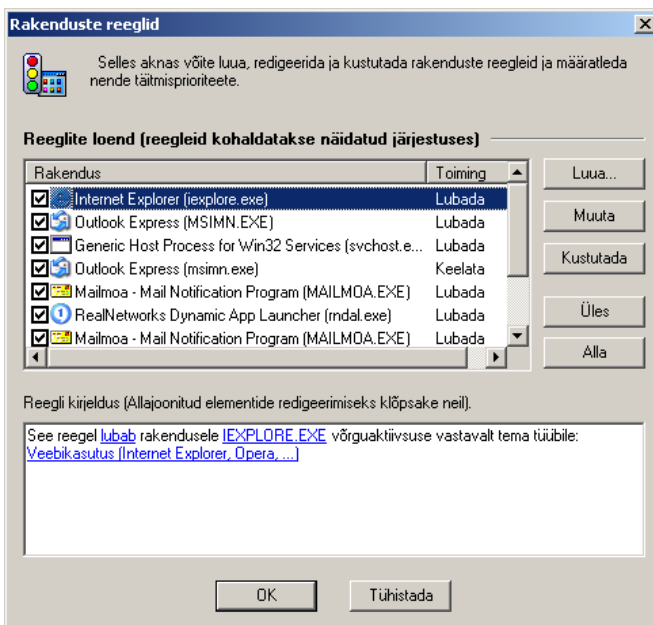
### 6.3.1. Töö reeglite loendiga



Rakenduste reeglite loendi avamiseks ,

Valige menüüs **Teenindus** korraldus **Rakenduste reeglid**.

Seejärel avaneb ekraanil dialoogiaken **Rakenduste reeglid** (joonis 23).



Joonis 23. Dialoogiaken **Rakenduste reeglid**

Dialoogiakna vasakus ülasosas asub rakenduste reeglite loend. Veerus "Rakendus" on kuvatud rakenduse ikoon, nimetus ning märkeruut, mis näitab, kas antud reegel on sisse või välja lülitatud. Veerg "Toiming" näitab, kas reegel on lubav – **Lubada** või keelav – **Keelata**.

Reeglid paiknevad loendis vastavalt nende tähtsusprioriteedi vähenemisele: esimesena täidetakse loendis esimesena seisev reegel, seejärel loendis teine seisev reegel jne. Juhul, kui rakendus püüab sooritada võrguoperatsiooni, vaadatakse reeglite loend ülalt alla läbi kuni leitakse antud operatsiooni lubav või keelav reegel või lõpeb loend. Kui reeglit ei leitud, rakendatakse vaikimisi toimingut (vt. p. 4.2 lk. 23). Nii tuleb rakendusele vaid osade operatsioonide keelamiseks luua kaks reeglit, millest üks – loendis kõrgemal asuv peab lubama antud rakendusele teatud operatsioonid ja teine – allpool asuv, keelama antud rakendusele kõik operatsioonid. Sel juhul leiab Kaspersky Anti-Hacker, kui rakendus püüab sooritada lubatud operatsiooni, reeglite loendi läbivaatamisel lubava reegli, aga kõigi teiste operatsioonide korral keelava reegli.

Näiteks keelab kolmas reegel joonisel 23 Internet Explorerile igasuguse võrguaktiivsuse, kuid teine reegel lubab talle pääsu interneti HTTP-protokolliga. Kuna teise reegli prioriteet on kõrgem, kui kolmandal, siis võib Internet Explorer ühenduda HTTP-serveritega (ja ainult nendega).

Pöörake tähelepanu, et täidetakse ainult reegleid, mille nimetuse kõrval olev märkeruut on sisse lülitatud. Näiteks on joonisel 23 neljas ja viies reegel välja lülitatud.



*Loendis oleva reegli täitmise ajutiseks sisse või välja lülitamiseks,*

lülitage sisse või välja reeglite loendis vastava reegli nimetuse kõrval asuv märkeruut.

Reeglite loendist paremal asuvad juhtimisnupud, mille abil võite:

- **Luuu** – luua uue reegli. Nupule vajutamisel avaneb rakenduste reeglite loomise viisard;
- **Muuta** – redigeerida loendis valitud reeglit. Antud nupule vajutamisel avaneb reeglite redigeerimise viisard, kus võite muuta valitud reegli parameetreid;
- **Kustutada** – kustutada loendis valitud reegli;
- **Üles** – paigutada loendis valitud reegli ühe rea võrra ülespoole, st. suurendada selle prioriteeti;
- **Alla** – paigutada loendis valitud reegli ühe rea võrra allapoole, st. vähendada selle prioriteeti.

Loendis valitud reegli muutmiseks võite vajutada klaviatuuriklahvile <ENTER> või klõpsata kaks korda hiirega valitud reeglil. Loendis valitud reegli kustutamiseks võite vajutada klaviatuuriklahvile <DEL>, aga uue reegli lisamiseks klahvile <INS>.

Reeglite loendiga töötades võite kasutada ka selle järgmisi punkte sisaldavat kontekstmenüüd:

- **Muuta** – redigeerida loendis valitud reeglit;
- **Kustutada** – kustutada loendis valitud reegel;
- **Luuu koopia** – luua loendis valitud reegli koopia. Loodud koopia paigutatakse valitud reegli alla.

Reeglite loendi all asub aken loendis valitud reegli lühikirjeldusega. Samasugust akent näete ka reegli loomise ja redigeerimise viisardis, mistõttu räägime sellest üksikasjalikumalt.

Reegli kirjeldamise aknas on musta värviga kirjutatud reegli mittemuudetav tekst ja sinise värviga ning allajoonitult reegli muudetavad parameetrid. Kui parameeter on rasvases kirjas, siis tuleb sisestada selle väärtus.



*Reegli parameetri sisestamiseks või muutmiseks,*

1. Klõpsake hiirega reegli kirjeldamise aknas soovitud parameetril.
2. Avanevas dialoogiaknas valige vajalik parameeter (parameetrite otstarvet ja nende sisestusaknaid kirjeldatakse järgmistes punktides).

Dialoogiakna **Rakenduste reeglid** alaosas asuvad järgmised nupud:

- **OK** – sulgeda aken ja säilitada kõik sooritatud muudatused;
- **Tühistada** – sulgeda aken ilma muudatusi säilitamata.



*Kõik loendis tehtud muudatused jõustuvad kohe peale nende säilitamist.*

## 6.3.2. Uue reegli lisamine

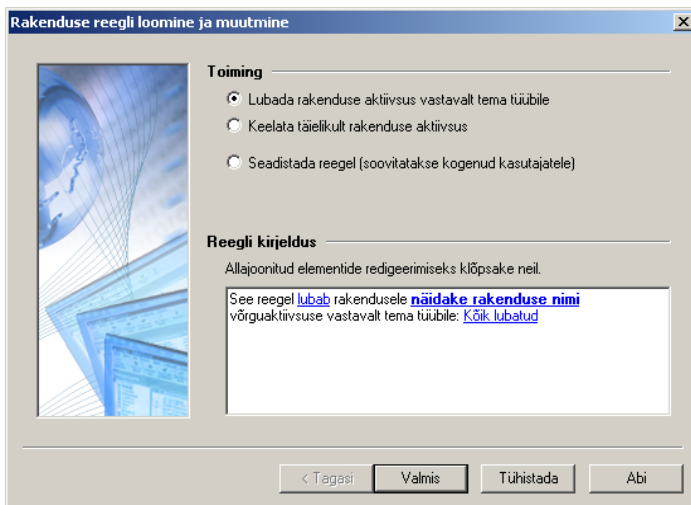


*Rakenduste reeglite viisardi avamiseks,*

vajutage dialoogiaknas **Rakenduste reeglid** olevale nupule **Luu** (joonis 23).

### 6.3.2.1. Samm 1. Reegli seadistamine

Peale viisardi avamist ilmub ekraanile joonisel 24 näidatud aken.



Joonis 24. Rakenduste reegli loomise viisardi esimene aken

Grupis **Toiming** võite valida ühe kolmest variandist:

<b>Toiming</b>	<b>Reegli kirjeldus</b>
<ul style="list-style-type: none"> <li>• <b>Lubada rakenduse aktiivsus vastavalt tema tüübile;</b></li> </ul>	See reegel <a href="#">lubab</a> rakendusele <a href="#">EXPLORE.EXE</a> võrguaktiivsuse vastavalt tema tüübile: <a href="#">Veebikasutus (Internet Explorer, Opera, ...)</a>
<ul style="list-style-type: none"> <li>• <b>Keelata täielikult rakenduse aktiivsus;</b></li> </ul>	See reegel <a href="#">keelab</a> rakendusele <a href="#">EXPLORE.EXE</a> igasuguse võrguaktiivsuse
<ul style="list-style-type: none"> <li>• <b>Seadistada reegel.</b></li> </ul>	See reegel <a href="#">lubab</a> rakendusele <a href="#">EXPLORE.EXE</a> <a href="#">luua ühendusi</a> kaugarvutitega protokolliga TCP



Variandi **Seadistada reegel** valimisel on viisardi järgmisel sammul võimalik täpsustada täiendavaid parameetreid:

- internetirakenduse tüüp (klient või server);
- protokoll;
- kaugaadress;

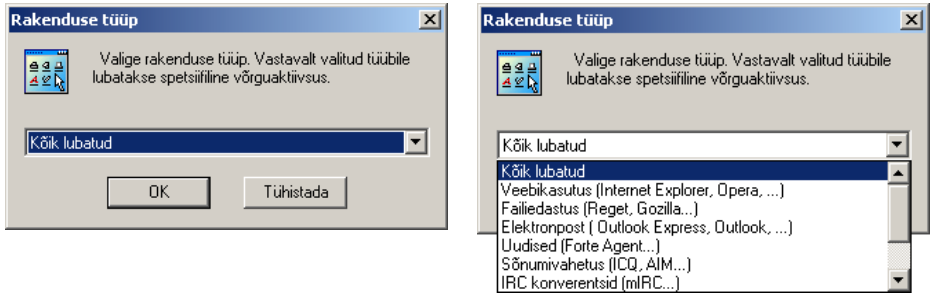
- kaugport;
- lokaalport.



*Rakendusele selle tüübile vastavat võrgusuhtlust lubava reegli loomiseks,*

1. Valige valikunuppude grupis **Toiming** variant **Lubada rakenduse aktiivsus vastavalt tema tüübile**.
2. Klõpsake väljas **Reegli kirjeldus** oleval real "Näidake rakenduse nimi" ning avanevas aknas **Rakenduse valik** näidake rakenduse nimi, millele Te loodavat reeglit soovite kohaldada.
3. Rakenduse tüüp näidatakse samuti väljas **Reegli kirjeldus**. Vaikimisi on selleks tüüp "Lubada kõik", mis ei piira vähimalgi määral rakenduse aktiivsust. Tüübi muutmiseks klõpsake sellel hiirega ning valige avanevas dialoogiaknas **Rakenduse tüüp** (joonis 25) olevast ripploendist vajalik väärtus ja vajutage nupule **OK**.
  - Veebikasutus – veebibrauseritele Internet Explorer, Netscape Navigator jt. Lubab töötada HTTP, HTTPS, FTP protokollidega ja kasutada standardseid proksi-servereid.
  - Failiedastus – Regetile, Gozillale jt. analoogsetele programmidele. Lubab töötada HTTP, HTTPS, FTP, TFTP protokollidega ja kasutada standardseid proksi-servereid.
  - Elektronpost – postiprogrammidele MS Outlook, MS Outlook Express, the Bat jt. Lubab töötada SMTP, NNTP, POP3, IMAP4 protokollidega.
  - Uudised – uudisteprogrammidele nagu Forte Agent jt. Lubab töötada SMTP, NNTP protokollidega.
  - Sõnumivahetus – ICQ, AIM ja teistele chat-programmidele. Lubab kasutada standardseid proksi-servereid ning ka Teie arvuti vahetat ühendust vestluskaaslase arvutiga.
  - IRC konverentsid – mIRC-le jt. sarnastele programmidele. Võimaldab IRC võrkude kasutajate standardset autentifitseerimist ja juurdepääsu IRC-serveri portidele.
  - Ärikonverentsid – MS NetMeetingule jt. analoogsetele programmidele. Lubab töötada protokollidega HTTP, HTTPS standardsete proksi-serverite kaudu ning toetab tööd kohtvõrgus (LDAP jt.).

- Kaughaldus – Telnetile jt. Lubab töötada protokollidega Telnet ja SSH.
- Ajasünkronisatsioon – Timehookile jt. analoogsetele programmidele. Lubab ühenduda time ja daytime-serveritega.



Joonis 25. Rakenduse tüübi valimine



*Igasuguse võrgusuhtluse keelamiseks rakendusele,*

1. Valige valikunuppude grupis **Toiming** variant **Keelata täielikult rakenduse aktiivsus**.
2. Klõpsake väljas **Reegli kirjeldus** oleval real "Näidake rakenduse nimi". Avanevas aknas **Rakenduse valik** näidake rakenduse nimi, millele tuleb kohaldada keelavat reeglit.

Kui ülalloetletud reeglite seadistusvõimalused on ebapiisavad: näiteks tahate lubada ühenduse ainult teatud IP-aadressiga, siis määratlege reegli täiendavad parameetrid.

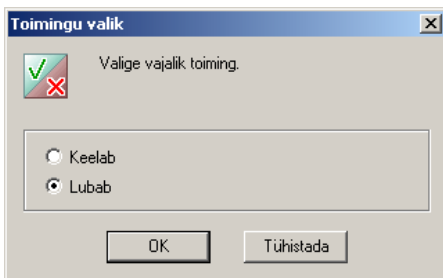


*Reegli täiendavate parameetrite määratlemiseks,*

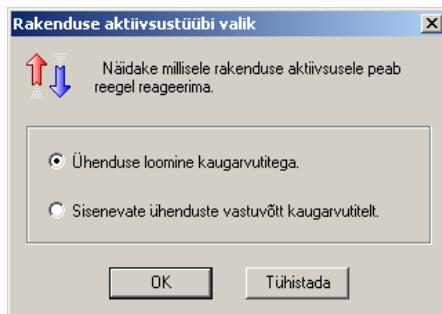
1. Valige valikunuppude grupis **Toiming** variant **Seadistada reegel**.
2. Klõpsake väljas **Reegli kirjeldus** oleval real "Näidake rakenduse nimi". Avanevas aknas **Rakenduse valik** näidake rakenduse nimi, millele reeglit tuleb kohaldada.
3. Klõpsake väljas **Reegli kirjeldus** oleval real "Lubab". Avanevas dialoogiaknas **Toimingu valik** (joonis 26) näidake vajalik toiming ja vajutage nupule **OK**:

- **Keelab;**
  - **Lubab.**
4. Näidake, millisele rakenduse aktiivsusele peab antud reegel reageerima: kas ühenduse loomisele (vaikimisi) või vastuvõtule. Vaikeväärtuse muutmiseks klõpsake väljas **Reegli kirjeldus** oleval real "Kehtestada ühendus" ning näidake avanevas dialoogiaknas **Rakenduse aktiivsustüübi valik** (joonis 27) vajalik aktiivsusvariant **Sisenevate ühenduste vastuvõtt kaugarvutitelt** ja vajutage nupule **OK**.

Lõpetanud töö esimeses viisardiaknas vajutage nupule **Edasi**.



Joonis 26. Toimingu valimine



Joonis 27. Rakenduse aktiivsustüübi valimine



Kui vajutate nupule **Edasi** ilma rakendust valimata, siis ilmub ekraanile hoiatus vajadusest jätkata tööd endises viisardiaknas.

### 6.3.2.2. Samm 2. Reegli täitmistingimused

Reegli täitmistingimuste sisestusaken ilmub üksnes juhul, kui valisite valikunuppude grupis **Toiming** nupu **Seadistada reegel**.

Antud aknas võite täpsustada protokollid, kaugarvuti aadressi ja porte.

Ripploend **Protokoll** sisaldab rea eelseadistatud protokollide nimetusi ja neile vastavaid pordinumbreid:

- HTTP;
- IMAP;
- SMTP;
- NNTP;

- POP3;
- DNS.

Kui soovite anda mõne muu pordi numbri, valige väärtus:

- Muu TCP-I baseeruv protokoll – TCP-protokollil baseeruvatele teenistustele;
- Muu UDP-I baseeruv protokoll – UDP-protokollil baseeruvatele teenistustele.

Grupis **Parameetrid** on kuvatud täiendavate parameetrite loend, mille sisu sõltub valitud protokollist.



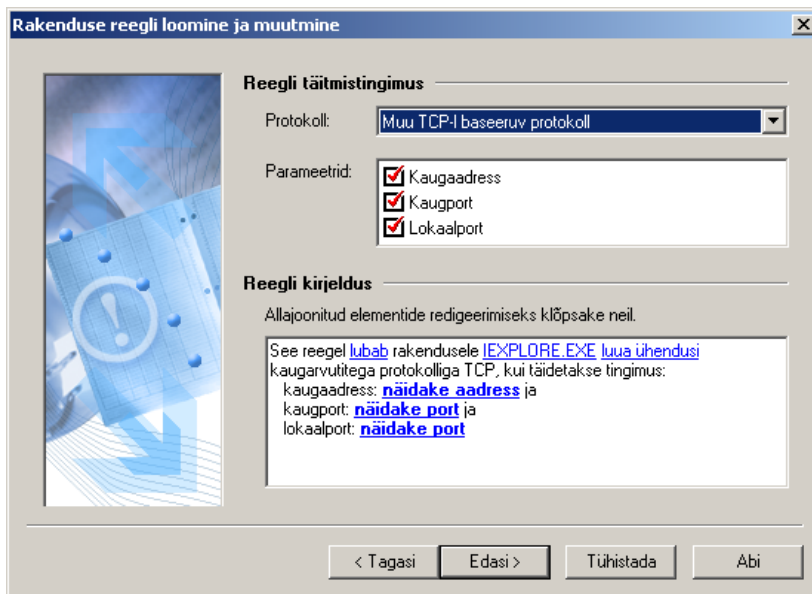
**Kaugaadress** – andmevahetuses osaleva kaugarvuti aadress. Aadressi sisestamiseks klõpsake hiirega väljas **Reegli kirjeldus** oleval real "Näidake aadress". Kui soovite sisestada aadresside loendi, hoidke hiireklõpsu ajal all klaviatuuriklahvi <CTRL>. Üksikasjalikumalt vt. p. 6.3.2.2.1 lk. 54.



**Kaugport** – kaugpordi number. Pordi sisestamiseks klõpsake hiirega väljas **Reegli kirjeldus** reast "Kaugport" paremal asuval real "Näidake port". Kui soovite sisestada portide loendi, klõpsake hiirega hoides samaaegselt all klahvi <CTRL>. Üksikasjalikumalt vt. p. 6.3.2.2.2 lk. 56.



**Lokaalport** – lokaalpordi number. Pordi sisestamiseks klõpsake hiirega väljas **Reegli kirjeldus** reast "Lokaalport" paremal asuval real "Näidake port". Kui soovite sisestada portide loendi, klõpsake hiirega hoides samaaegselt all klahvi <CTRL>. Üksikasjalikumalt vt. p. 6.3.2.2.2 lk. 56.

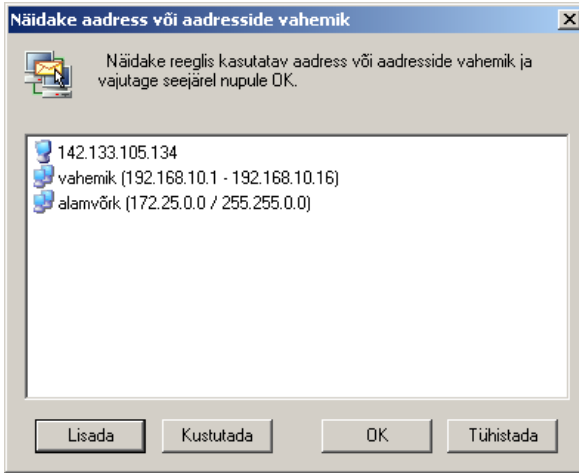


Joonis 28. Reegli täitmistingimuste sisestamine

### 6.3.2.2.1. Aadressi või aadresside vahemiku sisestamine

Aadressi sisestamiseks kasutatakse kahte dialoogiakent.

Dialoogiakent **Näidake aadress või aadresside vahemik** (joonis 29) ilmub, kui klõpsate hiirega reeglite viisardis aadressi-parameetri nimetusel, hoides samaaegselt all klaviatuuriklahvi <CTRL>.

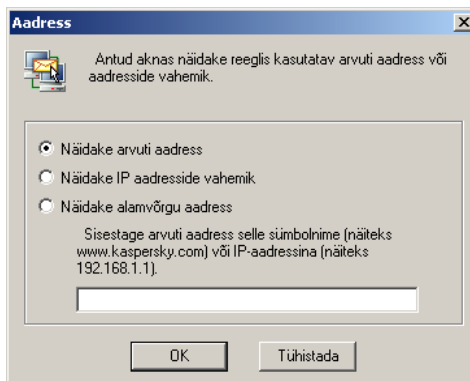


Joonis 29. Dialoogiaken **Näidake aadress või aadresside vahemik**

Aknas asuvasse loendisse võite lisada nuppudega **Lisada** ja **Kustutada** suvalise hulga aadresse, aadresside vahemikke või võrguaadresse. Peale aadresside loendi formeerimist vajutage tagasipöördumiseks reeglite loomise viisardi nupule **OK**.

Vajutades aknas **Näidake aadress või aadresside vahemik** nupule **Lisada** ilmub aken **Address** (joonis 30). Sama aken ilmub ka siis, kui klõpsate hiirega aadressi-parameetri nimetusel reeglite viisardis.

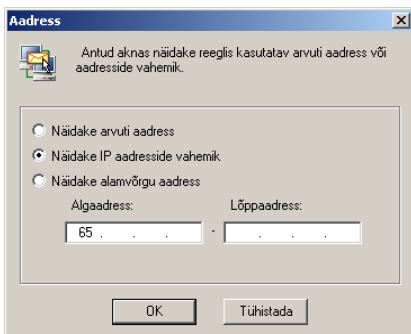
Dialoogiaken **Address** on mõeldud reeglis kasutatava aadressi, aadresside vahemiku või võrguaadressi sisestamiseks (joonis 30).



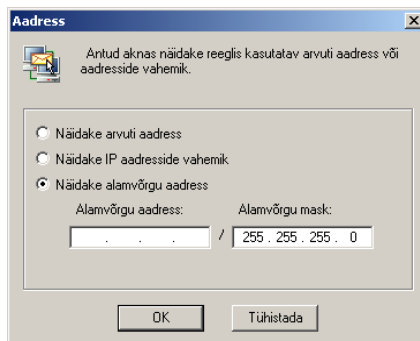
Joonis 30. Dialoogiaken **Address**. Arvuti aadressi sisestamine

Võite valida ühe kolmest variandist:

- **Näidake arvuti aadress** – sisestusväljas näidatakse arvuti sümbolnimi (näiteks `www.kaspersky.com`) või selle IP aadress (näiteks `192.68.1.1`);
- **Näidake IP aadresside vahemik** – väljas **Algaadress** näidatakse aadresside vahemiku alguse IP aadress, aga väljas **Lõppaadress** – vahemiku lõpu IP aadress (joonis 31);
- **Näidake alamvõrgu aadress** – väljas **Alamvõrgu aadress** näidatakse alamvõrgu aadress, aga väljas **Alamvõrgu mask** – selle mask (joonis 32).



Joonis 31. Aadresside vahemiku sisestamine



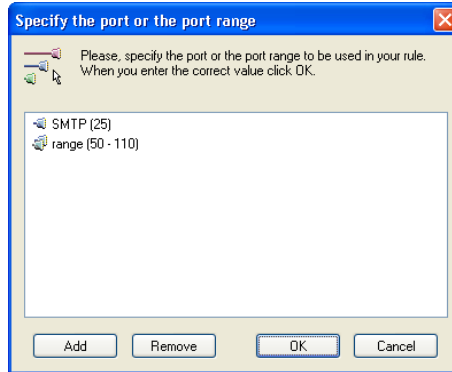
Joonis 32. Alamvõrgu aadressi sisestamine

Peale aadressi sisestamist vajutage nupule **OK**.

### 6.3.2.2.2. Pordi sisestamine

Pordinumbrite sisestamine toimub kahe dialoogiakna abil.

Dialoogiaken **Näidake port või portide vahemik** (joonis 33) ilmub, kui klõpsate hiirega reeglite viisardis pordiparameetri nimetusel, hoides sealjuures all klahvi **<CTRL>**.



Joonis 33. Dialoogiaken **Näidake port või portide vahemik**

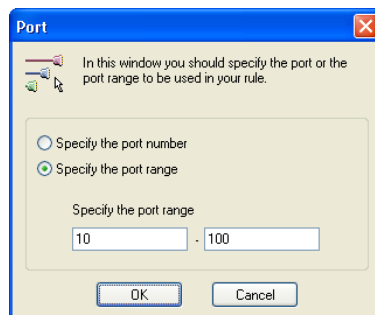
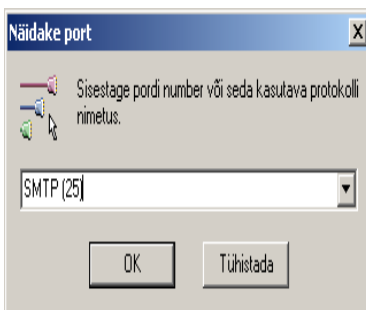
Aknas asuvasse loendisse võite nuppude **Lisada** ja **Kustutada** abil lisada suvalise hulga portide numbreid ja nende vahemikke. Peale portideloendi formeerimist vajutage tagsipöördumiseks reeglite viisardisse nupule **OK**.

Vajutades aknas **Näidake port või portide vahemik** nupule **Lisada** ilmub aken **Port** (joonis 30). Sama aken ilmub ka siis, kui klõpsate hiirega pordiparameetri nimetusega real reeglite viisardis.

Dialoogiaken **Port** on mõeldud reeglis kasutatava pordinumbriga või portide vahemiku sisestamiseks (joonis 34).

Võite valida ühe kahest variandist:

- **Näidata pordinumber** – võite valida redigeeritavast ripploendist ühe eelseadistatud väärtustest või sisestada pordinumbriga käsitsi.
- **Näidata portide vahemik** – esimeses väljas näidake vahemiku algpordi number ja teises vahemiku lõpppordi number (joonis 35).



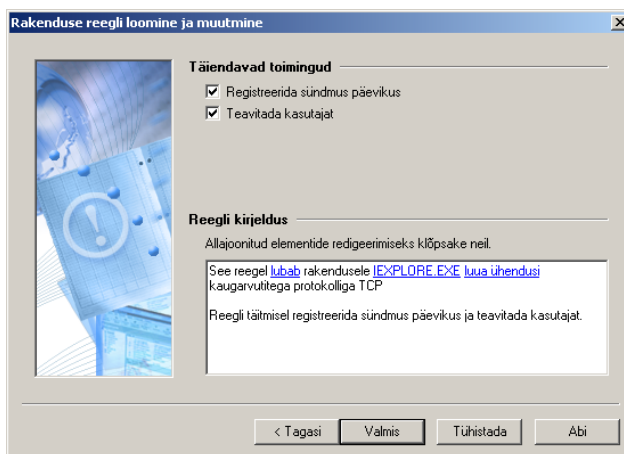
Joonis 34. Dialoogiaken **Port**

Joonis 35. Alamvõrgu aadressi sisestamine

Peale pordinumbrite sisestamist vajutage nupule **OK**.

### 6.3.2.3. Samm 3. Täiendavad toimingud

Täiendavate toimingutena võite informatsiooni säilitamiseks aset leidnud võrgusündmusest päevikus lülitada sisse märkeruudu **Registreerida sündmus päevikus** ning sündmusest teavitava hoiatusteate väljastamiseks märkeruudu **Teavitada kasutajat** (joonis 18).



Joonis 36. Täiendavad toimingud

## 6.4. Pakettide filtreerimise reeglite seadistamine

*Kuidas seadistada pakettide filtreerimise reeglid? Pakettide filtreerimise reeglite loomise viisard*

### 6.4.1. Töö reeglite loendiga

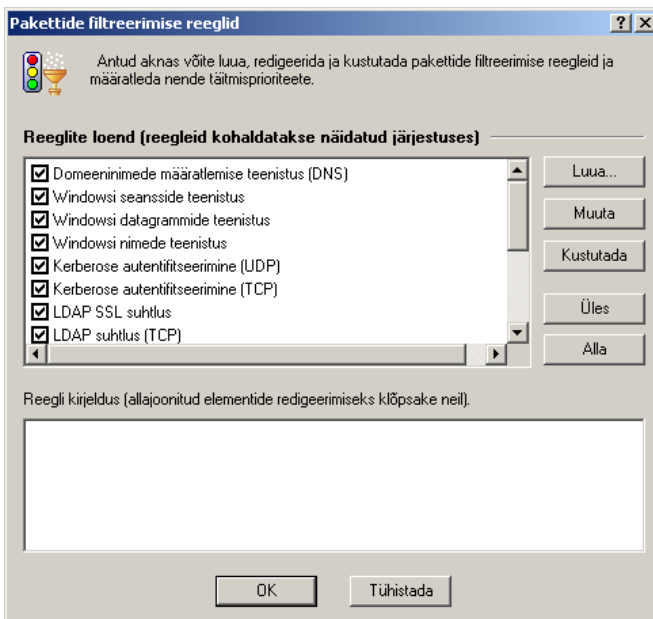
Töö pakettide filtreerimise reeglitega on analoogne tööle rakenduste reeglitega.



*Pakettide filtreerimise reeglite loendi avamiseks,*

Valige menüüs **Teenindus** korraldus **Pakettide filtreerimise reeglid**.

Seejärel avaneb ekraanil dialoogiaken **Pakettide filtreerimise reeglid** (joonis 37).



Joonis 37. Dialoogiaken **Pakettide filtreerimise reeglid**

Dialoogiakna vasakus ülaosas asub pakettide filtreerimise reeglite loend. Iga reegli nimetuse ees asub reegli seisundit, sisse või välja lülitatud, näitav märkeruut.

Reeglid paiknevad loendis vastavalt nende tähtsusprioriteedi vähenemisele: esimesena täidetakse loendis esimesena seisev reegel, seejärel loendis teiseks seisev reegel jne. Pöörake tähelepanu, et täidetakse ainult reeglid, mille nimetuse kõrval olev märkeruut on sisse lülitatud.



*Loendis oleva reegli täitmise ajutiseks sisse või välja lülitamiseks,*

*lülitage sisse või välja reeglite loendis vastava reegli nimetuse kõrval asuv märkeruut.*

Reeglite loendist paremal asuvad juhtimisnupud, mille abil võite:

- **Luua** – luua uue reegli. Nupule vajutamisel avaneb pakettide filtreerimise reeglite loomise viisard;
- **Muuta** – redigeerida loendis valitud reeglit. Nupule vajutamisel avaneb pakettide filtreerimise reeglite redigeerimise viisard;
- **Kustutada** – kustutada loendis valitud reegli;

- **Üles** – paigutada loendis valitud reegli ühe koha võrra ülespoole, st. tõsta reegli prioriteeti;
- **Alla** – paigutada loendis valitud reegli ühe koha võrra allapoole, st. alandada reegli prioriteeti.

Loendis valitud reegli muutmiseks võite vajutada klaviatuuriklahvile **<ENTER>** või klõpsata kaks korda hiirega reegli nimetusel. Loendis valitud reegli kustutamiseks võite vajutada klahvile **<DEL>**, aga uue reegli lisamiseks klahvile **<INS>**.

Reeglite loendiga töötades võib kasutada ka järgmisi punkte sisaldavat kontekstmenüüd:

- **Muuta** – redigeerida loendis valitud reeglit;
- **Kustutada** – kustutada loendis valitud reegel;
- **Luu koopia** – luua loendis valitud reegli koopia. Loodud koopia paigutatakse valitud reegli alla.

Reeglite loendi all asub aken loendis valitud reegli lühikirjeldusega. Samasugust aken näete ka reeglite loomise ja redigeerimise viisardis, seetõttu räägime sellest üksikasjalikumalt.

Reegli kirjeldamise aknas on musta värviga kirjutatud reegli mittemuudetav tekst ja sinise värviga ning allajoonitult reegli muudetavad parameetrid. Kui parameeter on rasvases kirjas, siis tuleb sisestada selle väärtus.



*Reegli parameetri sisestamiseks või muutmiseks,*

1. Klõpsake hiirega reegli kirjeldamise aknas soovitud parameetril.
2. Avanevas dialoogiaknas valige vajalik parameeter (parameetrite otstarvet ja nende sisestusaknaid kirjeldatakse järgmistes punktides).

Dialoogiakna **Pakettide filtreerimise reeglid** alaosas asuvad järgmised nupud:

- **OK** – sulgeda aken ja säilitada kõik sooritatud muudatused;
- **Tühistada** – sulgeda aken ilma muudatusi säilitamata.



*Kõik reeglite loendi muudatused jõustuvad kohe peale nende säilitamist.*

Pakettide filtreerimise reeglid on kõrgema prioriteediga, kui rakenduste reeglid ja täidetakse esimestena.

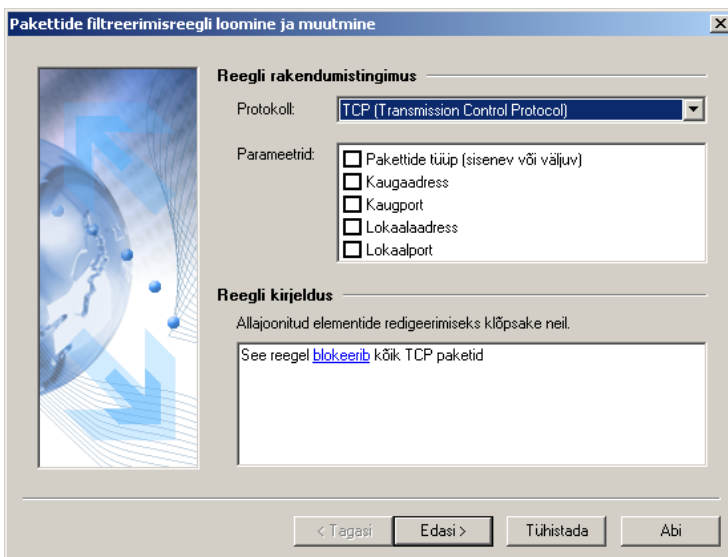
## 6.4.2. Uue reegli lisamine

Pakettide filtreerimise reeglite loomise viisard on analoogne rakenduste reeglite loomise viisardile ja koosneb kahest sammust.

### 6.4.2.1. Samm 1. Reegli rakendumistingimuste sisestamine

Pakettide filtreerimise reegli loomise esimesel sammul võite määratleda:

- kasutatava protokoll (TCP, UDP, ICMP, muud IP protokollid);
- pakettide sihtaadressi;
- liikluse suuna (väljuv, sisenev);
- protokoll spetsiifilised väärtused (TCP ja UDP protokollide puhul – pordid, ICMP protokollide puhul – teadete tüübid, teiste IP protokollide puhul – protokoll number);
- toiming (lubada/keelata).



Joonis 38. Pakettide filtreerimise reeglite loomise viisardi esimene aken

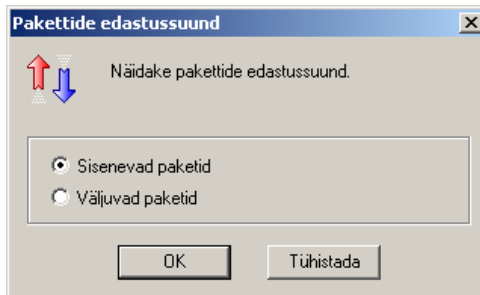


*Filtreerimisreegli määratlemiseks,*

1. valige ripploendis **Protokoll** filtreeritav protokoll: **TCP (Transmission Control Protocol)**, **UDP (User Datagram Protocol)**, **ICMP (Internet Control Message Protocol)** või **Muud IP protokollid**. Vaikimisi on valitud TCP-protokoll.
2. Märkeruutude grupis **Parameetrid** andke



**Pakettide tüüp (sisenev või väljuv)** – pakettide edastussuund. Vaikimisi on märkeruut välja lülitatud, mis vastab liikluse kontrollile mõlemas suunas. Kui soovite, et programm kontrolliks ainult sisenevat või ainult väljuvat liiklust, lülitage märkeruut sisse ja andke väljas **Reegli kirjeldus** liikluse suund. Liikluse suuna sisestamiseks klõpsake hiirega sellele vastaval real. Avanevas dialoogiaknas **Pakettide edastussuund** valige vajalik variant ja vajutage siis nupule **OK**.



Joonis 39. Dialoogiaken **Pakettide edastussuund**

3. Märkeruutude grupis **Parameetrid** kuvatakse ka täiendavaid parameetreid, mille koostis sõltub valitud protokollist.
  - TCP ja UDP protokollide korral võib näidata **Kaugpordi** ja **Lokaalpordi**.
  - ICMP protokollil korral võib näidata **ICMP teate tüübi**.
  - muude IP protokollide korral võib näidata **Protokoll**.



**Kaugaadress** – kaugarvuti aadress (kõigile protokollidele).



**Lokaalaadress** – lokaalarvuti aadress (kõigile protokollidele). Aadressi sisestamiseks klõpsake hiirega väljas **Reegli kirjeldus** reast "Lokaalaadress" paremal asuval real "Näidake aadress". Kui soovite anda aadresside loendit, siis hoidke samaaegselt all klaviatuuriklahvi **<CTRL>**. Üksikasjalikumalt vt. p. 6.3.2.2.1 lk. 54.



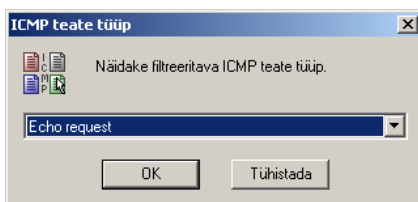
**Kaugport** – kaugarvuti pordinumber (TCP ja UDP protokollidele).

**Lokaalport** – lokaalarvuti pordinumber (TCP ja UDP protokollidele).

Pordi sisestamiseks tuleb klõpsata hiirega väljas **Reegli kirjeldus** reast "Kaugport" paremal oleval real "Näidake port". Kui soovite sisestada portide loendi, klõpsake hiirega, hoides all klahvi **<CTRL>**. Üksikasjalikumalt vaadake punktist 6.3.2.2.2).

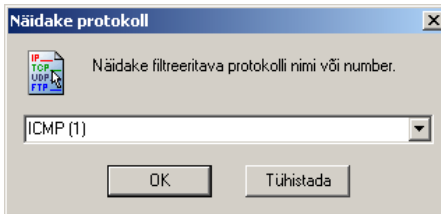
**ICMP teate tüüp** – ICMP teate tüüp (ainult ICMP protokollile). Tüübi sisestamiseks klõpsake hiirega väljas **Reegli kirjeldus** oleval real "Näidake teate tüüp ". Avanevas dialoogiaknas **ICMP teate tüüp** (joonis 40) valige ripploendist vajalik väärtus ja vajutage seejärel nupule **OK**.

- Echo request;
- Echo reply;
- Trace route (TTL exceed);
- Net unreachable;
- Host unreachable;
- Protocol unreachable;
- Port unreachable;
- Redirect for host;
- Redirect for net;
- Redirect for TOS and net;
- Redirect for TOS and host.



Joonis 40. Dialoogiaken **ICMP teate tüüp**

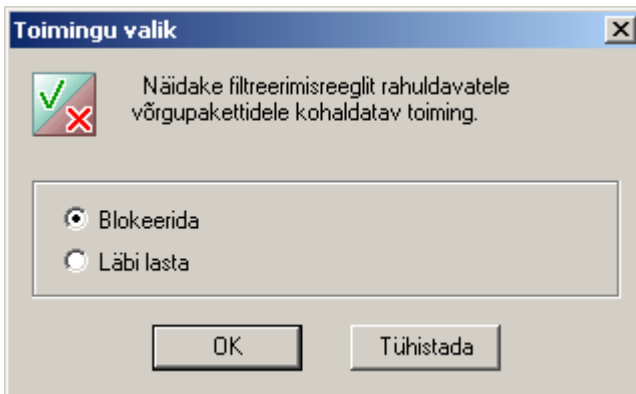
**Protokoll** – protokollide nimetus või number (ainult IP-protokollidele). Juhul, kui Te antud märkeruutu sisse ei lülita, filtreeritakse kõiki IP protokolle. Teatud protokollide sisestamiseks lülitage märkeruut sisse ja klõpsake hiirega väljas **Reegli kirjeldus** asuval real "Näidake protokoll". Avanevas dialoogiaknas **Näidake protokoll** (joonis 41) valige ripploendist vajalik väärtus ja vajutage nupule **OK**. Allpool toodud protokollide loendis on toodud sulgudes vastav protokollide number.



Joonis 41. Dialoogiaken **Näidake protokoll**

- ICMP(1);
- IGMP,RGMP(2);
- GGP(3);
- IP in IP encapsulation(4);
- TCP(6);
- IGRP(9);
- UDP(17);
- GRE(47);
- ESP(50);
- AH(51);
- IP with encryption(53).

4. Määratlege programmi poolt üllaloetletud tingimusi rahuldava paketi avastamisel sooritatav toiming: blokeerida või lubada. Vaikimisi sellised paketid blokeeritakse. Väärtuse muutmiseks klõpsake sellel väljas **Reegli kirjeldus**, valige avanevas aknas **Toimingu valik** sobiv variant ja vajutage nupule **OK** (joonis 42).

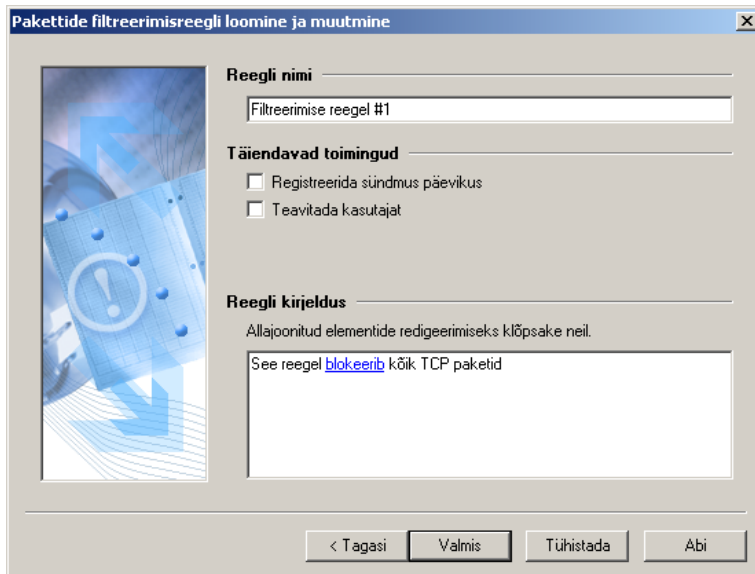


Joonis 42. Dialoogiaken **Toimingu valik**

### 6.4.2.2. Samm 2. Reegli nimetuse ja täiendavate toimingute sisestamine

Pakettide filtreerimise reegli loomise teisel sammul tuleb sisestada selle nimetus väljas **Reegli nimi**. Reegli nimetus kuvatakse reeglite loendis ja aitab neid identifitseerida. Vaikimisi pakutakse järgmise struktuuriga unikaalset reeglinime: "Filtreerimise reegel #<reegli number>". Soovitame Teil sisestada reegli spetsiifikale vastava nimetuse.

Täiendavate toimingutena võite informatsiooni säilitamiseks aset leidnud võrgusündmusest päevikus lülitada sisse märkeruudu **Registreerida sündmus päevikus** ning sündmusest teavitava hoiatusteate väljastamiseks märkeruudu **Teavitada kasutajat** (joonis 18).



Joonis 43. Reegli nimetuse ja täiendavate toimingute sisestamine

## 6.5. Rünakute detektor

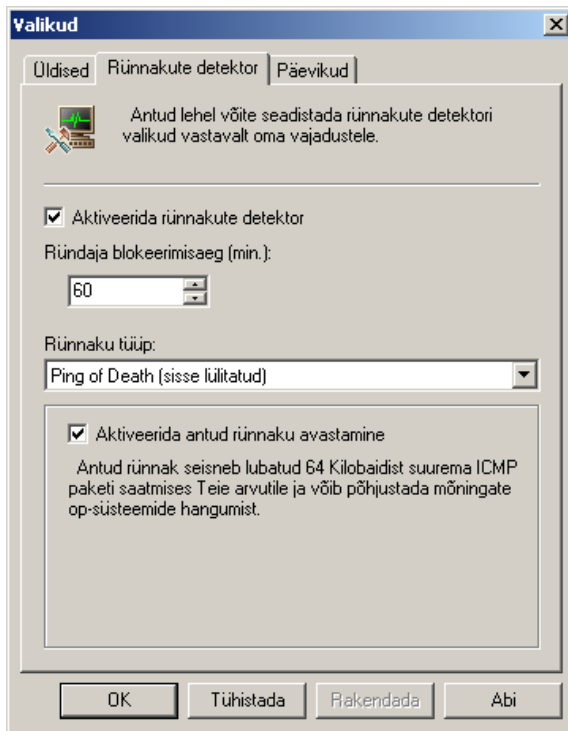
*Kuidas seadistada optimaalselt rünakute detektor?*

### 6.5.1. Rünakute detektori seadistusaken



*Rünakute detektori seadistusakna avamiseks,*

Valige menüüs **Teenindus** korraldus **Valikud** ja minge lehele **Rünakute detektor** (joonis 44).



Joonis 44. Dialoogiakna **Valikud** leht **Rünnakute detektor**

Soovitav on hoida pidevalt sisse lülitatuna lehe ülaosas asuv märkeruut  **Aktiveerida rünnakute detektor**, sest just sellest sõltub, kas Teie arvuti vastaste rünnakute detektor on aktiveeritud või mitte.

Allpool asuvas arvväljas **Ründaja blokeerimisaeg** sisestage aeg, mille jooksul ründav arvuti peab jääma täielikult blokeerituks, kui õnnestus tuvastada selle aadress. Antud parameeter on ühine kõigile rünnakutüüpidele.



**Ründaja blokeerimisaeg** muudatus jõustub kohe peale vajutust nuppudele **OK** või **Rakendada** aknas **Valikud** ja toimib kõigi edaspidi avastatavatele rünnakute korral. Juba toimunud rünnakute tõttu blokeeritud arvutite blokeerimisaeg ei muutu.

Akna alaosas paikneva paneeli sisu muutub sõltuvalt ripploendis **Rünnaku tüüp** valitud rünnakutüübist.

Selleks, et programm avastaks valitud tüüpi rünnakud, lülitage sisse märkeruut **Aktiveerida antud rünnaku avastamine**. Otsustamisel on Teile abiks märkeruudu all olev rünnaku kirjeldus.

## 6.5.2. Avastatavate häkkerirünnakute loend

Kaspersky Anti-Hacker avastab enamlevinud DoS rünnakud (*SYN Flood*, *UDP Flood*, *ICMP Flood*), *Ping of death*, *Land*, *Helkem*, *Lovesan* ja *SmbDie* rünnakud ning ka tavaliselt võimsamatele rünnakutele eelneva portide skaneerimise:

- *Ping of death* rünnak seisneb lubatud 64 Kb väärtust ületava ICMP-paketi saatmises. See rünnak võib põhjustada mõningate operatsioonisüsteemide hangumist.
- *Land* rünnak seisneb päringu edastamises ohverarvuti avatud portide ühenduse loomiseks iseendaga. Rünnak viib ohverarvuti lõputusse tsüklisse, mille tulemusel kasvab järsult protsessori koormus ja võib hanguda operatsioonisüsteem.
- *TCP portide skaneerimine* seisneb katses avastada ohverarvuti avatud TCP-porte. Rünnakut kasutatakse süsteemi nõrkade kohtade otsimiseks ja eelneb tavaliselt palju võimsamale rünnakule. Selle rünnaku tuvastamiseks võite seadistada **Portide hulga**, mida kaugarvuti püüab avada ja **Aja**, mille jooksul see toimub.
- *UDP portide skaneerimine* on analoogne TCP-portide skaneerimisele ja seisneb katses avastada ohverarvuti avatud UDP-porte. Rünnak tuvastatakse ohverarvuti erinevatele portidele teatud ajavahemikus saadetud UDP-pakettide hulga järgi. Rünnakut kasutatakse süsteemi nõrkade kohtade otsimiseks ja eelneb tavaliselt palju võimsamale rünnakule. Selle rünnaku tuvastamiseks võite seadistada **Portide hulga**, mida kaugarvuti püüab avada ja **Aja**, mille jooksul see toimub.
- *SYN Flood* rünnak seisneb suure hulga päringute saatmises ohverarvutitele väärühenduste tekitamiseks. Süsteem reserveerib igale sellisele ühendusele teatud ressursid ja lakkab nende ammendumises reageerimast teistele ühenduskatsetele. Antud rünnaku tuvastamiseks võite määratleda **Ühenduste hulga**, mida kaugarvuti püüab luua ja **Aja** mille jooksul see toimub.
- *UDP Flood* rünnak seisneb tänu oma struktuurile lõputult ohverarvuti ja sellele kättesaadava suvalise aadressi vahel vahetatavate UDP-pakettide lähetamises ohverarvutite, mille tulemusena raisatakse mõlema arvuti ressursid ja koormatakse üle sidekanal. Antud rünnaku tuvastamiseks võite määratleda sisenevate **UDP pakettide hulga** ja **Aja**, mille jooksul need saavad.

- *ICMP Flood* rünnak seisneb suure hulga ICMP-pakettide saatmises ohverarvutile. Rünnak viib selleni, et kasvab oluliselt igale saabunud pakatile vastama sunnitud ohverarvuti protsessori koormus. Antud rünnaku tuvastamiseks võite määratleda sisenevate **ICMP pakettide hulga** ja nende saabumiseks kuluva **Aja**.
- *Helkern rünnak* seisneb spetsiaalse kujuga UDP-pakettide saatmises teie arvutile, mis on võimelised täitma kahjurkoodi. Rünnak põhjustab interneti aeglustumist.
- *Lovesan rünnak* seisneb katses avastada operatsioonisüsteemide Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server 2003 DCOM RPC teenistuses olevaid auke ja nende olemasolul saadetakse Teie arvutile kahjurprogramm, mis võimaldab sooritada Teie arvutiga suvalisi manipulatsioone.
- *SmbDie rünnak* seisneb katses tekitada ühendus kasutades SMB-protokolli ja selle õnnestumisel saadetakse arvutile spetsiaalse kujuga pakett, mis püüab tekitada puhvri ületäitumise, mille tulemuseks on arvuti restart. Rünnakule on aldistatud operatsioonisüsteemid Windows 2k/XP/NT.

# PEATÜKK 7. PROGRAMMI TÖÖTULEMUSTE VAATAMINE

## 7.1. Jooksva seisundi vaatamine

*Aktiivsete võrgurakenduste,  
ühenduste ja avatud portide loendite  
vaatamine*


Programm Kaspersky Anti-Hacker registreerib pidevalt kõigi Teie arvutile paigaldatud rakenduste võrgukasutust. Aktiivset võrgukasutust kuvavat informatsiooni saate vaadata kolmes allkirjeldatud loendis.

- **Aktiivsete võrgurakenduste loend.** Kogu aktiivne võrgukasutus on grupeeritud selle initsieerinud rakenduste järgi. Kõigi rakenduste puhul on toodud antud rakendusega seotud portide ja ühenduste loend.
- **Aktiivsete ühenduste loend.** Kuvatakse kõik sisenevad ja väljuvad ühendused, kaugarvutite aadressid ja portide numbrid.
- **Avatud portide loend.** Kuvatakse Teie arvuti avatud portid.

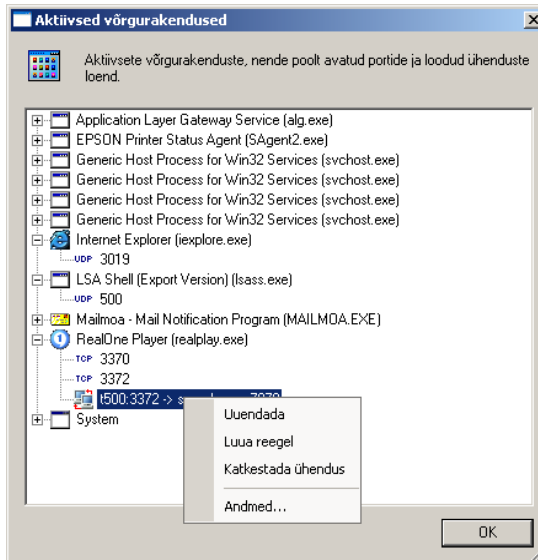
### 7.1.1. Aktiivsete võrgurakenduste loend



*Kui soovite teada, millised võrgurakendused on hetkel Teie arvutil aktiivsed,*

valige menüüs **Vaatlus** alammenüü **Näidata** ja selles korraldus **Aktiivseid võrgurakendusi** (joonis 45) või vajutage tööriistaribal olevale nupule .



Seejärel ilmub ekraanile dialoogiaken **Aktiivsed võrgurakendused**.



Joonis 45. Dialogiakn **Aktiivsed võrgurakendused**

Antud dialoogiaknas võite vaadata aktiivsete võrgurakenduste ja neile kuuluvate võrguressursside loendit. Selles navigeerimise lihtsustamiseks on rakendused järjestatud nende nimede järgi ja iga rakenduse nimetusest vasakul asub selle ikoon.

Avades rea rakenduse nimetusega, võite vaadata antud konkreetsele rakendusele kuuluvate avatud portide ja ühenduste loendit.

- Avatud port tähistatakse sõltuvalt selle tüübist ikooniga **TCP** või **UDP**, millest paremal kuvatakse porti number.
- Ühendus tähistatakse ikooniga , kui ühenduse initsiaatoriks on Teie arvuti, või ikooniga , kui ühendus on loodud väljastpoolt. Ikonist paremal tuuakse ühenduse parameetrid: <initsiaatori address>:<initsiaatori port> → <sihtaaddress>:<sihtport>

Aktiivsete võrgurakenduste loendit uuendatakse automaatselt kaks korda sekundis.

Loend omab järgmisi elemente sisaldavat kontekstmenüüd:

- **Uuendada** – uuendada aktiivsete võrgurakenduste loendis kuvatav info;

- **Luu reegel** – luua loendis valitud pordi või ühenduse alusel reegel. Programm avab rakenduste reeglite loomise viisardi, täites selle Teie poolt valitud pordi või ühenduse andmetega;
- **Katkestada ühendus** – katkestada loendis valitud ühendus (korraldus on kättesaadav üksnes ühenduse valimisel);

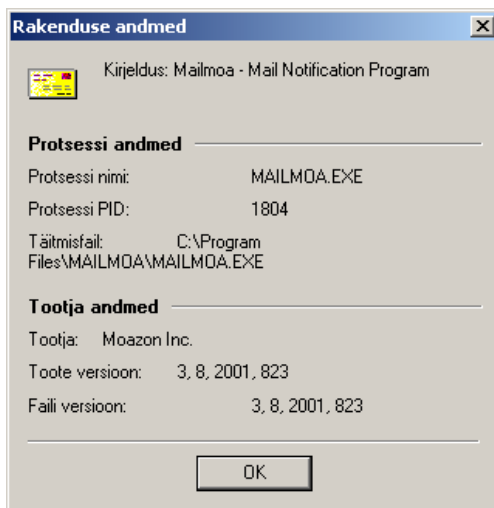


Tähelepanu! Ühenduse sunniviisilisel katkestamisel võib mõningate rakenduste töös ilmnedä häireid.

- **Andmed** – näidata detailsemat informatsiooni loendis valitud elemendi: rakenduse (joonis 46), ühenduse (joonis 48) või pordi (joonis 50) kohta.



Tabel võib sisaldada ühesuguseid rakenduste nimetusi, mis tähendab, et ühest ja samast rakendusest on käivitatud mitu koopiat. Pöörake tähelepanu, et ühesuguse nimetusega rakendused omavad erineva sisuga avatud portide ja ühenduste loendeid.



Joonis 46. Dialogiaken **Rakenduse andmed**

Dialogiakena **Rakenduse andmed** ülaosas asub sektsioon **Protsessi andmed**:

- **Protsessi nimi** – täidetava faili nimi;
- **Protsessi PID** – protsessi identifikaator;
- **Täitmisfail** – täielik tee täidetava failini;


Akna alaosas asub sektsioon **Tootja andmed**:

- **Tootja** – programmi valmistanud firma;
- **Toote versioon** – programmi versiooninumber;
- **Faili versioon** – täidetava faili versiooninumber.



## 7.1.2. Aktiivsete ühenduste loend



*Aktiivsete ühenduste loendi vaatamiseks,*

valige menüüs **Vaade** alammenüü **Näidata** ja seal korraldus **Aktiivseid ühendusi** (joonis 47) või vajutage tööriistaribal olevale nupule .

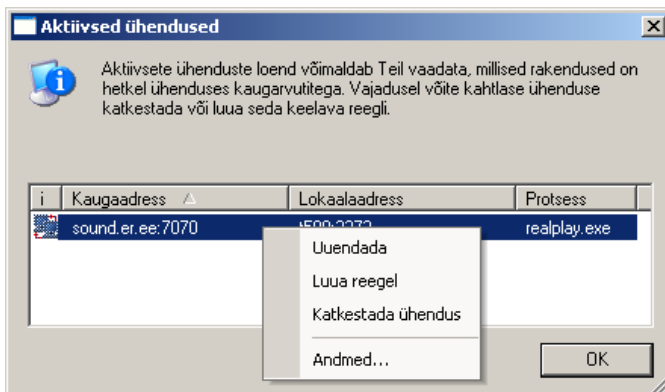
Seejärel ilmub ekraanile dialoogiaken **Aktiivsed ühendused**.

Loendi iga rida vastab ühele ühendusele. Kui ühenduse initsiaatoriks on Teie arvuti, tähistatakse see ikooniga , kui aga ühendus on loodud väljastpoolt, siis ikooniga .

Igat ühenduse juures on toodud järgmised parameetrid:

- **Kaugaadress** – ühenduses osaleva kaugarvuti aadress ja port;
- **Lokaalaadress** – Teie arvuti aadress ja port;
- **Protsess** – ühenduse loonud protsess.

Võite sorteerida loendid kõigi loetletud parameetrite alusel.

Joonis 47. Dialoogiaken **Aktiivsed ühendused**

Aktiivsete ühenduste loendit uuendatakse automaatselt kaks korda sekundis.

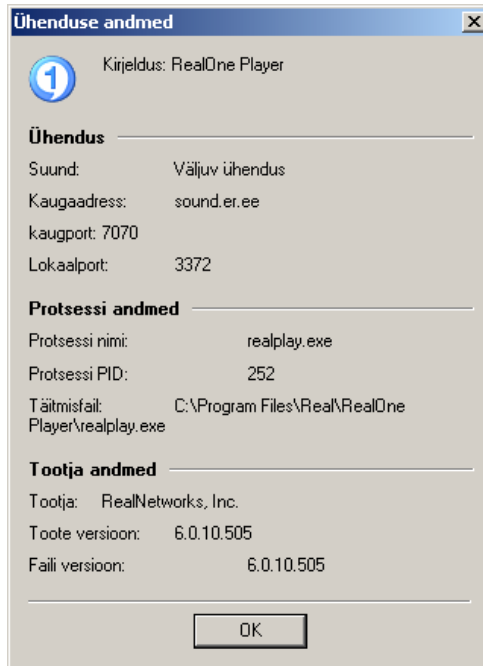
Vajadusel võite soovimatud ühendused katkestada ja/või luua reeglid sarnaste ühenduste keelamiseks tulevikus, kasutades selleks kontekstmenüüd:

- **Uuendada** – uuendada aktiivsete ühenduste loendi sisu;
- **Luu reegel** – luua loendis valitud ühenduse baasil uus reegel. Programm avab rakenduste reeglite loomise viisardi täites selle Teie poolt valitud ühenduse andmetega;
- **Katkestada ühendus** – katkestada loendis valitud ühendus;



**Tähelepanu!** Ühenduse sunniviisilisel katkestamisel võib mõningate rakenduste töös ilmneda häireid.

- **Andmed** – näidata detailsemat informatsiooni loendis valitud ühendusest (joonis 48).



Joonis 48. Dialoogiaken **Ühenduse andmed**

Dialoogiakna **Ühenduse andmed** sektsioon **Ühendus** sisaldab järgmisi andmeid:


- **Suund** – sisenev või väljuv ühendus;
- **Kaugaadress** – kaugarvuti sümbolnimi või IP-aadress;
- **Kaugport** – kaugpordi number;
- **Lokaalport** – lokaalpordi number;

Allpool asuvad sektsioonid **Protsessi andmed** ja **Tootja andmed** (vt. p. 7.1.1 lk. 70).

## 7.1.3. Avatud portide loend



Avatud portide loendi vaatamiseks,

valige menüüs **Vaatlus** alammenüü **Näidata** ja selles korraldus **Avatud porte** (joonis 49) või vajutage tööriistaribal olevale nupule .

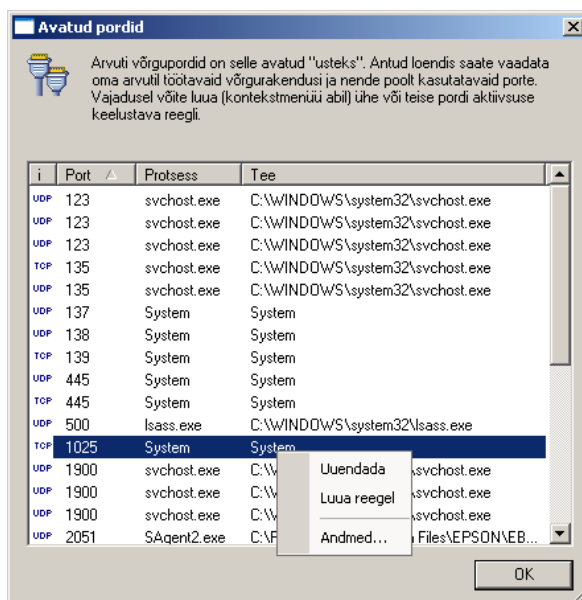
Seejärel ilmub ekraanile dialoogiaken **Avatud pordid**.

Iga loendi rida vastab ühele avatud pordile. Porte tähistatakse vastavalt nende tüübile ikoonidega **TCP** või **UDP**.

Iga avatud pordi kohta tuuakse ära järgmised andmed:

- **Lokaalport** – pordi number;
- **Protsess** – pordi avanud protsess;
- **Tee** – täielik tee täidetava moodulini.

Võite sorteerida loendit kõigi eelloetletud parameetrite järgi.

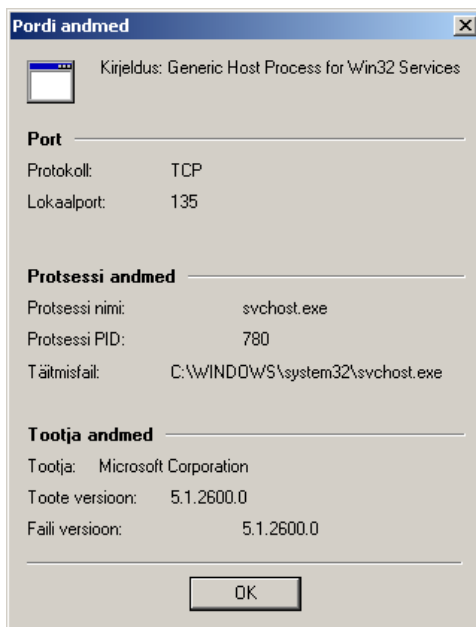


Joonis 49. Dialoogiaken **Avatud pordid**

Avatud portide loendit uuendatakse automaatselt kaks korda sekundis.

Vajadusel võite luua reegli, mis keelab edasised ühendused valitud porti kaudu, kasutades selleks kontekstmenüüd:

- **Uuendada** – uuendada avatud portide loendi sisu;
- **Lua reegel** – luua loendis valitud porti alusel reegel. Programm avab rakenduste reeglite loomise viisardi, täites selle Teie poolt valitud porti andmetega;
- **Andmed** – näidata loendis valitud porti detailsemaid andmeid (joonis 50).



Joonis 50. Dialoogiaken **Porti andmed**

Dialoogiakna **Porti andmed** sektsioon **Port** sisaldab järgmist informatsiooni:

- **Protokoll** – protokollini nimi;
- **Lokaalport** – lokaalporti number.

Allpool paiknevad sektsioonid **Protsessi andmed** ja **Tootja andmed** (vt. p. 7.1.1 lk. 70).

## 7.2. Töö päevikutega

*Päevikuteakna avamine ja kirjeldus.*

*Päeviku valimine. Päeviku säilitamine failis*

Teie arvutil toimuvaid võrgusündmusi registreeritakse ja säilitatakse *päevikutes*. Erinevate sündmuste jaoks on ette nähtud kolme tüüpi päevikud:

- **Võrgurünnakute päevik.** Antud päevikus säilitatakse informatsiooni viimastest rünnakutest Teie arvutile (vt. p. 6.5 lk. 66);
- **Rakenduste võrguaktiivsuse päevik.** Antud päevikus registreeritakse sündmused, mis Te määrasite protokollitavateks rakenduste reeglite loomise viisardis (vt. p. 0 lk. 57);
- **Pakettide filtreerimise päevik.** Antud päevikus registreeritakse sündmused, mis Te määrasite protokollitavateks pakettide filtreerimise reeglite loomise viisardis (vt. p. 6.4.2.2 lk. 65).

Töö kõigi päevikutega toimub ühises aknas (*päevikuteaknas*).

Päevikute suurus võib olla piiratud, samuti võite kehtestada päevikute automaatse puhastamise režiimi igal programmi käivitamisel või säilitada neis pikemaajalisi andmeid (vt. p. 7.2.4 lk. 83).

Soovi korral võite päeviku ka sunniviisil puhastada või säilitada selle failis.

### 7.2.1. Päevikuteakna avamine



*Päevikuteakna avamiseks*

valige menüüs **Vaatlus** alammenüü **Päevikud** ja selles vajalik päevik.

Seejärel avaneb ekraanil päevikuteaken (joonis 51).

## 7.2.2. Päevikuteaken

Päevikuteaken koosneb järgmistest osadest:

- peamenüü;
- aruandetabel;
- vajaliku päeviku valimist võimaldavad järjehoidjad.

### 7.2.2.1. Peamenüü

Päevikuteakna ülaosas asub *peamenüü*.

Tabel 4

Menüüelement	Otstarve
Fail → Säilitada failis	Säilitada aktiivne päevik failis
Abi → Kaspersky Anti-Hackeri abisüsteem	Avada abisüsteem
Abi → Kaspersky Anti-Hacker Internetis	Näidata Kaspersky Lab'i kodulehte Internetis
Abi → Programmi info	Näidata programmi üldandmeid

### 7.2.2.2. Aruandetabel

Aruandetabelis on kuvatud valitud päevik. Selle vaatamiseks võite kasutada paremas servas olevat kerimisriba.

Aruandetabel omab vaikumisi kaheelemendilist kontekstmenüüd, mis laieneb sõltuvalt valitud päevikust:

- **Puhastada päevik** – puhastada valitud päevik;
- **Näidata viimast kirjet** – näidata tabeli nähtavas osas alati sissekannet viimasest sündmusest;

- **Mitte protokollida antud sündmusi** – valitud sündmust enam mitte päevikus registreerida. Korraldus on kättesaadav kõigile päevikutele peale häkkerirünnakute päeviku;
- **Luu reegel** – luua valitud sündmuse alusel reegel. Reegli loomisel paigutatakse see reeglite loendisse, kui kõige prioriteetsem.

### 7.2.2.3. Järjehoidjad

Järjehoidjad on mõeldud vajaliku päeviku valimiseks:

- Võrgurünnakud;
- Rakenduste aktiivsus;
- Pakettide filtreerimine.

## 7.2.3. Päeviku valimine

### 7.2.3.1. Võrgurünnakute päevik

Võite vaadata võrgurünnakute päevikut, kus on registreeritud kõik avastatud katsed rünnata Teie arvutit (vt. p. 6.5 lk. 66).



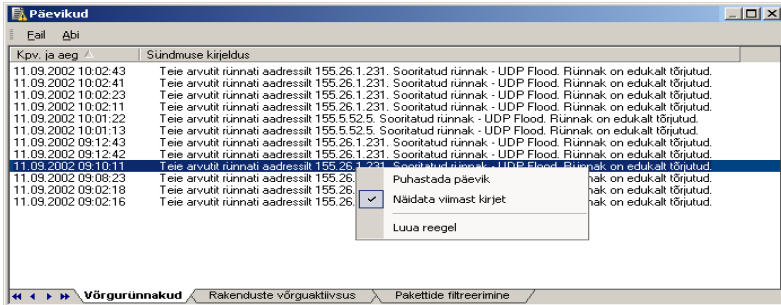
*Võrgurünnakute päeviku vaatamiseks,*

valige menüüs **Vaatlus** alammenüü **Päevikud** ja selles korraldus **Võrgurünnakute päevik**.

Seejärel avaneb ekraanil aken **Päevikud** esiplaanil oleva leheküljega **Võrgurünnakud** (joonis 51), kus on kuvatud:

- **Kpv. ja aeg** – Teie arvuti rünnakukatse toimumise kuupäev ja kellaaeg;
- **Sündmuse kirjeldus** – võrgurünnaku kirjeldus: selle nimetus ja rünnanud arvuti aadress, kui see õnnestus tuvastada.

Sündmuste loendit on võimalik sorteerida ainult kuupäeva ja kellaaja järgi.



Joonis 51. Võrgurünnakute päevik

## 7.2.3.2. Rakenduste aktiivsuse päevik

Võite vaadata rakenduste, millistele on rakenduste reeglites kehtestatud protokollimise režiim (vt. p. 0 lk. 57), aktiivsuse päevikut.



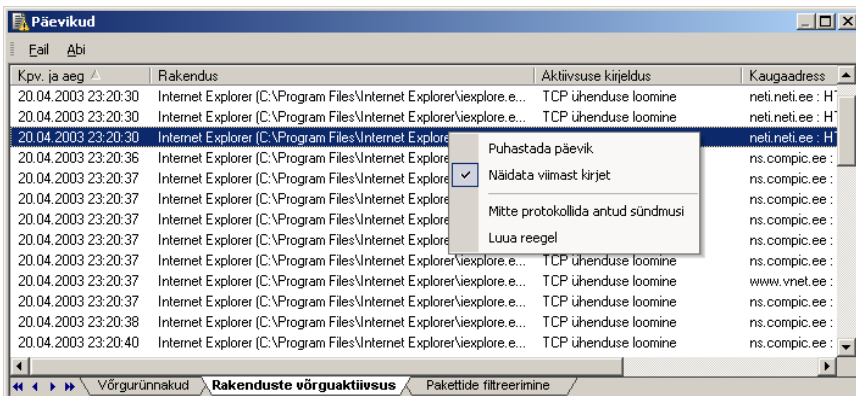
*Rakenduste aktiivsuse päeviku vaatamiseks,*

valige menüüs **Vaatlus** alammenüü **Päevikud** ja seal korraldus **Rakenduste võrguaktiivsuse päevik**.

Seejärel avaneb ekraanil aken **Päevikud** esiplaanil oleva leheküljega **Rakenduste võrguaktiivsus** (joonis 52), kus on kuvatud:

- **Kpv. ja aeg** – sündmuse toimumise kuupäev ja kellaaeg;
- **Rakendus** – rakenduse nimetus ja tee täitmisfailini;
- **Aktiivsuse kirjeldus** – mis nimelt juhtus;
- **Lokaalaadress** – lokaalaadress;
- **Kaugadress** – kaugaadress.

Sündmuste loendit võib sorteerida ainult kuupäeva ja kellaaaja järgi.



Joonis 52. Rakenduste aktiivsuse päevik

### 7.2.3.3. Pakettide filtreerimise päevik

Võite vaadata pakettide tasandil toimuva aktiivsuse, kui see oli määratud protokollida pakettide filtreerimise reeglites (vt. p. 6.4.2.2 lk. 65), päevikut.



*Rakenduste aktiivsuse päeviku vaatamiseks,*

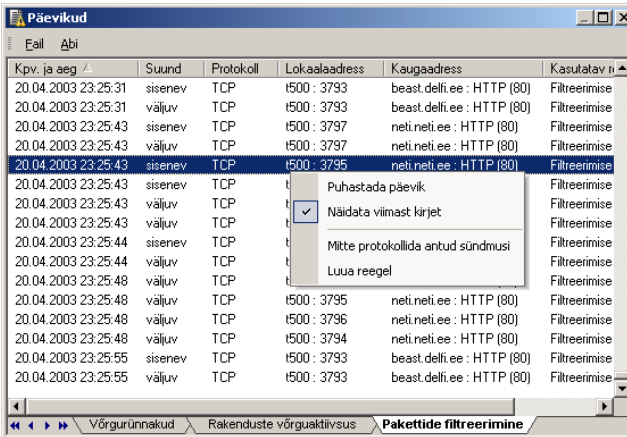
valige menüüs **Vaatus** alammenüü **Päevikud** ja seal korraldus **Pakettide filtreerimise päevik**.

Seejärel avaneb ekraanil aken **Päevikud** esiplaanil oleva leheküljega **Pakettide filtreerimine** (joonis 53), kus on kuvatud:

- **Kpv. ja aeg** – sündmuse toimumise kuupäev ja kellaaeg;
- **Suund** – sisenev või väljuv pakett;
- **Protokoll** – protokollini nimetus;
- **Lokaalaadress** – lokaalaadress;
- **Kaugaadress** – kaugaadress;
- **Kasutatav reegel** – rakendunud reegli nimi.

Musta värviga kuvatakse lubatud paketid ja punasega keelatud.

Sündmuste loendit võib sorteerida ainult kuupäeva ja kellaaja järgi.



Joonis 53. Paketite filtreerimise päevik

## 7.2.4. Päevikuvalikute seadistamine



*Päevikuvalikute seadistamiseks,*

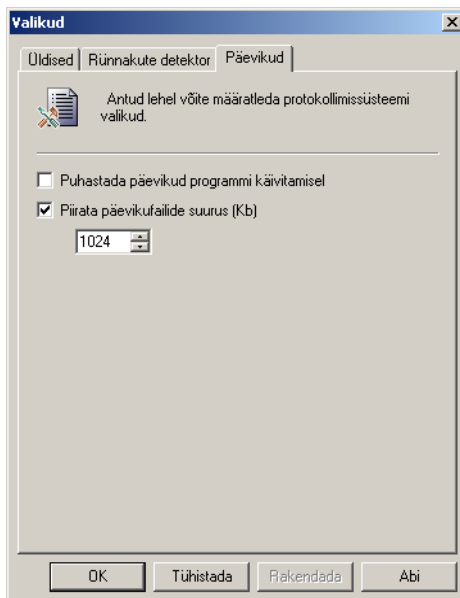
Valige menüüs **Teenindus** korraldus **Valikud** ja minge lehele **Päevikud** (joonis 54).

Võite määratleda kaks järgmist parameetrit:

- Puhastada päevikud programmi käivitamisel** – programmi käivitamisel puhastatakse kõik kolm päevikut.
- Piirata päevikufailide suurus (KB)** – kehtestada päevikufailide maksimaalsuuruseks allolevas sisestusväljas näidatud väärtus. Maksimaalsuuruse saavutamisel hakatakse uute kirjade päevikusse lisamisel eemaldama kõige vanemaid.



Pöörake tähelepanu, et antud välja abil ei määratle Te mitte kõigi kolme faili üldsuurust vaid üksnes ÜHE päevikufaili suuruse. Programmi normaalseks tööks vajaliku kettaruumi arvestamisel tuleb korrutada sisestatud väärtus kolmega.

Joonis 54. Dialoogiakna **Valikud** leht **Päevikud**

## 7.2.5. Päeviku säilitamine failis



Aknas **Päevikud** valitud päeviku säilitamiseks failis,

valige menüüs **Fail** korraldus **Säilitada failis**. Avanevas dialoogiaknas sisestage faili nimi. Päevik säilitatakse lihttekstina.

# LISE A. KASPERSKY LAB LTD.

*Kaspersky Lab. Antiviirustooted.*

*Koordinaadid*

**Kaspersky Lab Ltd.** on 1997. aastal asutatud rahvusvaheline erakapitalile rajanev antiviirus tarkvara arendusfirmade grupp, esindustega Moskvas (Venemaal), Cambridgeis (Inglismaal) ja Pleasantonis (USA-s), kes on kontsentreerinud kõik oma jõupingutused infokaitse tehnoloogiate ning tarkvara arendusele, marketingile ning jaotamisele.

Kaspersky Lab Ltd. on maailma üks tunnustatumaid antiviirustehnoloogiate arendajaid ja paljud praktiliselt kõigi kaasaegsete antiviiruste funktsionaalsed lahendused olid esmakordselt loodud just meie kompaniis. Mitmed maailma suuremad antiviirustarkvara tootjad kasutavad oma toodetes Kaspersky Anti-Viruse antiviirustuuma. Kaspersky Anti-Viruse erakordne loodetavus ja kvaliteet on leidnud kinnitust ka kõige erinevamate riikide arvutiväljaannete ning sõltumatute testimislaboratooriumite poolt väljastatud arvukate sertifikaatide ja auhindade näol.

Kaspersky Lab'i peamiseks tegevusvaldkonnaks on **antiviirused**, millele on kontsentreeritud kompanii põhilised jõupingutused. Pakutav tootevalik on suunatud nii koduarvutitele, kui igas suuruses korporatiivvõrkudele. Kaspersky Lab'i antiviiruslahendused tagavad kindla kontrolli kõigi potentsiaalsete arvutiviiruste sissetungiallikate üle: neid kasutatakse tööjaamadel, faili- ja veebiserveritel, postilüüsidel ja võrkudevahelistel ekraanidel. Mugavad haldusvahendid võimaldavad kasutajatel maksimaalselt automatiseerida nii üksikarvutite, kui korporatiivvõrkude antiviiruskaitset.

## A.1. Kaspersky Lab'i antiviirustooted

### Kaspersky Anti-Virus Lite

Kaspersky Lab'i tootevaliku kõige lihtsamalt kasutatav operatsioonisüsteemide Windows 95/98/Me, Windows 2000/NT Workstation, Windows XP juhtimisel töötavate koduarvutite kaitseks mõeldud antiviirustooded.

Kaspersky Anti-Virus Lite sisaldab:

- **antiviirus skannerit** lokaalsete kõvaketaste täieulatuslikuks antiviiruskontrolliks kasutaja otsesel korraldusel;

- **antiviirus monitori** kõigi kasutatavate täitmisfailide automaatseks kontrollimiseks reaajas.

### **Kaspersky Anti-Virus Personal/Personal Pro**

Spetsiaalselt operatsioonisüsteemide Windows 95/98/ME, Windows 2000/NT, Windows XP juhtimisel töötavate koduarvutite ja MS Office 2000 ärirakenduste ning postiprogrammide Outlook, Outlook Express antiviiruskaitseks loodud tarkvarapakett. Kaspersky Anti-Virus Personal/Personal Pro kätkeb endas programmi igapäevaste uuenduste internetist alla laadimiseks ning integreeritud antiviiruskaitse juhtimis- ja automatiseerimismoodulit. Unikaalne teise põlvkonna heuristiline analüüsisüsteem võimaldab efektiivselt neutraliseerida senitundmatud viirused ja lihtne ning mugav kasutajaliides teeb töö paketiiga kergeks ja meeldivaks.

Kaspersky Anti-Virus Personal sisaldab:

- **antiviirus skannerit** lokaal- ja võrguketaste täielikuks kontrollimiseks kasutaja nõudel;
- **antiviirus monitori** kõigi kasutatavate failide automaatseks kontrollimiseks reaajas;
- **postifiltrit** kogu siseneva ja väljuva posti taustrežiimis kontrollimiseks;
- **juhtimiskeskust** Kaspersky Anti-Viruse komponentide automaatkäivituseks vastavalt varem seatud ajakavale, nende tsentraliseeritud haldamiseks ja automaatseks viirusrännakustest teavitamiseks.

Kaspersky Anti-Virus Personal Pro sisaldab aga lisaks eelloetletutele veel kahte täiendavat komponenti:

- **muudatuste revidenti** kõigi kettamuudatuste jälgimiseks ning modifitseeritud failide ja algladimissektorite taastamiseks, kui selleks peaks tekkima vajadus;
- **käitumuslikku blokeerijat**, mis tagab 100%-lise makroviiruste vastase kaitse.

### **Kaspersky® Security for PDA**

Kaspersky® Security for PDA tagab Palm OS või Windows CE juhtimisel töötavatel pihuarvutitel säilitatavate aga samuti PC-lt, laienduskaartidelt jne. edastatavate andmete kindla antiviiruskaitse. Programm sisaldab optimaalse valiku antiviiruskaitse vahendeid: kasutaja nõudel nii pihuarvutil, kui igat tüüpi

laienduskaartidel säilitatavat infot kontrolliva **antiviirus skanneri**; andmete sünkroniseerimisel HotSync™ tehnoloogia või teiste pihuarvutitega viirusprogrammide ülevõttu teostava **antiviirus monitori**. Programm tagab samuti pihuarvutitel säilitatavate andmete kaitse sanktsioneerimata juurdepääsu eest šifreerides nii juurdepääsu seadmele, kui ka kogu pihuarvutil ja laienduskaartidel säilitatava info.

### **Kaspersky Anti-Virus Business Optimal**

Unikaalne konfigureeritav antiviiruskaitselahendus väikestele ja keskmise suurusega äriettevõtetele.

Kaspersky Anti-Virus Business Optimal pakub täieulatuslikku antiviiruskaitset:

- Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux juhtimisel töötavatele tööjaamadele;
- Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD juhtimisel töötavatele faili- ja rakendusserveritele;
- MS Exchange Server 5.5/2000, Lotus Notes/Domino, sendmail, Postfix, Qmail, Exim postilüüsidele.

Komplekti kuuluvad antiviirusprogrammid võite valida iseseisvalt vastavalt kasutatavatele operatsioonisüsteemidele ja rakendustele.

### **Kaspersky Corporate Suite**

Kaspersky Corporate Suite on integreeritud süsteem, mis tagab Teie korporatiivvõrgu infoturvalisuse sõltumata võrgu keerukusest ja suurusest. Kompleksi koosseisu kuuluvad tsentraliseeritud juhtimissüsteemiga ühendatud ja ühtset kasutajaliidest omavad programmikomponendid on mõeldud ettevõtte kõigi võrgusõlmede kaitseks ning on ühilduvad enamiku tänapäeval kasutatavate operatsioonisüsteemide ja tarkvararakendustega võimaldades luua Teie võrgu süsteemsete nõuetega täielikult ühilduva kaitsesüsteemi.

Kaspersky Corporate Suite tagab täieulatusliku antiviiruskaitse:

- Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux, OS/2 juhtimisel töötavatele tööjaamadele;
- Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD juhtimisel töötavatele faili- ja rakendusserveritele;
- MS Exchange Server 5.5/2000, Lotus Notes/Domino, sendmail, Postfix; Exim, Qmail postilüüsidele;
- CVP-ühilduvatele võrkudevahelistele ekraanidele;

- veebiserveritele;
- Palm OS juhtimisel töötavatele pihuarvutitele (PDA).

Komplekti kuuluvad antiviiirusprogrammid võite valida iseseisvalt vastavalt kasutatavatele operatsioonisüsteemidele ja rakendustele.

### **Kaspersky® Anti-Spam**

Kaspersky™ Anti-Spam on esimene vene tarkvarakompleks kaitseks soovimatute kirjade, spami ehk rämpsposti eest keskmistele ja väikeettevõtetele. Toode ühendab endas revolutsioonilisi lingvistilisi tekstianalüüsi tehnoloogiaid, kõiki kaasaegeid e-posti filtreerimismeetodeid (kaasa arvatud RBL loendid ja formaalsed kirjatunnused) ja unikaalset teenustevalikut, mis võimaldavad kasutajatel avastada ja hävitada kuni 95% soovimatust liiklusest.

Kaspersky® Anti-Spam kujutab endast ettevõtte võrgu "sisendisse" paigaldatavat filtrit, mis kontrollib sisenevas kirjades esinevat rämpsposti. Toode on ühildatav iga tellija võrgus kasutatava postisüsteemiga ja võib olla paigaldatud nii juba olemasolevale, kui spetsiaalselt eraldatud postiserverile.

Programmi kõrge efektiivsus saavutatakse tänu sisu filtreerimise baasi igapäevasele automaatsesele uuendamisele lingvistika laboratooriumi spetsialistide poolt esitatavate näidistega.

## **A.2. Meie kontaktandmed**

Kõigi oma küsimuste, kommentaaride või ettepanekutega võite pöörduda meie esindajate poole või vahetult Kaspersky Lab'i.

### **Kaspersky Lab:**

WWW: <http://www.kaspersky.com>

Müügiosakond: [sales@kaspersky.com](mailto:sales@kaspersky.com)

Tehniline tugi: [support@kaspersky.com](mailto:support@kaspersky.com)

Marketingi ja turustusosakond: [info@kaspersky.com](mailto:info@kaspersky.com)

Antiviiirus laboratoorium (üksnes uute viiruste saatmiseks arhiveeritud kujul):  
[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)

# LISE B. SELETAV SÕNASTIK

Rünnakute detektor .....	6, 23, 24, 63
Litsentsileping .....	6, 7
Õpetusaken .....	22, 37, 39
Võrgusündmustest teavitav aken.....	38
Rakenduste reeglid.....	21, 42
Pakettide filtreerimise reeglid.....	22, 55
Turvatasemed.....	5, 18, 22, 23, 36, 38
Tehnilise toe teenistus.....	10, 88
Paigaldus CD.....	6
Turvatasemete skaala .....	31, 38

# LISE C. KORDUMA KIPPUVAD KÜSIMUSED



Mõningate ülesannete täitmisel Teie arvutil tekivad vead ning Te soovite kontrollida ega need ei ole tingitud programmi Kaspersky Anti-Hacker tööst.



Minge mõneks ajaks turvasemele **Kõik lubatud** või laadige Kaspersky Anti-Hacker arvuti mälust välja. Kontrollige, kas situatsioon muutus. Kui esineb sama viga, siis ei ole see seotud Kaspersky Anti-Hackeri tööga. Kui viga ei teki, võtke ühendust Kaspersky Lab'i spetsialistidega.