Tallinna Ülikool
Informaatika Instituut

Arkadi Bojaršinov

VANEMLIKU JÄRELEVALVE TARKVARA ROLL LAPSE TURVALISE INTERNETIKASUTAMISE TAGAMISEL. LAPSEVANEMATE NÄGEMUS

Magistritöö

Juhendaja: MA Birgy Lorenz

Autor: ..... ”.....” 2013
Juhendaja: ..... ”.....” 2013
Instituudi direktor ..... ”.....” 2013

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....
Kuupäev Allkiri

Sisukord

Sissejuhatus

Järelevalve tarkvara roll laste internetiturvalisuse tagamisel on praegu aktuaalne aruteluteema nii Euroopas kui ka maailmas. Infotehnoloogia areng pakub meile üha rohkem võimalusi töös, meelelahutuses, õppimises ja nüüd ka laste kasvatamises. Turvalise internetikasutamise tagamiseks saavad lapsevanemad kasutada erinevaid strateegiaid, eelkõige see on selgitustöö ja laste harimine, suulised piirangud ja reeglid. Üha suuremat tähelepanu pälvivad niisugused tehnilised lahendused, mis oskavad potentsiaalselt ohtliku veebisisu tuvastada ja blokeerida ning anda lapsevanemale ülevaate lapse toimingutest internetis. Selliseid programme nimetatakse vanemliku järelevalve tarkvaraks *(parental control software).*

Uuringud (Lobe, Livingstone, Ólafsson ja Vodeb, 2011) on avastanud palju murettekitavaid fakte Eesti laste internetikasutamises. Selgus, et Eesti lapsed puutuvad võrreldes teiste Euroopa riikide lastega palju sagedamini kokku internetis levivate seksuaalsete materjalidega, küberkiusamisega, suhtlevad veebis tihedamini võõrastega ja käivad nendega päriselus kohtumas. Eesti lapsed on interneti liigkasutamises samuti Euroopas esirinnas. Vinter (2013) jõuab oma doktoritöös järelduseni, et Eestis kasutavad lapsed arvuteid võrdlemisi iseseisvalt, kas vanemate vähese juhendamisega või hoopis juhendamata, ning lapsevanemate teadlikkus *online*-riskidest on madal. On selge, et lapsed vajavad kaitset virtuaalmaailmas sama palju kui reaalelus, ning tänapäeva lapsevanemad peavad otsima vastust järgmisele küsimusele – millised meetodid on selleks kõige tõhusamad?

Vanemliku järelevalve tarkvara kasutamine Eestis on vähe arutletud ja uuritud teema, kuigi interneti mõjust ja laste internetiturvalisust on meedias kirjutatud palju enam rohkem. Erinevad sotsiaalsed kampaaniad ja internetiturvalisuse portaalid (Targalt Internetis[1], Laps Netis[2], Netiohud[3], Päriselt ka või?[4]) ignoreerivad järelevalve tarkavara temaatikat ning ei anna lapsevanematele nõu ega abi sellise tarkvara valimisel ja kasutamisel. Seega võib minu magistritööst neile abi olla.

Magistritöö eesmärk on välja selgitada, millisena tajuvad lapsevanemad vanemliku järelevalve tarkvara rolli laste internetiturvalisuse tagamisel?

[1]Targalt Internetis http://www.targaltinternetis.ee/
[2]Turvaline käitumine internetis http://lapsnetis.eesti.ee/
[3]Netiohud http://www.netiohud.ee/
[4]Päriselt ka või? http://päriseltkavõi.ee/

Vastavalt eesmärgile püstitasin järgmised **uurimisküsimused**:

1. Milliseid riske lapsevanemad tajuvad ja peavad probleemseks seoses laste internetis viibimisega?
2. Milliseid järelevalvestrateegiaid kasutavad lapsevanemad, et kaitsta oma last *online*-riskide eest?
3. Millisena näevad lapsevanemad vanemliku järelevalve tarkvara rolli võrreldes teiste järelevalvestrateegiatega?

Töö teoreetilises osas annan ülevaate võimalikest *online*-riskidest ja erinevatest vanemliku järelevalve strateegiatest, kirjeldan järelevalve tarkavara funktsionaalsust, analüüsin tarkvara eeliseid ja puuduseid.

Empiirilises osas uurin 4–12-aastaste laste vanemate arvamusi vanemliku järelevalve tarkvara kohta Eestis – milliseid riske vanemad tajuvad probleemseks, milliseid strateegiaid kasutavad, et tagada lapsele turvalist internetikasutamist ja kui suurt rolli selles mängivad tehnilised vahendid. Uurimistöö metoodikaks on kvantitatiivne kirjeldav uurimus, kus andmekogumiseks kasutan internetiküsitlust.

Viimases tööosas „Järeldused ja arutelu" tehakse järeldusi, millistel juhtumitel järelevalve vahendite rakendamine on otstarbekas ning jagatakse soovitusi, kuidas saab Eesti kontekstis vastava tarkavara kasutamist soodustada.

Kuigi vanemliku järelevalve funktsioone saab kasutada erinevates seadmetes (tahvelarvuti, nuti- ja mobiiltelefon, televiisor, mängukonsool, e-luger, Wifi ruuter), keskendutakse selles uurimistöös järelevalvevahenditele, mida rakendatakse tavaarvutis. Käesoleva uurimistöö kaudseks eesmärgiks on abistada lapsevanemaid, valida sobivat turvastrateegiat oma lapse kaitseks internetis ning tõsta sellealast teadlikkust. Töö tulemused pakuvad huvi lapsevanematele, lasteaia- ja kooliõpetajatele, koolide ja teiste haridusasutuste IT-juhtidele, IT spetsialistidele, turbetarkavara arendajatele, sotsiaaltöötajatele ning lastekaitseametnikele.

Töö koosneb neljast peatükist ja kolmest lisast; töös on kolm tabelit, kolm pilti ja 10 diagrammi.

Märksõnad: internetiturvalisus, vanemlik järelevalve internetis, vanemliku järelevalve tarkvara.

1. Teoreetiline raamistik

Magistritöö teoreetilise osa eesmärk on anda ülevaade järelevalve programmide võimalustest ja efektiivsusest, analüüsida, kuivõrd suudavad vanemliku järelevalve programmid tagada turvalist internetikasutust. Kirjanduse põhjal annan ülevaate võimalikest *online*-riskidest, millega lapsed internetis kokku puutuvad. Seejärel kirjeldan erinevaid järelevalvestrateegiaid, mida lapsevanemad võivad kasutada laste kaitseks *online*-riskide eest, toon lühidalt välja iga strateegia eelised ja puudused. Seejärel vaatlen detailsemalt tehnilist järelevalvet ning üritan vastata järgmistele küsimustele:

- Kas vanemliku järelevalve tarkvara funktsionaalsus on piisavalt lai ja katab peamiseid *online*-riske?
- Kas vanemliku järelevalve funktsioonid töötavad efektiivselt, mis on nende kasutegur?
- Milliseid negatiivseid tagajärgi võib vanemliku järelevalve kasutamine kaasa tuua?

Teoreetilise osa lõpus toon lühidalt välja järelevalve tarkavara kasutamise poolt- ja vastuargumendid.

1.1 Lapsi puudutavad ohud internetis

Eesti lapsed paistavad Euroopas silma aktiivse internetikasutusega: kui 82% Eesti lastest kasutavad internetti iga päev, siis Soomes on see näitaja 79%, Suurbritannias 70% ja Saksamaal vaid 55% (Livingstone, Haddon, Görzig ja Ólafsson, 2011). Suurema internetikasutusega kaasneb ka suurem riskide hulk. Internetikeskkond pakub lastele palju häid ja kasulikke võimalusi, kuid sisaldab endas nii materjale kui ka inimesi, kes võivad olla lastele emotsionaalsel ja füüsilisel tasemel ohtlikud.

Erinevate autorite (OECD, 2102; Lobe et al., 2011; Thierer, 2009;) *online*-riskide käsitlusi analüüsides jagaksin internetiohud nelja kategooriasse:

- ebasobiv sisu *(content-related risks*);
- suhtlemisega seotud riskid (*contact-related risks*);
- käitumuslikud riskid (*conduct-related risks*);
- interneti liigkasutamine (*excessive internet use*).

Parema ülevaate saamiseks on *online*-riskid esitatud ka tabelina (tabel 1).

Tabel 1. Peamised lastega seotud *online*-riskid

Ebasobiv sisu	**Suhtlemisega seotud riskid**	**Käitumuslikud riskid**	**Interneti liigkasutamine**
pornograafia; vägivald; rassism; ennasthävitavad materjalid (anoreksia, suitsiid); alkohol ja narkootikumid; ebatsensuurne tekst; relvad; häkkerlus; reklaam; oksjoniportaal; hasartmängud.	võõrastega suhtlemine veebis; *online*-tuttavatega päriselus kohtumised; lapse seksuaalne ahvatlemine; sekstimine[5]; küberkiusamine[6].	isiklike andmete avaldamine; salasõnade levitamine; endast tehtud ebasobivate piltide (video) veebi üles riputamine; end või teist kompromiteerivate kommentaaride postitamine; illegaalsete failide allalaadimine.	ülemäärane ajaveetmine arvutis; eemaldumine perest ja sõpradest; sotsiaalne isolatsioon; õppeedukuse langus; terviseprobleemid.

Ebasobiv sisu *(content-related risks)* on kõige laiem riskide kategooria, kuhu kuuluvad erinevad *online*-materjalid: pildid, tekstid, videofailid, mängud. Segadust võib tekitada see, et iga lapsevanema jaoks tähendab termin „ebasobiv sisu" eri asju, kuna väärtushinnangud ja arusaamad õigest-valest, lubatud-lubamatust on erinevad. Traditsiooniliselt liigitub Euroopas ja Ameerikas ebasobiva sisu alla pornograafia; vägivald ja julmus; rassismi ja vihkamist õhutav materjal; ennasthävitavad materjalid/nõuanded (anoreksia, suitsiid); alkoholi ja narkootikumide tarbimist propageeriv sisu; ebatsensuurne tekst; relvad; häkkerlus; lapsele suunatud reklaam ja kommertslik materjal; oksjoniportaalid; hasartmängud (Net Nanny, 2013; Kaspersky Lab, 2012a).

Lapsed saavad üsna suure osa oma teadmistest ja maailmatunnetusest läbi meedia, kujundavad arusaamad maailmast, õigest-valest, väärtustest just nii, nagu nad seda internetist ja televisioonist vahetult kogevad (Vinter, 2011). Kuna laste elukogemus on veel vähene, kipuvad nad usaldama seda, mida näevad ekraanil; neil kujunevad kergesti

[5] Seksuaalse sisuga sõnumite või fotode vahetamine (Whitby, 2012).

[6] Korduv ja tahtlik isiku ähvardamine, ahistamine, alandamine teise isiku või isikute rühma poolt interneti või mobiiltelefoni teel (Daphne, 2008).

eksitavad väärtused ja uskumused; ebasobivaid materjale hakatakse pidama normiks (American Academy of Pediatrics, 1999). Seega võivad ülalnimetatud materjalid moondada laste arusaamu reaalsusest.

Näiteks pornograafia ja seksistseenid võivad moondada arusaamu mehe ja naise seksuaalsusest, põhjustada muutusi noorte seksuaalkäitumises (Carlsson ja Feilitzen, 2006, viidatud Karu, 2010), mõjuda kehatajule ja enesehinnangule (Whitby, 2012). Uuringute kohaselt 29% Eesti lastest on näinud internetis seksuaalse alatooniga pilte ning 49% lastest tundis end sellest häirituna (Livingstone et al., 2011).

Vägivalda ja agressiooni sisaldavad veebilehed ja videod avaldavad lastele suurt mõju. Lapsed hakkavad vägivaldseid olukordi tajuma kui normaalset igapäevast nähtust, tekib arusaam, et agressioon on loomulik viis probleemide lahendamiseks (Luik, 2009). Näiteks viimase paari aasta jooksul on Eesti meedias mitu korda kirjutatud *happy slapping* juhtumitest koolilaste seas (Delfi, 2012; Postimees, 2012), mis kujutab endast isiku peksmise filmimist ning seejärel materjali levitamist internetis (Politsei- ja Piirivalveamet, 2011).

Web 2.0 kiire areng on loonud info avaldamiseks ja levitamiseks täiesti uued laiemad võimalused ning koos võimalustega on tekkinud ka uued ohud. Näiteks võivad lapsed külastada internetis narkootikumide tarvitamiskogemusi vahendavaid foorumeid või erinevate enesetapuviiside kohta infot jagavaid veebilehekülgi (Boyd, Ryan ja Leavitt, 2011). Populaarsed on noorte seas ka kõhnust propageerivad materjalid, mis on loonud olukorra, et anoreksia muutub üha olulisemaks probleemiks kogu maailmas (Bond, 2012). Enamasti kõik need materjalid, foorumid, blogid ja sotsiaalvõrgustike kogukonnad on kasutajate endi loodud ja nende õigsust on raske kontrollida.

Ei tasu alahinnata ka seda, et internetis võib ohustada lapsi veel reklaam ja tasulised teenused, kuna lastel, eelkõige väiksematel, puudub oskus kommertssisu kriitiliselt hinnata (OECD, 2012). Lapsed võivad ilma loata kasutada vanemate krediitkaardi andmeid või maksta teenuste ja kaupade eest mobiiltelefonilt helistamise või sõnumi saatmisega, kuni vanemad hakkavad tundma huvi suure telefoniarve vastu (Euroopa Komisjon, 2012).

Järgmine ohtude kategooria on **suhtlemisega seotud riskid** *(contact-related risks)*. See on eelkõige võõrastega suhtlemine *online*'is, kohtumised võõrastega päriselus, lapse seksuaalne ahvatlemine, sekstimine, küberkiusamine (OECD, 2012).

Eesti juhib Euroopas edetabelit nii võõrastega suhtlemisel internetis kui ka nendega reaalses elus kohtumisel: 54% Eesti lastest on suhelnud võõrastega *online*'is (keskmine Euroopa näitaja on 30%), ning 25% Eesti lastest on kohtunud võõrastega päriselus (Euroopa keskmine näitaja on 9%) (Lobe et al., 2011). 62% Eesti lastest (6–14 eluaastat) nõustub väitega et „Internet on hea koht uute sõprade saamiseks, kellega hiljem päriselus kohtuda" (Turu-uuringute AS, 2006). Kahjuks teiste inimeste motivatsioon lapsega suhtlusesse astuda ei ole alati läbinähtav ja hea. Lastel puudub elukogemuse pagas, nad on avatud uuele ja seetõttu naiivsed. Lapse jaoks on naiivsus loomulik, aga lastevanematele tähendab see kohustust seletada võimalikke riske seoses nii võõraste inimestega suhtlemise kui ka kohtumisega. On tähtis, et lapsed mõistaksid, et kõik ei pruugi internetis olla tõde – väga tihti kasutatakse seal valenime, vale vanust ning väljamõeldud elulugu. Laste Ekspluateerimis- ja Veebikaitse Keskuse andmetel (CEOP, 2013) on laste seksuaalne ahvatlemine internetis kasvav nähtus. Uuringud on välja toonud, et Eesti lapsevanemad alahindavad laste kokkupuuteid seksuaalse sisuga sõnumitega, näiteks arvab vaid 9% vanemaist, et tema laps on seksuaalsete sõnumitega kokku puutunud. Tegelikkuses on sellega kokku puutunud ligikaudu üks viiest lapsest (19%). (Livingstone et al., 2011)

2010. aastal toimunud uuringu kohaselt on 14% Eesti lastest (vanuses 9–16 eluaastat) viimase 12 kuu jooksul kogenud kiusamist internetis (Livingstone et al., 2011). Küberkiusamine võib olla üks tänapäeva kõige suuremaid internetikasutamise probleeme. Värskemad uuringud (Tuuling, 2013) näitavad, et 2013. aastal tunnistas juba 29% Eesti lastest (14–15 eluaastat), et nad on viimase aasta jooksul küberkiusamise ohvriks langenud. Küberkiusamine avaldab mõju ohvrile nii emotsionaalsel kui ka füüsilisel tasemel (O'Brien ja Moules, 2010), mõnedel juhtumitel võib küberkiusamine põhjustada enesetapukatseid (Daily Mail, 2012). Küberkiusajate motiivid on erinevad, Harris Interactive'i (2007) uuring on välja toonud, et vaid 64%-le ei meeldi kiusatav inimene, aga enamus küberkiusajatest (81%) peab seda lihtsalt naljakaks.

Käitumuslike riskide (*conduct-related risks*) alla käivad mõtlematud teod: isiklike andmete avaldamine, salasõnade levitamine, endast tehtud ebasobivate piltide (video failide) veebi üles riputamine, end või teist kompromiteerivate kommentaaride postitamine, illegaalsete failide allalaadimine jm (Whitby, 2012).

Lapsed võivad kergesti avaldada internetis oma isiklikke andmeid – telefoninumbrit, kodust aadressi, kooli, liikumisharjumusi, fotosid, kuna nad ei teadvusta endale ohte, mida selline

käitumine võib kaasa tuua – andmete kuritarvitamisest kuni füüsiliste rünnakuteni välja (EMT, 2009). Privaatsusriskid tekivad sageli seoses suhtlusportaalis kasutajaprofiili loomisega. 71% Eesti lastest on konto suhtlusportaalis, millest täiesti avalikud on 29% profiile ning 27% avaldavad seal ka isikuandmeid, näiteks kas telefoninumbrit või kodust aadressi (Livingstone et al., 2011). Üsna suur osa lapsi jagab kergemeelselt oma parooli tuttavatega ja sõpradega, kasutab ülikergeid paroole või unustab pärast suhtlusportaali kasutamist ennast välja logida. Sellise ohtliku käitumise tulemuseks võib olla näiteks identiteedivargus. (McAfee, 2009)

Endast kompromiteerivate piltide (või videofailide) veebis üles riputamine või tuttavatele saatmine on samuti riskantne käitumine, kuna neid materjale saab hiljem kasutada pildistatu hirmutamiseks või šantažeerimiseks (Whitby, 2012).

Riiklikult üha enam esile tõusnud probleem seoses illegaalsete failide (filmid, muusika, tarkvara) allalaadimisega, ei ole kahjuks kõige suurem lapsevanemate mure, kui allalaetud tarkvara ei sisalda pahavara või viirusi (Mandre, 2011).

Interneti liigkasutamise (*excessive internet use*) tõttu võivad kannatada lapse sotsiaalsed suhted, õppeedukus, tervis. Näiteks interneti liigkasutamine vähendab vahetut suhtlemist perekonna ja eakaaslastega, jätab vähem aega õppimiseks ja muudeks arendavateks tegevusteks. Kannatab teatud määral ka tervis: väsinud silmad, lihasvalud, ärrituvus, unehäired on interneti liigkasutamise füüsilised sümptomid, mis ilmnevad pideva arvuti ülekasutusega. (Vinter, 2011)

Uuringud näitavad (Lobe et al., 2011), et interneti liigkasutamises on Eesti lapsed Euroopas esikohal, 50% vastanutest on enda puhul täheldanud vähemalt üht interneti ülemäärasele kasutusele viitavat tunnust. Näiteks 30% Eesti lastest surfavad kas „väga sageli” või „üsna sageli” internetis ka siis, kui see huvi ei paku, ning 21% lastest on tulutult püüdnud veeta internetis vähem aega.

Toetudes kahele uuringule (Lobe et al., 2011; Flash Eurobarometer, 2008), võime võrrelda ohtusid, mida Eesti lapsed kõige sagedamini kogevad ja neid, mille üle lapsevanemad kõige rohkem muretsevad (tabel 2).

Tabel 2. Ohud internetis

Eesti lapsed kogevad (Lobe et al., 2011)	**Eesti lapsevanemad muretsevad** (Flash Eurobarometer, 2008)
1. Võõrastega suhtlemine 54%; 2. kasutajate loodud ohtlik veebisisu 36%; 3. seksuaalse alatooniga pildid 29%; 4. võõrastega kohtumine päriselus 25%; 5. seksuaalsete sõnumite saamine *(sexting)* 19%; 6. personaalse info kuritarvitamine 18%; 7. küberkiusamine 14%.	1. Seksuaalne või vägivaldne veebisisu 48%; 2. lapse seksuaalne ahvatlemine 39%; 3. isiklike andmete levitamine 34%; 4. enesevigastuse materjalid (sh suitsiid ja anoreksia) 34%; 5. küberkiusamine 33%; 6. interneti liigkasutamine (sotsiaalse isolatsiooni risk) 33%.

Tabelist on näha, et Eesti vanemad ülehindavad eelkõige seksuaalse veebisisuga seotud ohte, samas on nad palju muretumad lapse seksuaalse ahvatlemise ja küberkiusamisega seonduvas.

On tähtis mainida, et vaatamata väljatoodud riskidele ei ole internet lastele vaenulik keskkond. Enamus veebis toimuvast on arendav, õpetuslik ja huvitav. Pole mõtet võimalikele ohtudele üle reageerida, kuid neid ei tohi ka alahinnata. Tähtsaim ülesanne, mida lapsevanem peab ette võtma, on viia end kurssi võimalike *online*-riskidega, mis lapsi ohustada võivad, ning valida õige strateegiad nende maandamiseks.

1.2 Vanemliku järelevalve strateegiad

Vaatamata sellele, et internet pakub lastele palju häid võimalusi, realiseeruvad need võimalused vaid siis, kui lapsi suunab ja juhendab teadlik täiskasvanu. Informatsioon veebis on sageli küsitava väärtusega ja segadusttekitav ning nõuab orienteerumiseks võimet kriitiliselt mõelda, nähtut ja kuuldut analüüsida, mõtestada ning võrrelda seda tegelikkusega (Vinter, 2011). Seetõttu on vanemate juhendamine laste jaoks ülitähtis.

Terminiga „vanemlik järelevalve“ *(parential mediation)* tähistatakse lapsevanema juhendamist ja kasvatuslikku rolli lapse meediakasutuse jälgimisel ja suunamisel

(Livingstone ja Helsper, 2008, viidatud Oja, 2011). Internetikasutamise vanemlik järelevalve võib väljenduda erinevates kasvatustegevustes: selgitamine, julgustamine, koostegemine, või vastupidi: keelamine ja piiramine (Clark, 2011). Vanemliku järelevalve eesmärgiks on maandada võimalikke *online*-riske ja muuta lapsi iseseisvamaks ning kriitilisemaks internetikasutajaks (Mendoza, 2009).

Vanemliku järelevalve puhul tuuakse üldjoontes välja neli põhilist järelevalvestrateegiat (Hasebrink et al., 2011):

- aktiivne järelevalve *(active mediation)*;
- piirav järelevalve (*restrictive mediation*);
- monitoorimine *(monitoring)*;
- tehniline järelevalve *(technical mediation).*

Aktiivne järelvalve (*active mediation*) on interneti kasutamine koos lapsega, nähtu üle arutlemine, selgitamine, lapse kõrval asumine, kui viimane viibib internetis (Hasebrink et al., 2011). Aktiivne järelvalve on kõige tavalisem lapsevanema rakendatud juhendamise viis. Enamus lapsevanematest vestleb oma lapsega sellest, mida laps internetis teeb, selgitab lapsele meedia sisu ja selle tähendust (Duerager & Livingstone, 2012). Vanemad räägivad lapsega internetiturvalisust, annavad nõu, kuidas laps teistega võrgukeskkonnas suhtlema peaks ning aitavad probleemide korral (Livingstone et al., 2011).

Piirav järelevalve (*restrictive mediation*) on reeglite kehtestamine, mis reguleerivad arvuti ja interneti kasutust (Hasebrink et al., 2011). Uuringu Hart Research Associates järgi (2011) seavad lapsevanemad kõige sagedamini piirangud sisule, kasutuskohale ja ajale („kuidas", „kus" ja „kui palju" reeglid). Näiteks enamlevinud kus-reegel on arvuti kasutamine ühisruumis. Flash Eurobarometeri (2008) uuringu kohaselt on kõige sagedamini kehtestatavad kuidas-reeglid seotud turvalise internetikäitumisega – keelatakse lastele isiklike andmete levitamist, *online*-ostude tegemist, võõrastega suhtlemist, suhtlusportaalides registreerimist ja jututubades suhtlemist, natukene harvem keelatakse külastada teatud veebilehti, alla laadida muusikat, filme ja mänge.

Keelamisstrateegia miinusena võib tuua osade vanemate abitust reeglite kehtestamisel – näiteks vanem on liiga leebe või laps ignoreerib neid. Selle strateegia puuduseks on ka see, et kui vanemad veedavad palju aega kodust väljaspool või kui laps kasutab arvutit oma magamistoas, siis ei saa kontrollida reeglite täitmist.

Monitoorimine *(monitoring)* tähendab, et vanemad kontrollivad samas keskkonnas viibides, mida laps veebis on teinud. See hõlmab külastatud veebilehekülgede, e-kirjade ja saadetud sõnumite (suhtlusprogrammides, foorumites) kontrollimist, suhtlusvõrgustike profiili monitooringut (nt kontaktlisti läbivaatamist, profiililehe ehk seina lugemist). Oluline on märkida, et selle strateegia puhul lapsevanemad teostavad järelevalvet nö käsitsi, ilma spetsiifilist tarkvara kasutamata. (Duerager et al., 2012)

See strateegia on väheefektiivne teismeliste laste puhul, kuna nad õpivad oma internetikäitumist vanemate eest varjama. Näiteks 70% Ameerika noorukitest (13–17-aastased) üritavad oma vanemaid üle kavaldada: 53% lastest kustutab sirvimisajaloo, 20% kasutab veebilehitsejat privaatses režiimis *(private browsing)*, 15% loob salajase e-postkasti, ning 9% loovad sotsiaalvõrgustikes võltsprofiili spetsiaalselt oma vanematele demonstreerimiseks (McAfee, 2012).

Tehniline järelevalve *(technical mediation)* on tehnoloogiavahendite kasutamine järelevalveks ja *online*-riskide vähendamiseks. On olemas palju niisuguseid programme, mis filtreerivad ohtliku veebisisu, monitoorivad laste internetikasutust ning annavad tulemustest vanematele aruandes teada. Selliseid programme nimetatakse „vanemliku järelevalve" või „vanemliku kontrolli" programmideks *(parental control software)*. Lisaks eelpool nimetatule lubavad järelevalve vahendid piirata arvuti ja interneti kasutamisaega, tõkestada isikliku informatsiooni jagamist, kaitsta kasutajat ebasoovitavate kontaktide eest suhtlusprogrammides ja sotsiaalvõrgustikes jne. (GetParentalControls.org, 2010)

Uuringud näitavad (Livingstone et al., 2011), et tehnilise vahendite kasutamine Euroopas on suhteliselt vähepopulaarne. Näiteks ainult 16% Eesti (EE) vanemaist kasutab vanemliku järelevalve vahendeid, Euroopa keskmine näitaja on aga 33%. Kõige rohkem Euroopas kasutatakse tehnilist järelevalvet Suurbritannias (UK) – 54%. Teised Euroopa riigid, kus järelevalve tarkvara on levinud, on Iirimaa (IE) 48%, Prantsusmaa (FR) 44%, Türgi (TR) 38% (diagramm 1). Samuti on selline tarkvara levinud Ameerika Ühendriikides, kus on see kasutuses 54% peredes, kus kasvavad lapsed (Pew Research Center, 2011).

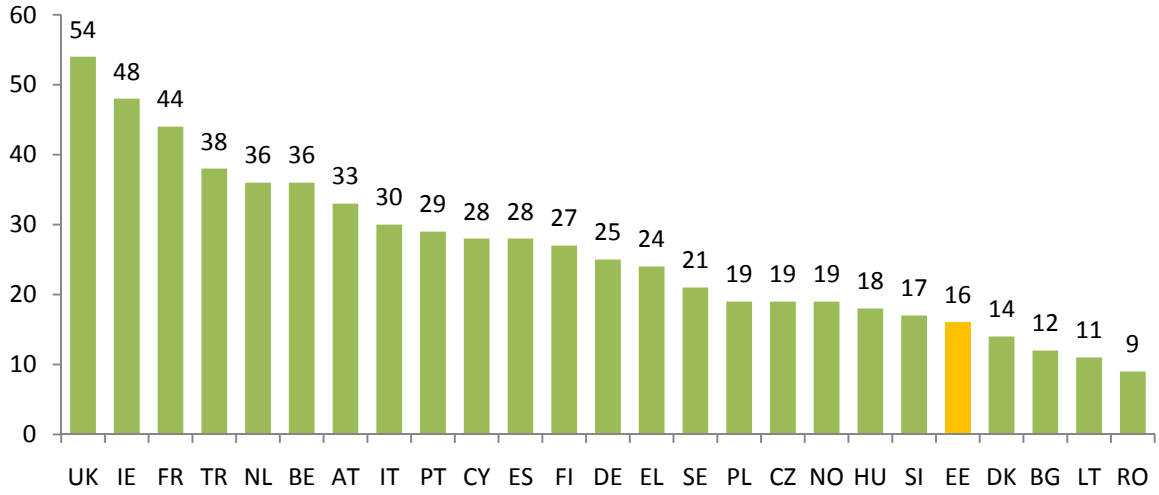


Diagramm 1. Järelevalve tarkavara kasutamine Euroopa riikides (Livingstone et al., 2011).

Vaatamata sellele, et kõik nimetatud järelevalvestrateegiad teenivad laste huve, arvab suur osa lastest Euroopas (44%), et vanemlik järelevalve piirab nende internetikasutust ning vabadust (Hasebrink et al., 2011). Lisaks sellele arvavad lapsed, et vanemlik järelevalve ei ole tõhus: 72% Eesti lastest väidab, et vanemate tegevus ei piira kuidagi seda, mida nad internetis teevad; ning 44% lastest ignoreerib vanemate antud juhiseid (Kalmus, 2013).

Need andmed viitavad sellele, et lapsevanemad peavad ennast internetiturvalisuse valdkonnas täiendama ja otsima uusi võimalusi, kuidas oma lapsi aidata. Et lapsed saaksid uute tehnoloogiatega kaasnevast ilmsest kasust rõõmu tunda, on kaitse loomisel tähtis tegeleda nii lastele vastava hariduse andmisega kui ka vajadusel kasutada tehnoloogiat laste järelevalveks (Daphne, 2008).

1.3 Tehniline strateegia – vanemliku järelevalve tarkvara

Järelevalve tarkvara roll ja kasutamine laste internetiturvalisuse tagamisel on Euroopas aruteludes järjest populaarsem. Näiteks Euroopa komisjon välja töötatud ja avalikustatud „Lastele parema Interneti loomise Euroopa strateegia" (2012) seab üheks eesmärgiks *„vanemliku kontrolli vahendite ulatuslikuma kättesaadavust ja kasutamist"*. Strateegia soovitab Euroopa Liidu liikmesriikidele tagada vanemliku kontrolli vahendite kättesaadavust erinevates keeltes, et eri riikide lapsevanemad saaksid vahendite kasutamise või mittekasutamise üle teadlikult otsustada.

Sama dokument seab reeglid ettevõtetele, et nad peaksid *„tagama kõigis Euroopas saadaolevates internetipõhistes seadmetes hõlpsalt konfigureeritavad, kasutajasõbralikud ja kõigile kättesaadavad vanemliku kontrolli vahendid”*. Lahendusi tuleb ettevõtetel reklaamida, et neist oldaks võimalikult teadlikud ja neid võimalikult palju kasutataks. (Euroopa Komisjon, 2012)

Euroopa Komisjoni tasemel tehakse ka teisi samme riskide vähendamiseks internetis. Näiteks luuakse üha rohkem vahendeid, mille abil saab teatada isiklike andmete kuritarvitamisest või kiusamisest internetis, toetatakse liikmesriikides õigusnormide väljatöötamist, mis mõjutavad laste turvalisust internetis. Rakendatakse seksuaalset vägivalda kajastavatest materjalidest teatamise vihjeliine (nt INHOPE[7]), et saaks kergesti raporteerida sisust ja kontaktidest, mis tunduvad lapsele kahjulikena. Toimub ka veebilehtede, mängude, *online*-videote ning muusika sisu hindamine, et järelevalve programmid ja veebilehitsejad oleksid suutelised *online*-materjale vanuse järgi klassifitseerima. On ilmselge, et laste internetiohutus on tõsine ja kompleksne probleem, mille lahendamiseks tuleb kaasata erinevaid osapooli ja rakendada erinevaid kaitsemehhanisme. (Euroopa Komisjon, 2013)

1.3.1 Vanemliku järelevalve tarkvara

Esimesed järelevalve programmid tulid turule eelmise sajandi lõpus 90-ndatel aastatel. 1993. aastal tuli välja filtreerimise programm „PG-13”, mis kaks aastat hiljem on ilmunud uue nime all „CYBERsitter” (CYBERsitter, 2013). Märkimisväärne on see, et programm on siiamaani vanemliku järelevalve tarkvara turul populaarne toode (Top Ten Reviews, 2013). 1995. aastal tuli välja veel kolm rakendust – Net Nanny, CyberPatrol ja SurfWatch. Tol ajal oli järelevalve programmide funktsionaalsus üsna piiratud, eelkõige filtreeriti veebisisu ja jäeti meelde külastatud veebilehti (Burt, 2002).

Vanemliku järelevalve programmid said kiiresti populaarseks Ameerika Ühendriikides (Heins, Cho ja Feldman, 2006). Näiteks 1997. aastal korraldatud uuringu FamilyPC Survey järgi 26% Ameerika peredest, kus lapsed kasutasid internetti, rakendati erinevaid vanemliku kontrolli vahendeid. 2000. aastal oli see näitaja juba 33% (National Center for Missing and Exploited Children, 2001). Samal ajal 74% Ameerika üldhariduskoolidest kasutas

[7] Eri maade vihjeliine ühendav rahvusvaheline võrgustik http://www.inhope.org

filtreerimistarkvara lokaalses võrgus (National Center for Education Statistics, 2001). Laienes ka programmide funktsionaalsus, tekkis võimalus piirata interneti kasutusaega, blokeerida arvutis erinevaid rakendusi, keelata e-posti ja suhtlusprogrammide kasutamist (Thierer, 2009).

Vanemliku järelevalve vahendid said nii populaarseks, et 2003. aastal otsustas Apple **integreerida vastavad funktsioonid oma operatsioonisüsteemi** Mac OS X (10.3) („Parental Control Software", n.d.). Kolm aastat hiljem tegi seda ka Microsoft oma Vista operatsioonisüsteemiga (Microsoft, 2007). Tuleb märkida, et operatsioonisüsteemi sisseehitatud funktsionaalsused ei ole nii laiad nagu eraldiseisvatel programmidel, kuid on piisavad, et otsustada, kas see strateegia põhimõtteliselt sobib konkreetsele lapsele või mitte.

Paljud tänapäeva turbetarkvara tootjad (Kaspersky Lab, Symantec, F-Secure jt) lisavad **vanemliku kontrolli oma viirusetõrjeprogrammidesse**, mis annab kasutajale võimaluse kaitsta üheaegselt nii oma last *online*-ohtude eest kui ka arvutit viiruste ja pahavara eest. Niisugused programmid pakuvad palju rohkem võimalusi kui operatsioonisüsteemi integreeritud vanemlik kontroll. Miinusena võib tuua vaid selle, et tavaliselt sellised kaks-ühes-rakendused on tasulised ning nende seadistamine võib osutada keeruliseks. (GetParentalControls.org, 2010)

Need kasutajad, kes soovivad lihtsamat lahendust, võivad installeerida **veebilehitseja laienduse** *(add-on, plug-in).* Laiendust on lihtne seadistada ja kasutada, tavaliselt on see ka tasuta ning piiratud funktsionaalsusega, peamine ülesanne on ohtliku veebisisu filtreerimine. Tuleb silmas pidada, et veebilehitseja laiendused ei ole turvalised, nendest saab kergesti mööda hiilida. Seega sobib selline lahendus vaid väiksematele lastele, kes ei ole nii osavad, et laiendust välja lülitada või installeerida mõnda teist veebilehitsejat. (Gizmo's Freeware, 2013)

Üldjoontes võib peamisi vanemliku järelevalve vahendeid jagada neljaks:

- iseseisvad programmid;
- operatsioonisüsteemi integreeritud võimalused;
- viirusetõrje tarkvarasse integreeritud võimalused;
- veebilehitseja laiendused.

Tähtis on mainida seda, et see klassifikatsioon ei ole täielik, sest eksisteerib terve hulk muid vahendeid, mida võib ka pidada vanemliku järelevalve tarkavaraks.

1.3.2 Muud tehnilised järelevalve võimalused

Vanemliku järelevalve vahendina võib vaadelda ka **turvalist otsingut** *(safe search)*. *SafeSearch* on otsingumootorites kasutatav funktsioon seksuaalset sisu sisaldavate veebilehtede eemaldamiseks otsingutulemustest. *SafeSearch* aitab vältida sisu, mida kasutaja ei soovi näha, või soovib, et tema lapsed seda isegi juhuslikult ei näeks. Näiteks Google'i otsingumootoris on vaikimisi sisse lülitatud mõõdukas otsingutulemuste filtreerimine, mis aitab otsingutulemustes ära hoida siivutuid kujutisi. Soovi korral saab määrata seadeks ka „range filtreerimise", mis eemaldab tulemustest lisaks kujutistele ka noortele ebasobivad tekstid. (Google, 2013)

Turvalist otsingut pakuvad kõik populaarsed otsingumootorid: Google, Bing, Yahoo. *SafeSearch* funktsiooni sisaldab ka laste seas populaarne videoportaal YouTube. Siinjuures tuleb mainida, et eksisteerivad ka **lapsesõbralikud otsingumootorid.** Näiteks Kidrex[8] kasutab Google turvalise otsingu tehnoloogiat ning lisaks oma andmebaasi, mis teeb otsingu veel turvalisemaks (Kidrex.org, 2013).

Järgmine vanemliku järelevalve vahend on **lapsesõbralik brauser** *(child-safe browser).* See on veebilehitseja, mis on loodud spetsiaalselt lastele (üldjuhul väikelastele kuni 7 eluaastat). Brauser, millel on lihtne kasutajaliides, sisaldab integreeritud veebisisu filtreerimise ja vanemliku kontrolli funktsioone, nagu näiteks veebiajaloo salvestamine (nt KidsOnlineBrowser[9], KidZui[10], KidSplorer[11]) (PCWorld, 2009).

Veel üks alternatiiv nö klassikalisele vanemliku järelevalve programmile on **lapsesõbralik operatsioonisüsteem** (nt Qimo[12], Edubuntu[13], Kiddix[14]). Enamus lastele mõeldud operatsioonisüsteemidest on loodud Linux baasil, nad sisaldavad palju eelinstallitud mänge ja hariduslikke rakendusi ning reeglina on varustatud internetisisu filtreerimise funktsiooniga (Chaipetta, 2013).

Eksisteerib ka järelevalve programme, millel on **kitsas funktsionaalsus**, nad on loodud, et lahendada spetsiifilisi probleeme. Näiteks Facebooki jälgimiseks on mõeldud rakendus

[8]Lapsesõbralik otsingumootor Kidrex http://www.kidrex.org/
[9]Lapsesõbralik veebilehitseja http://kidsonline.com/kids-browser-download.html
[10]Lapsesõbralik veebilehitseja http://www.kidzui.com/
[11]Lapsesõbralik veebilehitseja http://www.devicode.com/products/kidsplorer?/kidsplorer/
[12]Lapsesõbralik operatsioonisüsteem http://www.qimo4kids.com/what-is-qimo/
[13]Lapsesõbralik operatsioonisüsteem Edubuntu http://www.edubuntu.org/
[14]Lapsesõbralik operatsioonisüsteem Kiddix http://www.kiddix-computing.com/home/index.php

EyeGuardian[15] või ebatsensuursete sõnade blokeerimiseks saab kasutada BadWordsFilterit[16], religioosse veebisisu filtreerimiseks on loodud aga programm GodBlock[17].

Vanemlikku järelevalvet võrgu tasemel *(server-based filtering)* saab korraldada teenusena. Sel juhul loob vanemliku kontrolli seadistused internetiühenduse pakkuja *(Internet service provider, ISP)* ning see rakendub kõikides seadmetes, mida koduses võrgus kasutatakse: süle-, tahvel- ja lauaarvutites, nutitelefonides ja mängukonsoolides. Selliste lahenduste kasutamine on muutumas Euroopas üha tavalisemaks. (Whitby, 2012)

Teenusena on levinud ka veebisisu filtreerimise võimalus DNS serverite kaudu. Kasutaja muudab oma arvutis DNS serveri aadressi ning internetiliiklus käib läbi uue serveri, kus on installeeritud filtreerimise tarkvara. Üks maailma populaarsematest DNS serveritest koos sisufiltriga on OpenDNS[18], mis pakub kodukasutajale palju tasuta võimalusi: filtreerida veebisisu (oma valikul erinevate kategooriate järgi), luua lubatud ja keelatud nimekirja, vaadata internetikasutamise statistikat – milliseid veebilehti külastati ja milliseid blokeeriti (OpenDNS, 2013). Selline lahendus sobib lapsevanematele, kes on huvitatud võimalusest filtreerida ohtliku veebisisu, kuid ei soovi kulutada aega ja raha täisfunktsionaalse järelevalve programmi omandamisele ja tundmaõppimisele. Tuleb silmas pidada, et DNS-i filtreerimisest saab kergesti mööda minna, muutes koduarvutis DNS'i aadressi.

Oma perele sobiva järelevalve vahendi valimisel peab lapsevanem kindlasti arvesse võtma laspe arvutikasutamisharjumusi ja vanust, kuna erineva vanusega lastel on erinevad vajadused (Insafe, 2013a). On tähtis mõista, et ei ole universaalset vanemliku kontrolli programmi, mis sobiks kõikidele lastele. GetParentalControls.org (2010) annab soovitusi, milliseid järelevalve vahendeid kasutada sõltuvalt lapse vanusest. Näiteks väiksemate laste (kuni 7 eluaastat) puhul peetakse tähtsaimaks funktsiooniks veebisisu filtererimist ning veebifilter peab olema sätestatud maksimaalsele turvalisusele *(high level filtering)*, et võimalikult kindlalt kaitsta last ebasobivate *online*-materjalide eest. Märgitakse, et selles vanuses on äärmiselt tähtis lapsevanema kõrvalolek ja otsene jälgimine. Pole mõtet osta kallist multifunktsionaalset programmi, kuna laps tavaliselt veel ei kasuta (või kasutab vähe) e-posti, kiirsuhtlusprogramme, sotsiaalvõrgustikke. Sobib ka Mac'i või Windows'i

[15]Vanemliku kontrolli programm http://eyeguardian.com/
[16]Vanemliku kontrolli programm http://zeinabsoft.com/bad-words-filter/
[17]Vanemliku kontrolli programm http://godblock.com/
[18] Avalik DNS server koos sisufiltriga http://www.opendns.com/

operatsioonisüsteemi integreeritud vanemlik kontroll või ISP pakutav lahendus. Alternatiivina võib lapsevanem installeerida lapsesõbraliku veebilehitseja. Otsingumootorite ja videoportaalide seadistustes peaks olema aktiveeritud turvaline otsing. Neil, kel on lapsed vanuses 8–13 eluaastat, soovitatakse soetada juba täisfunktsionaalne programm, et jälgida lapse suhtlusprogrammide ja sotsiaalvõrgustike kasutamist ning vajadusel blokeerida teatud rakendused (näiteks P2P programmid). Samuti soovitatakse pöörata tähelepanu sellele, et ostetav programm lubaks hallata lapse kontakte (e-postis, kiirsuhtlusprogrammides, sotsiaalvõrgustikes). See võimaldaks lapsevanemal saada ülevaadet, kellega laps suhtleb, ning vajadusel blokeerida ebasoovitavad kontaktid. Alates 14. eluaastast soovitatakse anda lapsele rohkem vabadust ja iseseisvust interneti kasutamisel – vähem piirata ja keelata, kuid jätkata siiski jälgida lapse käitumist võrgumaailmas. (GetParentalControls.org, 2010)

1.3.3 Vanemliku järelevalve tarkvara funktsionaalsus

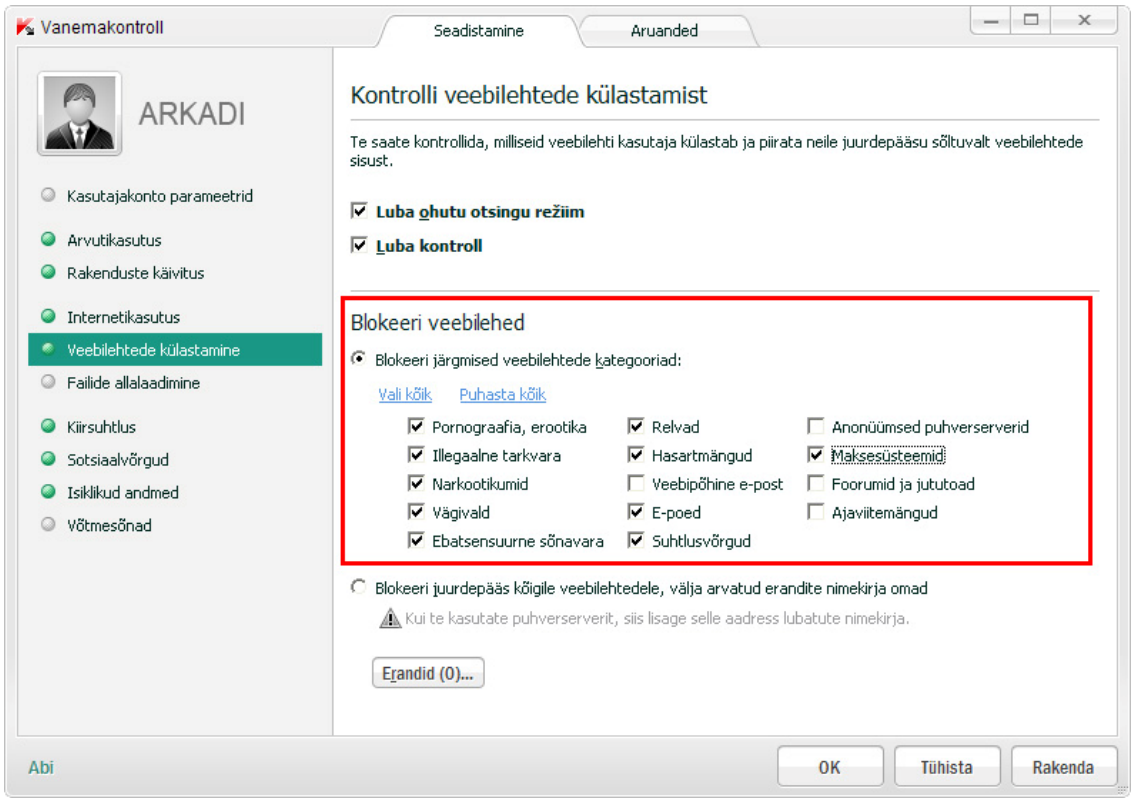
Vanemliku järelevalve vahendid ja nende funktsionaalsused on väga mitmekesised, alustades elementaarsest veebilehitseja laiendusest, mis täidab ühte eesmärki, ja lõpetades täisfunktsionaalsega tarkavaraga, mille pakutavate võimaluste arsenal võib segadusse viia isegi edasijõudnud arvutikasutaja. Enamikul järelevalve programmidel on kolm peamist funktsionaalset valdkonda (Sip-Bench, 2013):

- veebisisu filtreerimine/blokeerimine *(content filtering);*
- kasutuspiirangute seadmine (*usage blocking*);
- lapse internetiaktiivsuse monitoorimine ja lapsevanemale „raporteerimine” (*monitor and report*).

Veebisisu filtreerimine *(content filtering)* on üks peamistest vanemliku järelevalve tarkvara võimalustest ja ülesannetest. Filtrid võimaldavad blokeerida juurdepääsu teatavatele veebilehtedele ning kasutaja võib ise otsustada, milliseid lehti blokeeritakse. (National Computer Board, 2012)

Kasutajale kiire ja mugav võimalus kahtlaseid lehti blokeerida on filtreerimine **kategooriate järgi**, kuna ebasobiva sisu kategooriad on programmis juba eelmääratletud. Tuleb valida neist see, mida peate oma lapsele sobimatuks (nt pornograafia, vägivald, relvad, narkootikumid, oksjonid, hasartmängud jm) ja programm teab juba ise, mida keelata ja mida lubada (Heins, Cho ja Feldman, 2006). Erinevates programmides on need kategooriad

erinevad. Näiteks K9 Web Protection[19] veebifiltris on olemas 69 erinevat kategooriat (lisa 1) (K9 Web Protection, 2013), mida saab märkida keelatuks, samas kui Kaspersky Internet Security pakub 14 kategooriat (Kaspersky, 2012b). Nende hulgas on pornograafia, illegaalne tarkvara, narkootikumid, ebatsensuurne tekst, suhtlusvõrgud, hasartmängud, e-poed jm (pilt 1).



Pilt 1. Veebisisu filtreerimise kategooriad (Kaspersky Internet Security)

Kui veebisisu filtreerimine on aktiveeritud**,** hakkab järelevalve programm tuvastama ja blokeerima määratletud lehti. Blokeerimisel ekraanile ilmub vastav teatis (pilt 2).

Pilt 2. Blokeerimise teatis (Windows Live Family Safety).

[19]Vanemliku järelevalve programm http://www1.k9webprotection.com/

Teine võimalus, kuidas ebasobivat veebisisu **filtreerida**, **on märksõnade järgi.** Selleks peab kasutaja ise sisestama tarkvarasse keelavaid märksõnu (nt „suitsiid", „erootika", „striptiis" jm.). Internetis liikumisel blokeeritakse lehed, mis sisaldavad määratud märksõnu kas metaandmetes[20], veebiaadressis või veebilehe pealkirjades (BitDefender, 2012). Selle meetodi miinuseks on keelelised piirangud; näiteks kui programmi on sisestatud eestikeelne sõna "erootika", siis ei pruugi tarkvara blokeerida saksakeelseid veebilehti, mis sisaldavad sõna „erotik". Kuid on ka edasiarenenud järelevalve programme, mis oskavad skaneerida pildimaterjale ning, sõltuvalt palja naha tekstuurist ja kogusest, tuvastavad pornograafiat (Insafe, 2013a).

Kolmas võimalus veebilehti filtreerida on blokeerimine **veebiaadressi järgi**, mis nimetatakse musta (keelatud) ja valge (lubatud) nimekirja kasutamist. Sellisel juhul saab määrata veebiaadressid (URL-aadressid), mis on kuvamiseks lubatud või keelatud (Sip-Bench, 2013).

Valge nimekiri lubab ligipääsu ainult kindlatele (valitud) lehtedele, kõik ülejäänu blokeeritakse. Valget nimekirja võib olla kasulik kasutada väikese lapse puhul, kelle internetikasutamine on vähene ja piirdub konkreetsete lehtedega (näiteks 3–5 mängulehte) (Insafe, 2013a). Samas võib probleemiks kujuneda see, et näiteks Mängukoobas.ee[21] sisaldab hulgaliselt viiteid teistele keskkondadele, ning siis ei saa laps tegelikkuses ikkagi internetis käimist harjutada, sest enamik veebilehti on keelatud. Lapsevanem peab olema varem lehega tutvunud, et veenduda, mida vastaval lehel koos piiranguga teha saab või ei saa, et vältida oma lapse pettumust interneti kasutamisel.

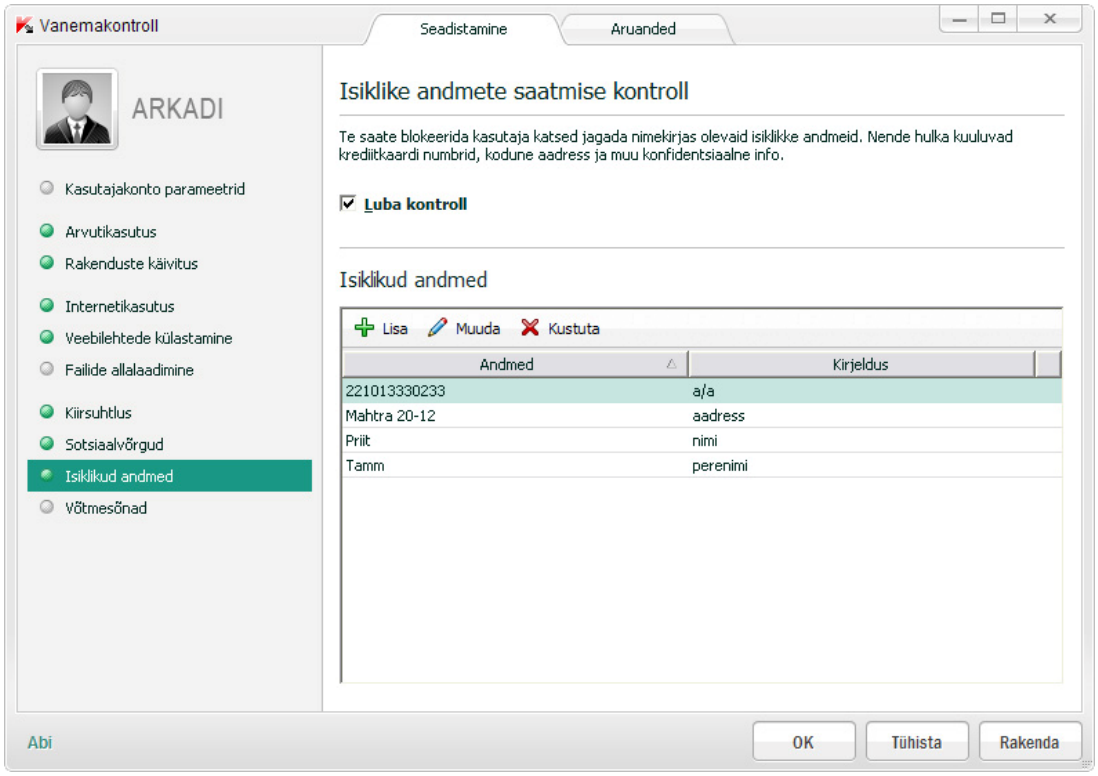
Musta nimekirja puhul valitakse lehed, mille kuvamine on keelatud (kõik teised lehed on lubatud). Peamine probleem on see, et selliseid lehti on internetis tohutult palju, piiratavate aadresside otsimine ja sisestamine on tülikas. Reeglina vanemliku kontrolli programm omab vaikimisi määratud musta nimekirja, mida lapsevanem võib omalt poolt täiendada. (MTAC, 2102)

Kasutuspiirangute seadmine annab võimaluse keelata kas teatud programmide kasutamist, teatud tegevuste sooritamist või seada ajalisi piiranguid. Näiteks võib keelata mängude mängimist, failide alla laadimist, veebikaamera kasutamist või keelata erinevaid

[20] Veebilehe sisu kirjeldavad märksõnad
[21] Eestis populaarne mänguleht http:\\mangukoobas.ee

programme: Windows Media Player, Skype, P2P[22] rakendusi (nt Torrent). Samuti võib keelata ostude sooritamist või näiteks videovoo kuvamist (YouTube, Vimeo). (National Computer Board, 2012)

Isiklike andmete privaatsuse tagamiseks on mõnedel programmidel funktsioon, mis takistab personaalse info avaldamist. Tuleb sisestada programmi sõnad, numbrid ja nende kombinatsioonid, mida programm ei luba internetis (sotsiaalvõrgustikes, e-kirjades, jututubades, foorumites) avalikustada (Kaspersky, 2012c). Näiteks „Priit", „Tamm", „55631120", „Mahtra 20-12" jne (pilt 3). Selle kaitsefunktsiooni kasutamisel tuleb arvestada, et laps võib oma andmeid kirjutada väga erineval moel, sealhulgas ka kirjavigadega.



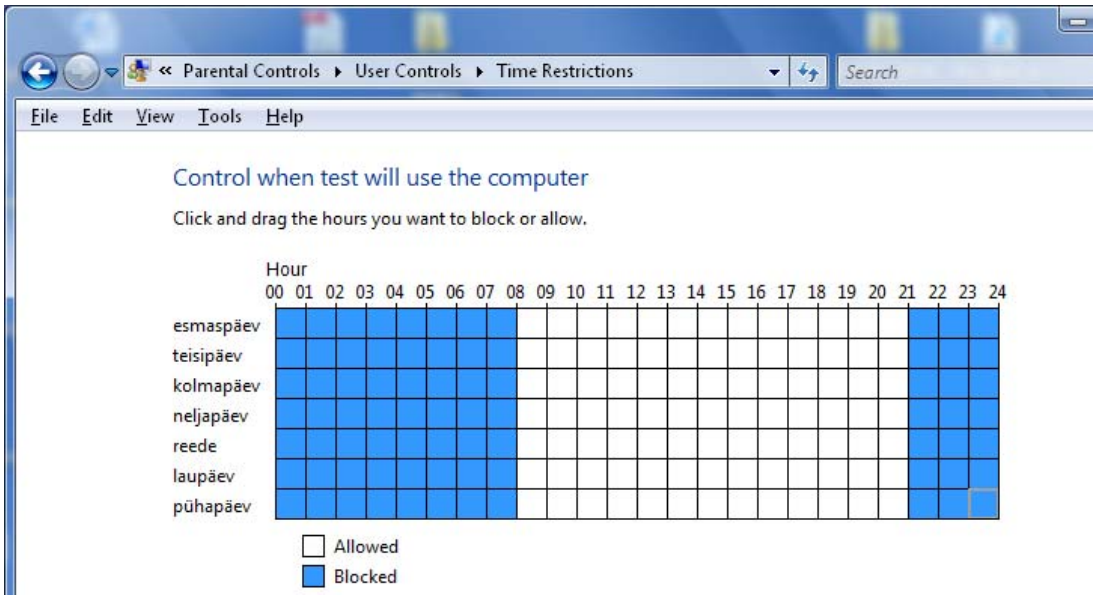
Pilt 3. Isiklike andmete kaitse (Kaspersky Internet Security)

Vanemliku kontrolli piirangud võivad olla seotud ka **suhtlemisega** *online*'is, näiteks on e-posti ja sotsiaalvõrgustikke kasutuse blokeerimine, kiirsuhtlusprogrammide käivituse keelamine. Paljudes järelevalve programmides on kättesaadav ka paindlikum kaitsemehhanism – kontaktide haldamine (*contact management*), mis toimib valge nimekirja põhimõttel, ehk lapsevanem saab valida isikuid (sotsiaalvõrgustikes,

[22] failijagamisprogrammid

suhtlusprogrammides, e-postis), kellega lapsele on lubatud suhelda, kõik teised kontaktid blokeeritakse (National Computer Board, 2012).

Kasutusaja piiramine lubab kehtestada arvutikasutamisele ajalised piirangud. Võimalik on määrata piiranguid tunni ja nädalapäevade kaupa – ajad, millal laps võib arvutisse sisse logida (pilt 3) (Microsoft, 2103). Paljud programmid oskavad eraldi piirata nii arvuti- (*computer usage*) kui ka interneti kasutusaega (*internet usage*) (Sip-Bench, 2013).



Joonis 1. Windows Vista ajapiirangud (laps saab arvutit kasutada iga päev kell 8-21)

Lapse internetiaktiivsuse monitoorimine ja selle aruanne annab võimaluse jälgida ja salvestada lapse aktiivsust arvutis. Üldjuhul võib saada aruande järgmiste asjade kohta:

- külastatud veebilehed;
- veebilehed, mis blokeeriti;
- käivitatud programmid/mängud;
- allalaetud failid;
- meediafailide (muusika, video) loetelu, mida arvutis mängiti;
- saadud ja saadetud sõnumid (e-postis, jututubades, kiirsuhtlusprogrammides, sotsiaalvõrgustikes). (Sip-Bench, 2013; BitDefender, 2012)

Mõned tõhusamad programmid pakuvad ka ekraanipilte külastatud lehtedest (*screenshots*), või lubavad jälgida tegevusi reaalajas. Osa programmidest saadavad lapsevanemale SMSi või e-kirja siis, kui blokeerimine käivitub (Top Ten Reviews, 2013b).

Siinjuures on tähtis mainida, et järelevalve programmid jagunevad tingimuslikult kaheks: nii lapsele nähtavad kui ka nähtamatud programmid, millega saab lapse teadmata tema internetikasutust jälgida. Viimase hulgas on näiteks SpectorPro[23], SniperSpy[24], KidLogger[25], WebWatcher[26]. Psühholoogid aga ei soovita kasutada nähtamatu jälgimise tarkvara, kuna kui laps selle avastab, siis võib hiljem usalduse taastamine osutada raskeks (Whitby, 2012). Samuti hoiatavad turvaeksperdid, et mõned järelevalve rakendused jälgivad tegevusi veebis nii detailselt, et see võib hoopis rikkuda lapse õigusi privaatsusele (Sip-Bench, 2013; Foltz, 2011).

Kokkuvõtteks võib öelda, et järelevalve tarkvara funktsionaalsus on üsna võimas. Kuigi pakutav kaitse ei ole sajaprotsendiliselt tõhus, on see piisavalt lai ja katab suurema osa võimalikest *online*-riskidest, nagu näiteks ohtlik veebisisu, ebasoovitavad kontaktid, privaatsusriskid, mille üle lapsevanemad võiks muret tunda.

1.3.4 Mobiilne vanemlik järelevalve: nutitelefonid ja tahvelarvutid

Mobiilseadmete kasutamine laste ja noorte seas muutub üha populaarsemaks, kuna need vahendid võimaldavad pidevat interneti ühendust ning olla alati *online*'is (Insafe, 2013b). Kaasaskantavate vahendite (mobiiltelefoni või pihuarvuti) abil kasutab internetti kokku 38% Eesti lastest, kusjuures 31% kasutab selleks mobiiltelefoni, mis on Euroopa keskmine tase (Kalmus, 2013). Nutiseadmeid saab edukalt kasutada õppetöös või mõne muu kasuliku tegevuse juures. Samas on oluline silmas pidada, et tegemist on seadmega, mille arutu kasutamine võib põhjustada muret nii lapsele kui ka tema vanemale, milleks on suurenenud telefoniarved, telefoni väärkasutus, tervise halvenemine („Päriselt ka või?", 2013).

Uute seadmetega kaasnevad ka uued probleemid. Näiteks mobiilseadmed on muutunud erinevat sorti ahistamise lihtsmaks, näiteks küberkiusamise teostamise vahendiks on tihti mobiil- ja nutitelefonid (Common Sense Media, 2010). Teine murettekkitav trend on alaealiste seas leviv sekstimine – seksuaalse sisuga sõnumite või fotode vahetamine, kus põhiliseks vahendiks on samuti mobiiltelefon (Whitby, 2012).

[23]Järelevalve programm SpectorPro http://www.spectorsoft.com/products/SpectorPro_Windows/
[24]Järelevalve programm SniperSpy http://www.sniperspy.com/
[25]Järelevalve programm KidLogger http://kidlogger.net/
[26]Järelevalve programm WebWatcher http://www.webwatcher.com/

Nutitelefonide vanemliku järelevalve funktsioonid on seotud nii interneti kui ka telefoni kasutamisega. Mobiilne järelevalve tarkvara oskab veebisisu filtreerida, allalaadimist keelata, piirata interneti kasutamise aega või vajadusel blokeerida internetti (Sip-Bench, 2103). Lisaks sellele on terve hulk funktsioone, mis on seotud telefoni kasutamisega, näiteks saab piirata telefonikõnede ja sõnumite hulka, keelata teatud numbritele helistamise või saada teatud numbritelt kõnesid, võib lubada väljahelistamist üksnes kindlaksmääratud numbritele (Whitby, 2012). Tarkvara abil saab kergesti ülevaate mobiiltelefoni kasutamisest – nii kõnede ja SMS'ide loetelust kui ka külastatud veebilehtedest (PhoneSheriff, 2013).

Nutitelefonide ja tahvelarvutite kõige suurem funktsionaalne omapära on **geolokatsiooni võimalus** (*geolocation).* Geolokatsioonitehnoloogia abil saab kindlaks määrata internetti kasutava inimese täpse asukoha. Paljud vanemad on geolokatsioonitehnoloogiast kuulnud, kuna seda on reklaamitud kui võimalust, millega vanemad saavad oma kodust eemal viibivate laste asukohta tuvastada (Whitby, 2012). Samas võib sellist võimalust ära kasutada ka mõni halb inimene, kes lapsega internetis suhtlusesse on asunud. GPSi (geolokatsiooni) andmed jäävad külge nii tehtud piltidele, videotele kui ka on nähtavad näiteks sotsiaalvõrgustikes (Perry, 2012). Uuring Hart Research Associates (2011) on välja toonud, et 14% Ameerika vanematest, kelle lastel on nutitelefon, kasutavad geolokatsiooni, et saada teada oma lapse asukoht.

Mobiiltelefonide ja tahvelarvutite jaoks on kättesaadav terve hulk vanemliku järelevalve tarkvara erinevatele operatsioonisüsteemidele, nagu näiteks Android, iOS, Symbian, Windows Phone, BlackBerry jm (Top Ten Reviews, 2013c). Väärib mainimist, et Apple'i toodetes (iPhone, iPad, iTouch) on olemas sisseehitatud vanemlik kontroll, mis lubab kontrollida internetis surfamist, ostude sooritamist, ligipääsu erinevatele rakendustele (Apple Inc, 2013).

Sip-Bench (2013) eksperdid, kes testisid mobiilseid järelevalve vahendeid, jõudsid järelduseni, et nii efektiivsuse kui ka funktsionaalsuse osas jääb mobiilne järelevalve maha arvutile mõeldud tarkvarast.

1.3.5 Järelevalve tarkvara – poolt ja vastu

Järelevalve tarkvaral on olemas nii pooldajaid kui ka vastaseid. Enamus lapsevanematest, kes ei kasuta tehnilist järelevalvet, väidavad, et usaldavad oma last ja seetõttu ei tunne vajadust järelevalve programmide järele – Flash Eurobarometeri (2008) uuringu käigus nentisid seda 64% Euroopa vanemaist.

Erinevate uuringute (Jigsaw Research, 2012; Hart Research Associates, 2011) tulemused näitavad, et põhjused, miks ei kasutata vanemliku kontrolli tarkvara, võivad olla ka teistsugused. Näiteks uuring Jigsaw Research (2012) on välja toonud, et järelevalve programmide mittekasutamise peapõhjuseks on vanemate vähene teadlikkus järelevalve tarkvarast ja selle funktsionaalsusest ning vähene arusaam tarkvara töömehhanismist. Lisaks sellele on paljud lapsevanemad tunnistanud, et järelevalve tarkvara on nende jaoks võõras ja keeruline valdkond – neil ei jätku teadmisi ja oskusi, et valida õiget programmi; selle installeerimine ja seadmine tundub vanematele liiga keerukas ja nõuab palju aega ja vaeva. Lisaks selgus mõnede vanemate mure, et programmi kasutamine võib tekitada konflikte lapsega ja usalduse kaotust. Mõned lapsevanemad tõid välja selle, et respekteerivad oma lapse privaatsust ning ei soovi lapse eraellu sekkuda. Osa vanemaist peavad järelevalve tarkvara kasutamist isegi ebaeetiliseks nuhkimistegevuseks. Lapsevanemad, kes põhimõtteliselt ei kasuta järelevalve tarkvara, toovad välja ka argumendid, et nad ei saa isoleerida last reaalsusest, laps peab tutvuma päriseluga ühes oma puuduste ja ohtudega. (Jigsaw Research, 2012)

Üks levinud argument järelevalve tarkvara kasutamise vastu on ka risk piirata võimalusi edukuseks internetis. Seda ohtu tunnistavad nii lapsevanemad kui ka turvaeksperdid. Näiteks EU Kids Online uuringu meeskond jõudis järelduseni, et järelevalve tarkvara kasutamine vähendab nii lapse *online*-riske kui ka lapse meediaoskusi ja võimalusi (Livingstone et al., 2012), seega tekib küsimus, kas turvalisus kaalub üles positiivse internetikasutuse? Tähelepanuväärne on siinjuures, et see, mida vanemad peavad riskiks (näiteks võõrastega kohtumist), näevad lapsed sageli võimalusena (näiteks sõprussidemete loomisena) (Livingstone ja Haddon 2009, viidatud Karu, 2010). Seega piirid võimaluste ja riskide vahel on kohati hägusad ning sõltuvad vaatenurgast ja väärtushinnangutest (Kalmus, Keller ja Pruulmann-Vengerfeldt, 2009).

Pedagoogilisest vaatenurgast on tähtis tegeleda lapse meediakasvatusega, mille eesmärgiks on kriitilise mõtlemise ja meedia sisu analüüsimisoskuse arendamine (Vinter, 2013). On ilmselge, et need oskused arenevad eelkõige aktiivse vanemliku juhendamise käigus (selgitus, arutelu, nõustamine). Aktiivsel järelevalvel arenevad ka laste enesekaitse oskused ja vastutustundlik käitumine võrgus, kuna nad õpivad seda otse vanematelt (Euroopa Komisjon, 2012). Kuid see ei tähenda, et peaks loobuma teistest juhendamise strateegiatest: reeglitest, piirangutest, tehnilistest vahenditest.

Psühholoogid väidavad, et piirangute seadmine on tähtis kasvatusprotsessi osa, eakohased piirid tulevad lapse arengule kasuks ja tagavad lapsele turvatunde (Baumrind, 1991). Lapsevanemal on õigus otsustada, kas need piirangud on ainult suulised või kasutatakse lisaks ka tehnilisi abivahendeid. Mõned vanemad leiavad, et suuliste reeglite seadmine ja vahetu järelevalve on neile raske. Näiteks 17% Ameerika vanemaist tunnistasid, et neil on keeruline jälgida, mida laps teeb internetis ning kellega ta seal suhtleb (Hart Research Associates, 2011). Teatud olukordades võib tehniliste piirangute seadmine võib olla tõhusam ja efektiivsem kui suulised kokkulepped. Näiteks kui laps eirab kokkulepitud reegleid või kui vanemad on tihti kodust ära, siis tehniliste vahendite kasutamine tundub mõistliku otsusena (Thierer, 2009).

Tähtis küsimus järelevalve tarkvara puhul on see, kui efektiivsed on need vahendid tehnilisest küljest; kas nad tagavad loodetud kaitse? Et vastata nendele küsimustele, on Euroopa komisjon rahastanud Sip-Benchi uuringut, mille käigus eksperdid testisid ja evalveerisid erinevaid vanemliku kontrolli vahendeid. Uuringu viimases etapis (talv 2012/2013) analüüsiti 21 järelevalve programmi (lisa 2) (Sip-Bench, 2013). Uuringust selgus, et tarkvara filtreerimise tõhusus sõltub suurel määral veebisisu kategooriast – kõige efektiivsemalt filtreeritakse täiskasvanutele mõeldud materjale. Paljud programmid blokeerivad 90–95% pornograafiat sisaldavatest veebilehtedest. Näiteks blokeeris testi käigus Norton Online Family 95% pornolehti, Kaspersky Pure 93%, Telekom Kinderschutz Software 93%, K9 Web Protection 90% ning Windows Live Family Safety 88%. Vaid üksikud rakendused näitasid kehvi tulemusi, näiteks CyberPatrol suutis blokeerida vaid 65% pornolehtedest. (Sip-Bench, 2013)

Teiste ebasobivate materjalide filtreerimisel näitavad vanemliku kontrolli programmid madalamaid tulemusi. Näiteks vägivalla filtreerimisel näitas kõige suuremat efektiivsust programm Puresight Owl, mis suutis blokeerida 64% vägivalda sisaldavaid lehti, Mobicip

60%, Telekom Kinderschutz Software 59%, aga Windows Live Family Safety blokeeris vaid 13% vägivalda sisaldavatest veebilehtedest (Sip-Bench, 2013). Muu sisu puhul, nagu rassism, enesevigastamine, narkootikumid, hasartmängud, on filtreerimise kasutegur ühtlasi väike – enamik programmidest blokeerib kuni 50% ohtlikest veebilehtedest. Madalat efektiivsust seletavad eksperdid sellega, et suurem osa ebasobivatest materjalidest on kasutajate loodud (blogid, foorumid, suhtlusvõrgud) ning tunnistavad, et web 2.0 sisu filtreerimisel on järelevalve programmid väheefektiivsed (Sip-Bench, 2013). On ilmselge, et suutmatus tõhusalt filtreerida kasutaja loodud sisu on suur puudus, kuna web 2.0 materjalide osakaal internetis pidevalt kasvab ning seda infosisu peavad kasutajad tihti usaldusväärsemaks kui ametlikku infot (Bazaarvoice, 2012).

Vanemliku järelevalve programmide teine üldine probleem seisneb selles, et kahjuliku sisu filtreerimisel võib programm samal ajal tõkestada lubatud ja kasuliku sisu nägemist (Whitby, 2012). Näiteks blokeerivad paljud programmid rinnavähi, soolise võrdsuse, turvalise seksi teemat käsitlevaid materjale või hariduslikke veebilehti narkootikumide kahjulikkusest (Faulkner, 2012). Seda nähtust nimetatakse liigblokeerimiseks (*overblocking*). Sip-Bench (2013) uuringu andmetel on järelevalve programmide keskmine liigblokeerimise näitaja 20–30%, see tähendab, et ligi neljandik blokeeringutest sooritatakse eksikombel. Üleliigset blokeerimist märkavad ka järelevalve tarkvara kasutajad, näiteks 24% Suurbritannia lapsevanemaist nõustus, et vanemliku kontrolli programmid mõnikord tõkestavad neile ja teiste pereliikmetele juurdepääsu soovitud ohututele veebilehtedele (Ofcom, 2013).

Tuleb mainida ka seda, et mõnedel järelevalve programmidel on turvalisusprobleemid – programmi piirangutest möödahiilimine on liiga lihtne. Näiteks võivad lapsed pääseda keelatud veebilehtedele tõlkimissaitide kaudu (nt GoogleTranslate[27]) või Google Cash[28] kaudu. (Sharma, 2013)

Vaatamata kõigile nimetatud puudustele on kasutajate rahulolu järelevalve tarkavaraga suur, 93% Suurbritannia lapsevanematest tunnistas, et tajuvad oma last internetis paremini kaitstuna pärast tarkvara kasutusele võtmist ning vaid 7% vanemaist kahtleb programmi efektiivsuses (Ofcom, 2013). Samal ajal on tähtis meeles pidada, et tehniline järelvalve ei asenda aktiivset juhendamist ja lastevanemate otsest tähelepanu. Kui lapse peal kasutatakse

[27]Populaarne tasuta keeletõlke teenus http://translate.google.com/
[28]Puhverdatud veebilehe koopia

ainult tehnilist järelvalvet, siis see on väheefektiivne ja isegi kahjulik. Oluline on mõista, et tehnilised vahendid jäävad vaid üheks osaks lahendusest ning laste kasvatamist ei tasu jätta tehnika hooleks (Kirna, 2012).

2. Metoodika

Selles peatükis põhjendatakse uurimismeetodi valikut ning kirjeldatakse uuringu läbiviimise etappe ja põhimõtteid. On antud ülevaade uuringusse kaasatud valimist ja andmekogumise protsessist. Töö lisast (lisa 3) on võimalik leida ankeetküsitluse näidis.

2.1 Uuringu etapid

Käesoleva uurimistöö metoodikaks on kvantitatiivne kirjeldav uurimus *(Descriptive research)* (Hirsjärvi, Remes ja Sajavaara, 2005), kus andmekogumisel kasutati internetiküsitlust. Kvantitatiivse meetodi valikuks oli peamiselt kolm põhjust. Esiteks oli töö eesmärk võrrelda vastajate hinnanguid erinevatele järelevalve strateegiatele, mida kõige objektiivsemalt saab teha arvnäitajatega. Teiseks sobib küsimustik kui andmekogumise meetod hästi arvamuste ja käitumispraktikate selgitamiseks. Uuringu käigus sooviti saada ülevaadet vanemate kasutatavatest järelevalvepraktikatest 4–12-aastaste laste puhul internetis ja suhtumisest tehnilisse järelevalvesse. Veebipõhine küsimustik andis hea võimaluse esitada vastajatele suur hulk küsimusi kiiresti ja kompaktsel viisil.

Magistritöö uurimus koosnes kolmest etapist:

- Esimeses etapis identifitseeriti probleem ja sõnastati uurimisküsimus. Lähtuvalt uurimisküsimustest oli valitud sobiv uurimismeetod – küsitlus.
- Teine etapp oli küsimustiku loomine ning andmete kogumine. Koostasin veebipõhise küsitluse, mis sisaldas 36 küsimust. Andmete kogumiseks leidsin osalejad nn lumepallimeetodit *(snowball sampling)* kasutades (Fricker, 2012): jagasin ankeeti Facebooki keskkonnas ja saatsin välja kümnele vastajale, kes jagasid seda omakorda välja järgmistele vastajatele. Küsitlus viidi läbi kahe kuu jooksul vahemikus detsember 2012 – jaanuar 2013.
- Kolmandas etapis analüüsisin kogutud andmeid kirjeldava statistika meetoditega. Seejärel toimus tulemuste sõnastamine, kokkuvõtete ja ettepanekute tegemine.

2.2 Valimi moodustamine

Uuringu valimi moodustasid 77 lapsevanemat. Mittetõenäosuslik valim oli moodustatud internetikeskkonnas lumepallimeetodina. Lumepallimeetodi idee on sarnane

mugavusvalimile: kasutasin algselt enda poolt valitud isikuid ning valim laienes vasta-ise-ja-jaga-sõpradele-põhimõttel (Toompalu, 2010). Koostatud küsimustiku saatsin e-kirjaga laiali ja jagasin Facebooki keskkonnas, paludes seda täita ja edasi levitada. Valimile oli määratud piirang, et küsitluses saavad osaleda 4–12-aastaste laste lapsevanemad, kelle lapsed kasutavad arvutit ja internetti. Antud vanusevahemiku valisin seetõttu, et just need vanemad oleksid potentsiaalsed järelevalve tarkvara kasutajad.

Küsimustikule vastas kokku 77 inimest, neist oli 67 naist ja 10 meest. Tüdrukute vanemaid oli 47 ja poiste vanemaid 30. Vastanute hulgas on 59 inimest kõrgharidusega ja 18 kutseharidusega. Eelkooli laste (4–6-aastaste) lapsevanemaid on 21, 7–9-aastaste laste lapsevanemaid on 20 ja 10–12-aastaste laste vanemaid on 36.

Oluline on rõhutada, et valimi suurus ei anna võimalust teha üldistusi terve Eesti ehk kõikide Eesti lapsevanemate kohta. Kõik järeldused, mis on tehtud selle töö empiirilises osas, puudutavad vaid konkreetset valimit. Samamoodi on valimis rohkem naissoost vastajaid, mis seab samamoodi piirangu üldistamiseks.

2.3 Andmete kogumine ja andmeanalüüs

Uuringu küsitlus läbi viidi vahemikus detsember 2012 – jaanuar 2013. 36 uuringuküsimust jagunesid viieks osaks:

- küsimused lapse arvuti- ja internetikasutamise kohta (7 küsimust);
- lapsevanemate mured ja hirmud seoses laste internetikeskkonnas viibimisega (5 küsimust);
- küsimused lapsevanemate rakendatavatest järelevalvestrateegiatest (9 küsimust),
- lapsevanemate arvamused ja ootused järelevalve tarkvara suhtes (8 küsimust)
- demograafilised küsimused (7 küsimust).

Enamik küsimusi oli valikvastustega (12 küsimust) ja Likerti-skaala (Johns, 2010) küsimused (9 küsimust), kuid oli ka avatud vastustega küsimusi (8 küsimust), mis andsid vastajale võimaluse selgitada oma eelnevalt tehtud valikuid. Ankeedile vastamine toimus anonüümselt.

Küsimuste koostamisel olid võetud aluseks reaalsete järelevalve programmide funktsionaalsused ja võimalused, mida tutvustasin teoreetilises osas. Näiteks potentsiaalselt

ohtlikke *online*-tegevusi puudutav küsimus (nr 16) ja potentsiaalselt ohtlikke online-materjale puudutav küsimus (nr 17) põhinevad Sip-Bench uuringu materjalidel, mille käigus olid testimisel enamlevinud järelevalve programmid. Sama uuringu tulemustel põhineb ka järelevalve vahendite funktsioonide loetelu, mille tähtsust oma perele palusin lapsevanematelt hinnata küsimustes 18 ja 19. Küsimuste koostamisel olid sisendiks ka teoreetilises osas käsitletud *online*-riskid ja järelevalvestrateegiad.
Küsimuste vastused on analüüsitud tervikuna (kõik vastajad koos) ning seejärel filtreerituna lapsevanemate hariduse ja soo lõikes ning laste vanuse ja soo lõikes. Andmeanalüüsi käigus kasutasin kirjeldava statistika meetodeid: arvnäitajaid, diagramme ja sagedustabeleid. Andmete töötlemine ja analüüsimine oli läbi viidud MS Exceli tarkvara baasil.

Ankeedi koostamine ja täitmine toimus WebAnketa[29] keskkonnas. Selle keskkonna valisin seetõttu, et see annab võimaluse kasutada kõiki soovitud küsimuste tüüpe ja pakub sisseehitatud statistika ja andmeanalüüsi tööriistu.

[29] Veebipõhiste küsimustike koostamise vahend http://www.webanketa.com

3. Tulemused

Töö kolmandas osas on esitatud tulemused ja järeldused, mis kujunesid välja uuringus korraldatud küsitluse käigus. Esimeses peatükis tuuakse välja riskid, mida lapsevanemad tajuvad ja peavad probleemseks seoses laste internetikasutamisega. Teises alapeatükis kirjeldatakse strateegiaid ja meetmeid, mis kasutavad lapsevanemad selleks, et jälgida laste toiminguid internetis. Kolmandas alapeatükis keskendutakse tehnilise järelevalve strateegiale, analüüsitakse lapsevanemate arvamusi ja ootusi järelevalve tarkvara suhtes.

3.1 Riskid, mida lapsevanemad tajuvad ja probleemseks peavad seoses laste internetis viibimisega

Küsitluses osalenud lapsevanemad (96%) mõistavad, et internet võib olla potentsiaalselt ohtlik keskkond nende lapsele. Ohtlikumaks peavad internetti madalama haridusega lapsevanemad, kellel on nooremad lapsed (4–6-aastased), kui need, kellel on kõrgem haridus või kelle lapsed on vanemad (7–12-aastased).

Ligi neljandik (26%) vastanutest tunnistab, et nende laps on kogenud midagi negatiivset seoses internetiga viimase kuue kuu jooksul. Lastele antakse palju vabadust arvuti kasutamisel, näiteks 30% lapsi kasutab arvutit administraatori õigustes. See tähendab, et laps saab iseseisvalt installeerida ja eemaldada arvutiprogramme ilma oma vanemaid sellest teavitamata. Vanemate laste puhul (10–12 a) on see protsent märgatavalt kõrgem (50%), võrreldes eelkooli lastega (14%).

Keskmiselt viibib laps arvuti taga ligikaudu 90 minutit päevas, eelkooli laste puhul on see näitaja 60 minutit, ning koolilaste jaoks (7–12 a) kaks korda suurem – 120 minutit päevas. Koolieelikutest kasutab internetti igapäevaliselt 38% ning koolilastest 69%. Isiklikku arvutit või sülearvutit omab 26% lastest. Üldjuhul on need lapsed vanuses 10–12 eluaastat ning kasutavad arvutit ja internetti märgatavalt rohkem, s.t viibivad arvutis ligi 150 minutit päevas, 55% teeb seda administraatori õigustes, 85% kasutab internetti igapäevaliselt. Isikliku arvuti olemasolu suurendab seega nii arvuti kasutamise aega kui ka *online*-riskidega kokkupuutumise hulka.

Peamised *online*-riskid, mida lapsevanemad peavad probleemseks, on seotud suhtlemisega, osalemisega võrgustikes või foorumites. Lapsevanemad näevad kõige rohkem ohtu

suhtlemisel jututubades ja suhtlusvõrgustikes (diagramm 2). Rohkem kui neljandik vastanutest peab seda „väga ohtlikuks", ning umbes pool vastanutest „mõõdukalt ohtlikuks". Ohtlikuna tajuvad lapsevanemad ka failide allalaadimist ja nende avamist, foorumites suhtlemist, veebikaamera kasutamist suhtlemisel ja veebis surfamist. Lapsevanemate arvates kätkevad väiksemat ohtu kiirsuhtlusprogrammid (nagu Skype) ja *online*-mängud. Internetis video vaatamist (nt YouTube), infootsingut ja e-posti kasutamist hindavad enamik lapsevanematest pigem „mitteohtlikuks" või „väheohtlikuks". Ohtlike tegevustena toovad vanemad välja ka fotode ja isikliku informatsiooni avalikustamist internetis, piltide üles laadimist, programmide installeerimist.

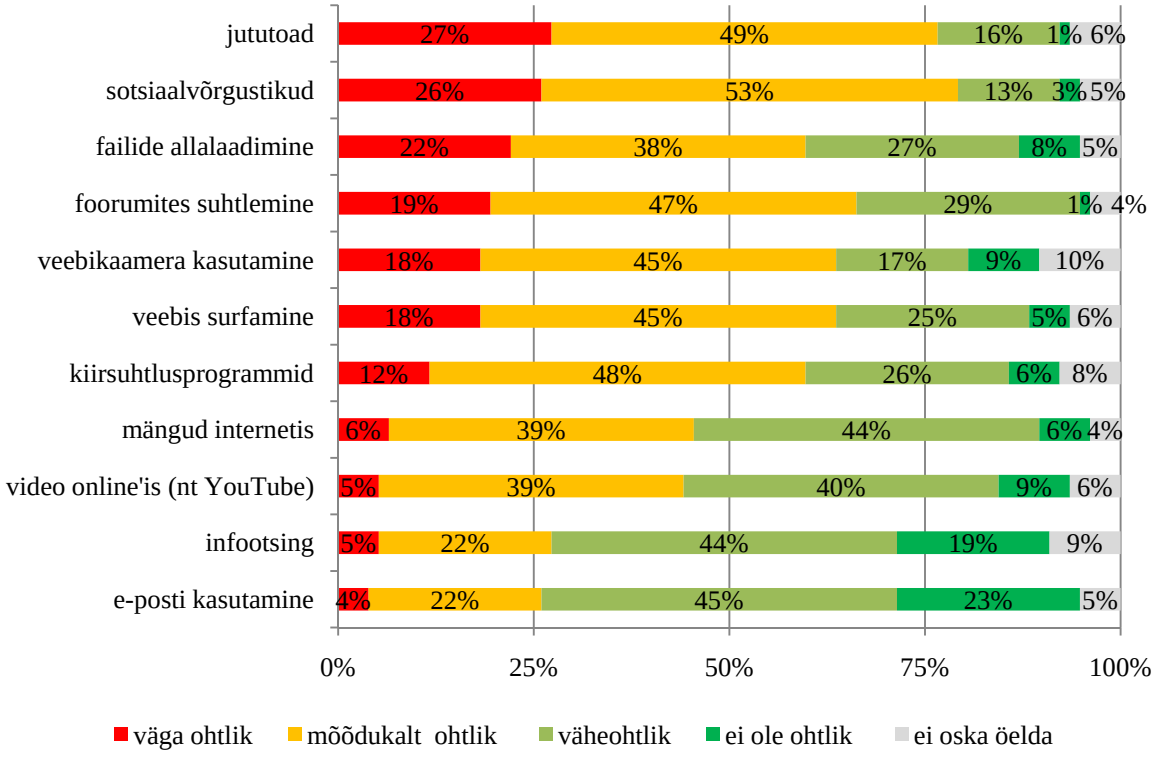


Diagramm 2. Lapsevanemate hinnangud potentsiaalselt ohtlikele online-tegevustele (kõik vastajad).

Analüüsides tulemusi laste vanuse lõikes ilmneb tendents, et nooremate laste vanemad muretsevad enam internetiturvalisuse pärast ja näevad ka suuremat ohtu erinevates *online*-toimingutes. Näiteks 29% eelkooliealiste laste vanematest peab internetis surfamist potentsiaalselt „väga ohtlikuks", 7–9-aastaste laste vanemate hulgas see arv on juba madalam – 25%, ning 10–12-aastaste laste vanemate seas langeb see näitaja 8%-le. Kui infootsingut peab „väga ohtlikuks" 19% eelkooliealiste laste vanemaist, siis kooliealiste laste vanemate hulgas on see näitaja hoopiski 0%. Koolieelikute vanemad on rohkem mures ka sotsiaalvõrgustike pärast – 38% peab neid „väga ohtlikuks", kuid 10–12-aastaste laste

vanematest on see protsent 19%. Tulemused viitavad sellele, et 10–12-aastaseid lapsi peavad lapsevanemad sageli piisavalt teadlikeks ja arvavad, et viimased tulevad ise paljude *online*-probleemidega toime.

Tüdrukute lapsevanemad hindavad erinevaid *online*-toiminguid ohtlikumaks, kui poiste vanemad. Tüdrukute lapsevanemad peavad kõige ohtlikumaks *online*-tegevuseks suhtlusvõrgustikus suhtlemist, samas kui poiste vanemad jututubades suhtlemist.

Kõige ohtlikum veebisisu on lapsevanemate arvates seksuaalsed materjalid, 87% vastanutest hindas neid „väga ohtlikuks" (diagramm 3). Seega hinnati pornograafiat ohtlikumaks kui enesevigastamisele ja suitsiidile õhutavaid materjale või vägivalda ja julmust propageerivaid veebilehti. Huvitav on see, et tüdrukute vanemad on rohkem mures pornograafia pärast: 94% peab seda „väga ohtlikuks", samal ajal aga poiste vanemate seas see näitaja on 79%. Ohtlikeks peavad lapsevanemad ka rassistlike materjale ja narkootikumide propageerimist. Veidi leebemini suhtutakse hasartmängudesse, relvadesse, ropendamisse, häkkimisse ja piraatlusesse.

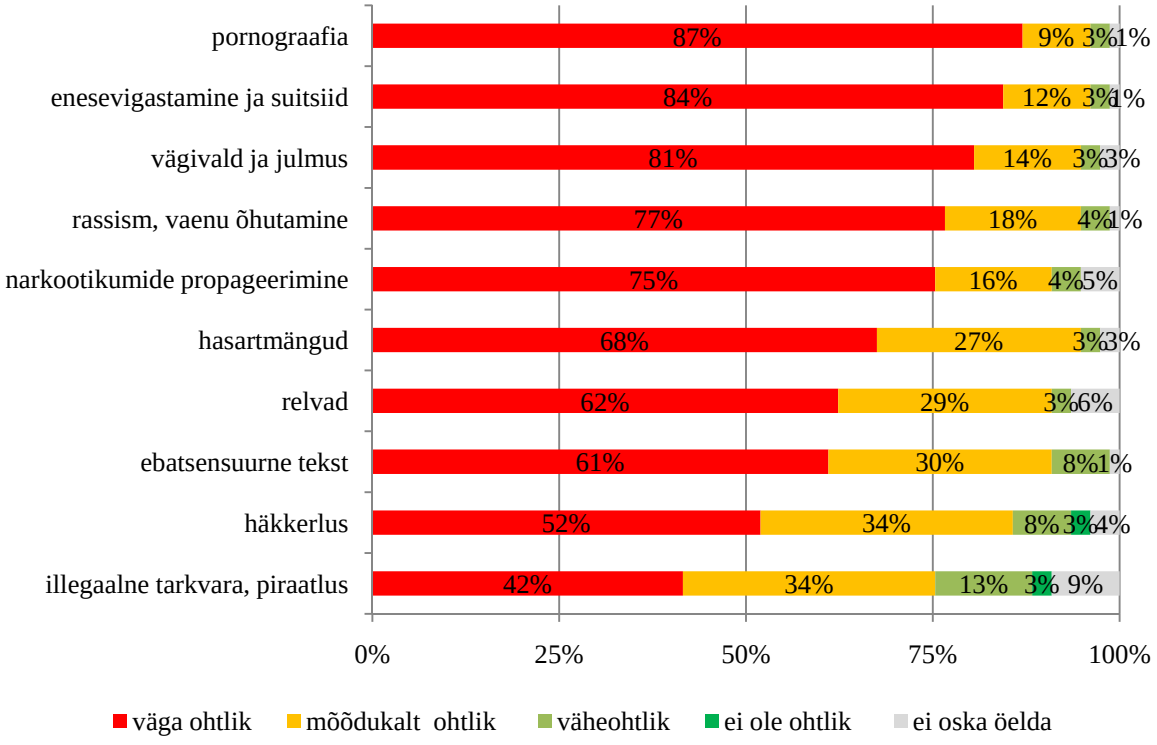


Diagramm 3. Lapsevanemate hinnangud potentsiaalselt ohtlikele *online*-materjalidele (kõik vastajad).

Vaadates tulemusi laste vanuse lõikes selgub, et nooremate laste (4–6 a ja 7–9 a) vanemad muretsevad kõige enam pornograafia üle ning 10–12-aastaste laste vanemad peavad kõige

ohtlikumaks veebisisuks enesetappu ja enesevigastamist propageerivaid veebilehti. Vanemate laste (10–12 a) vanemad näevad ohtu ka rassistlikes materjalides ja hasartmängudes. Eelkooli laste vanemad hindasid kõige ohtlikumaks pornograafiat, vägivalda, narkootikumide propageerimist ja ebatsensuurset teksti. Kõikides vanusegruppides kõige sallivam suhtumine on piraatlusse ja tarkvara ebaseaduslikku allalaadimisse.

Tüdrukute vanemate seas peeti kõiki *online*-materjale ohtlikumateks kui poiste vanemate puhul. Poiste lapsevanemate arvates on kõige ohtlikum veebisisu enesetappu ja enesevigastamist propageerivatel, tüdrukute vanemate hinnangul aga pornograafiateemalistel veebilehtedel. Ohtlike teemadena olid nimetatud ka e-kaubandus ja lastele suunatud internetireklaam. Samas üks vastanutest märkis, et *„pole ohtlikke teemasid, on ainult kehv selgitustöö”*.

Last peavad *online*-riskide eest kaitsma lapsevanemate arvates eelkõige nemad ise (diagramm 4). Samal ajal vaid 52% lapsevanemaist hindas oma teadmisi internetitohutuse valdkonnas heaks. 35 % lapsevanemaist tunneb puudust internetiohutuse materjalidest ning leiab, et selliseid materjale võiks lapsevanematele olla rohkem.

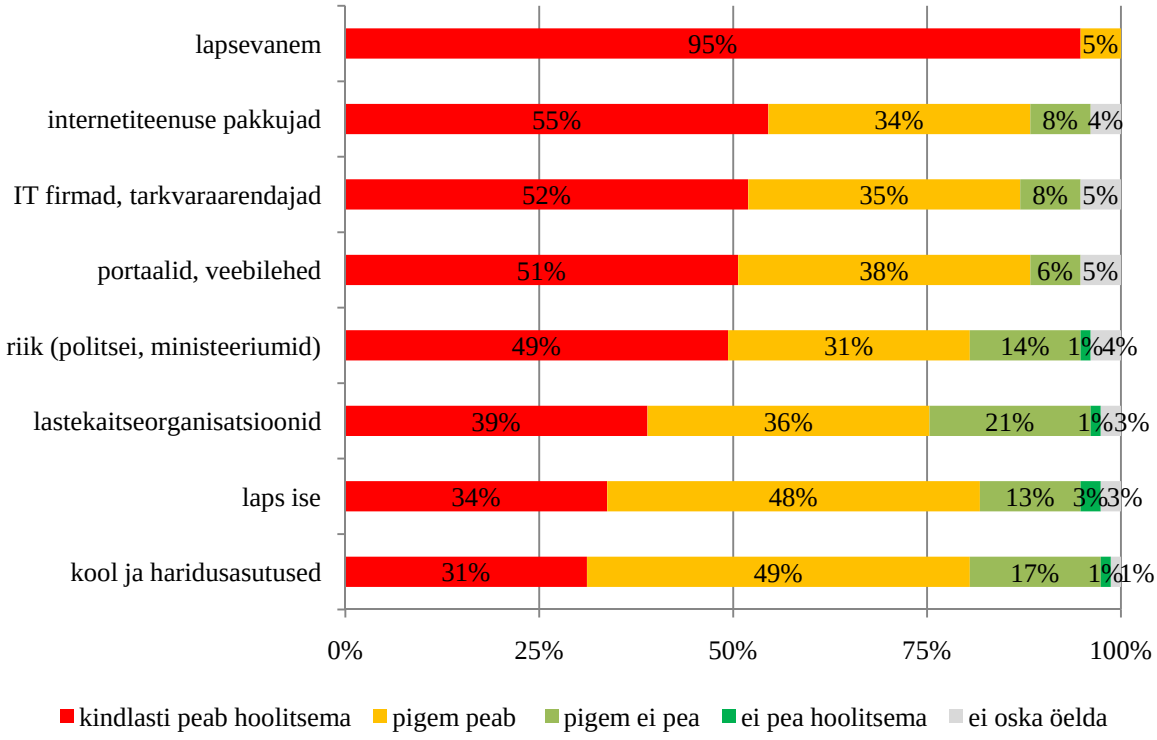


Diagramm 4. Kes peab hoolitsema internetiohutuse eest? (kõik vastajad)

Enamus (89%) lapsevanematest arvab, et interneti turvalisuse peavad lastele tagama ka internetiteenuse pakkujad (ISP). Mõnedes Euroopa riikides (nt Prantsusmaa, Suurbritannia, Saksamaa) on saanud kombeks, et internetiteenuse pakkuja pakub võrgu tasemel nii viirusetõrjet kui ka vanemliku kontrolli. Kahjuks peab tõdema, et Eestis sellist teenust veel ei ole. Aga see fakt, et lapsevanemad ootavad internetiteenuse pakkujatelt selles osas tuge, annab lootust, et niisugune praktika levib tulevikus ka Eestis.

Internetiohutuse eest peavad hoolitsema ka veebiportaalid ja nende omanikud, oma panuse peavad andma veel IT-firmad ja tarkvaraarendajad. Väiksemal määral loodavad lapsevanemad riigile ja lastekaitseorganisatsioonidele. Kõige vähem on neid lapsevanemaid, kes ootavad abi koolidelt ja teistest haridusasutustelt – ainult 31% vastanutest arvab, et kool „peab kindlasti hoolitsema" laste internetiturvalisuse alase hariduse eest. Samas diagramm 4 näitab selgelt, et enamus vanematest on veendunud, et internetiohutus on ühine probleem ja sellega peaksid tegelema kõik organisatsioonid, kes lastega kokku puutuvad või neile teenuseid osutavad.

Kokkuvõttes võib öelda, et kõige suurematekskes *online*-ohtudeks lastele peetakse pornograafiat, enesetappu ja enesevigastamist propageerivaid veebilehti ning suhtlemist võõraste inimestega jututubades ja sotsiaalvõrgustikes. Lapsevanemate arvates peavad lapsele turvalise interneti tagama nad ise ja selles oodatakse abi ka internetiteenuse pakkujatelt.

3.2 Järelevalvestrateegiad, mida lapsevanemad kasutavad, et kaitsta oma last *online*-riskide eest

Küsitluse vastused näitasid, et enamus lapsevanematest pürgivad ise kontrollima oma lapse tegutsemist *online*'is. Väitega „*lapsevanemal peab olema täielik kontroll selle üle, mida laps teeb internetis*", millega nõustus 84% lapsevanemaist. Selleks kasutavad lapsevanemad erinevaid järelevalvestrateegiaid.

Praktiliselt kõik vanemad (välja arvatud üks) kasutavad **aktiivse järelevalve meetodeid**. Kõige populaarsem viis teada saada oma lapse *online*-tegevustest on vestlus: 62% vastanuist räägib lapsega „regulaarselt" või „üsna sageli" sellest, mida ta teinud ja näinud internetis (diagramm 5).Teisalt 54% lapsevanemad julgustavad last *online*-muredest neile rääkima,

tehes seda „regulaarselt” või „üsna sageli”. Märkimist väärib ka see, et 8% lapsevanematest ei julgusta oma last kunagi internetis toimuvast rääkima. Tihti kasutatakse võimalust olla lapse lähedal, kui viimane viibib internetis, et vahetult kontrollida ja juhtida internetikasutust. Vähem on levinud lapsevanemate seas vestlemine interneti turvalisuse teemadel ning interneti kasutamine koos lapsega sama arvuti taga olles.

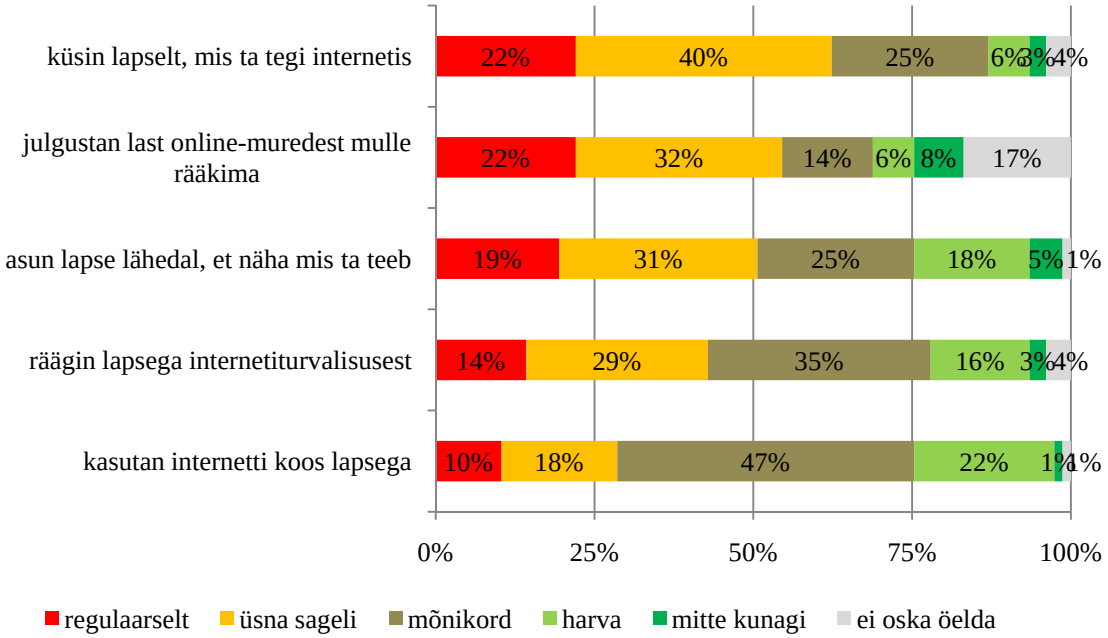


Diagramm 5. Aktiivse strateegia meetmete kasutamine (kõik vastajad)

Järelevalvemeetodi valik sõltub lapse vanusest. Näiteks väiksemate laste puhul (4–6 a) on kõige levinum meetod lapsevanema kohalolu samas ruumis või kasutatakse arvutit koos lapsega, 86% eelkooli laste vanematest teeb seda „regulaarselt” või „üsna sageli”. Kui laps saab vanemaks, siis vahetu kontroll nõrgeneb. Vanemate laste puhul (10–12 a) ei peeta lapsevanema juuresolekut enam nii oluliseks, vaid 25% lapsevanematest „regulaarselt” või „üsna sageli” asub lapse lähedal, kui viimane kasutab internetti või arvutit. Üldiselt võib öelda, et vanemaid lapsi kipuvad lapsevanemad kontrollima suuliselt ja väikesi lapsi eelistatakse jälgida vahetult, asudes lapse kõrval. Vastused tõid ka välja, et väiksemate lastega räägitakse tunduvalt vähem internetiturvalisusest. Näiteks kui 10–12-aastaste lastega räägib 53% lapsevanemaist „regulaarselt” või „üsna sageli”, siis eelkooliealiste lastega teeb seda ainult 24%. Kõige sagedasem kontrollimeetod on küsimus: „*Mida täna veebis tegid*? *Mis täna internetis juhtus*?“ Samas internetis juhtunud probleemidest julgustatakse pigem rääkima tüdrukuid kui poisse.

Vastuste analüüs lapsevanemate hariduse lõikes näitas, et kõrgharidusega vanemad kasutavad aktiivse järelevalve meetmeid harvem kui kutseharidusega lapsevanemad.

Näiteks koos lapsega „regulaarselt" kasutavad internetti 22% kutseharidusega vanemaist, samas kui kõrgharidusega lapsevanematest teeb seda ainult 7%.

Kui vaadata tulemusi lapsevanemate soo lõikes, siis selgub, et aktiivsete järelevalve meetodite rakendamine on pigem emade mure. Näiteks 66% küsitlus osalenud emadest küsib „regulaarselt" või „üsna sageli" lapselt mis viimane internetis teinud on, isade hulgas see näitaja on 40%. Emad räägivad lastega sagedamini internetiturvalisusest ja ka viibivad lapse kõrval, kui ta arvutit kasutab.

Monitoorimise strateegia osutus vastanute seas vähem populaarseks kui aktiivne järelevalve – umbes neljandik vastanutest ei kasuta monitoorimise meetmeid. Kõige levinud viis monitooringu teostamiseks on veebilehitseja ajaloo kontrollimine, 21% lapsevanematest teeb seda „regulaarselt" või „üsna sageli" (diagramm 6). Mõnevõrra harvem kontrollitakse lapse sotsiaalvõrgustike profiile ja kontaktinimistut kiirsuhtlusprogrammides (nt Skype'is). 8% vanematest kontrollib „regulaarselt" või „üsna sageli" lapse e-postkasti sisu, 32% ei tee seda aga kunagi. Seadusandlikust vaatest võiks aga Eestis sellist e-posti kontrollimist pidada sõnumisaladuse rikkumiseks (karistusseadustik, §156), kui seda tehakse lapse teadmata või tema tahte vastaselt.

Diagrammil torkab silma suur „*ei oska öelda*" vastanute osakaal, tõenäoliselt see on seotud sellega, et kas pole olnud vajadust oma last sellisel viisil kontrollida, kas vastavat kontrollimeetodit peetakse väheefektiivseks või siis puudub sellekohane teave üleüldse.

Monitoorimisstrateegia mittekasutamise põhjusena toovadki lapsevanemad kõige sagedamini välja oma lapse usaldamist – *„mul on ligipääsud tema Facebooki ja meilikontodele, vajadusel saan käia kontrollimas, mida ta internetis teeb. Aga üldiselt ma usaldan teda."*

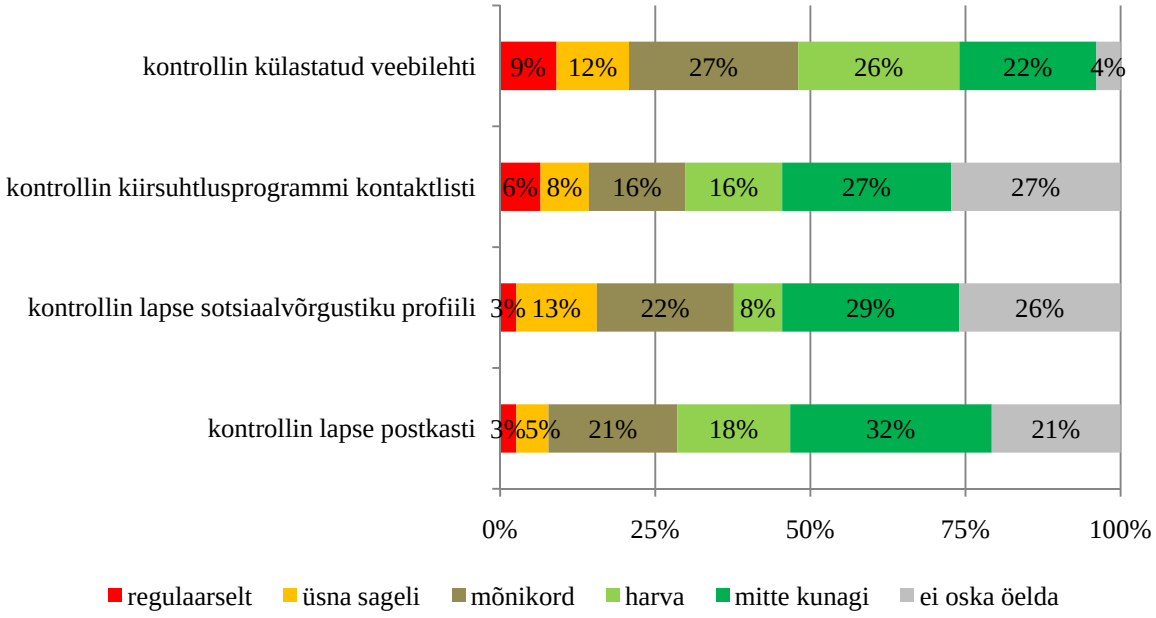


Diagramm 6. Monitoorimise strateegia meetmete kasutamine (kõik vastajad)

Vanemate vastused toovad välja, et monitoorimisstrateegia meetmeid püütakse pigem rakendada vanemate laste puhul. See on tingitud asjaoluga, et väiksed lapsed ei kasuta eriti selliseid internetiteenuseid nagu e-post, sotsiaalvõrgustikud, suhtlusprogrammid ning nende järele jõutakse valvata otseselt, lapse juures viibides. Vanuse kasvades veedab laps internetis rohkem aega ja seetõttu kasvab ka vanema vajadus lapse toiminguid monitoorida.

Kui vaadata tulemusi vanemate hariduse lõikes, siis selgub, et kutseharidusega lapsevanemad kalduvad rohkem oma last kontrollima kui kõrgharidusega vanemad. Samuti kontrollitakse poisse rohkem kui tüdrukuid. Näiteks kontrollib külastatud veebilehti „regulaarselt" 13% poiste ning vaid 6% tüdrukute vanemaist.

Uurimusest selgus, et uuringus osalenud emad kasutavad monitoorimise meetmeid märgatavalt sagedamini kui isad. Emade hulgas kõige populaarsem kontrollimise meetod oli sirvimisajaloo ülevaatamine, isade hulgas sotsiaalvõrgustike profiilide monitoorimine.

Piirav järelevalvestrateegia on vanemate seas peaaegu sama populaarne kui aktiivne, 86% peredes on kokku lepitud reeglid, mis reguleerivad laste meediakasutust. 81% perekondadest on reeglid seoses arvuti ja interneti kasutamisega, 51% televiisori vaatamisega, 34% kehtestavad piiranguid seoses mobiil- või nutitelefoniga (diagramm 7). Kõige harvem reguleeritakse peredes mängukonsoolide kasutamist. Piirangud seoses meedia tarbimisega puuduvad 14% peredest. Sagedamini piirangud puuduvad peredes, kus on eelkooliealised lapsed.

Piiravaid reegleid eelistavad rakendada pigem kõrgharidusega vanemad, kui seda teevad kutseharidusega vanemad. Näiteks 54% kõrgharidusega lapsevanematest piirab televiisori vaatamist, kutseharidusega vanematest teeb seda 39%. Arvuti ja interneti kasutamisega seavad piiranguid 83% kõrgharidusega lapsevanematest, kutseharidusega vanematest jälle 72%. Arvuti ja interneti tarbimise osas seatakse poistele piiranguid sagedamini (90%) kui tüdrukutele (74%).

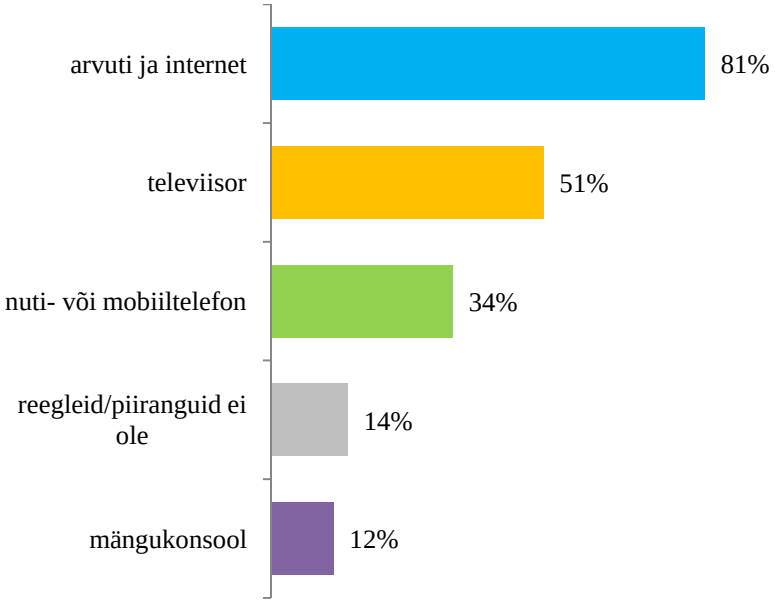


Diagramm 7. Reeglite ja piirangute kehtestamine erinevate meedia seadmete kasutusele

Kui uurisin, milliseid piiranguid kasutatakse, siis avatud küsimusele, mis on peamised reeglid ja piirangud seoses arvuti ja interneti kasutamisega, vastas 73 lapsevanemat. Kodeerisin vastused ja nad on esitatud tabelis 3.

Tabel 3. Piirangud seoses interneti ja arvuti kasutamisega

Piirang	**Nimetatud kordade arv**
Ajalised piirangud	45
Arvuti preemiana hea õppimise eest	18
Ainult teatud veebilehekülgede kasutamine	11
Mängude keelamine	5
Keeld võõrastega suhelda	3
Tasuliste teenuste keelamine	2
Ainult lubatud programmide kasutamine	1
Mitte avaldada isiklikku infot	1

- Kõige sagedamini seavad vanemad lastele ajalisi piiranguid, näiteks „*ajaline piir 2 tundi päevas, mitte rohkem*" või „*õhtuti peale kella 21.00 ei tohi olla arvutis*". Vanemad tunnistavad, et suulised ajalised piirangud töötavad üsna hästi ning 71% lapsevanematest leiab, et nende laps ei veeda internetis liiga palju aega.
- Vanemad seostavad tihti arvuti kasutamist õppeedukusega ning lubavad lapsel meelelahutuslikult arvutit kasutada vaid siis, kui koolitööd on tehtud või kui õppeedukus on hea. See tähendab, et arvutit kasutatakse tihti preemiana hea õppimise eest: „*enne internetti niisama surfama ei saa, kui koolitööd on tehtud*" või „*kui õppeedukus langeb on kohe arvutikasutamise keeld peal*" ning „*kui käitumine või õppimine ei ole korras, siis arvutisse ei lubata"*.
- Järgmine populaarne piirang puudutab veebisisu, ehk lapsele lubatakse vaadata ainult teatud veebilehekülgi – „*uute saitide külastamine vaid koos vanematega*" või „*ei tohi vaadata halbu asju*", „*laps vaatab ainult teatud lehte netis ja seda piiratud aja jooksul*". Veebisisu piiranguid seatakse sagedamini peale väiksematele lastele.
- Arvutimängude mängimise piiramine tõi aga järgmised põhjendused: „*neti mänge ei luba mängida, eriti neid mis on seotud vägivalla ja kuritegevusega ning sõja mängud*" või „*mängude mängimine on lubatud ainult nädalavahetustel*".
- Suhtlemisega seotud reeglid keelavad eelkõige võõrastega vestlemist või kokkupuudet – „*üldiselt kehtib reegel VÕÕRASTEGA EI RÄÄGI*", „*võõrastega ei suhtle ja võõrale lehele minnes tuleb küsib enne, kas võib sinna minna*" või „*lapsele on tehtud selgeks, et mitte kunagi ei anna võõrastele infot oma kodu kohta, telefoninumbrit jms.*

Andmete põhjal saab teha järeldusi, et peamised interneti ja arvutiga seotud riskid, mis lapsevanemad teadvustavad ja reeglites kajastavad on: arvuti liigkasutamine, õppeedukuse langus, ohtlik veebisisu, arvutimängud, võõrastega suhtlemine, materiaalsed riskid, privaatsusriskid. Märkimisväärne on, et suuremad riskid, nagu võõrastega suhtlemine ja personaalse info avaldamine, kajastuvad reeglites tegelikult üsna vähe. Imestama paneb aga see, et suhtlusportaalid ei leidnud piirangutes üldse mainimist, kuigi küsitluse käigus lapsevanemad hindasid sotsiaalvõrgustikke lastele potentsiaalselt väga ohtlikus.

Küsitlusest selgus, et enamus lapsevanemaist (63%) leiab, et piirav strateegia töötab nende peredes efektiivselt ning piirangutest on „palju" või „pigem palju" abi.

Tehnilise järelevalve strateegia oli vastanute seas kõige vähem levinud. Küsimusele „Kas arvutisse, mis teie laps kodus kasutab, on installeeritud vanemliku kontrolli programm või mõni sarnane tarkvara?" vastas jaatavalt 12% respondente (ehk 9 inimest). Toon välja ka selle, et kõik järelevalve tarkvara kasutajad on kõrgharidusega.

Kasutatavat järelevalve programmi suutis nimetada vaid 4 vastajat, – kaks korda oli nimetatud Windows'i operatsioonisüsteemi integreeritud järelevalve vahend, üks kord Net Nanny programm ja Kaspersky viirusetõrje.

Kuus lapsevanemat kasutavad järelevalve tarkvara veebisisu filtreerimiseks, viis vastajat külastatud veebilehtede monitoorimiseks ja programmide blokeerimiseks, neli vanemat piiravad arvuti kasutusaega ning üks lapsevanem blokeerib sotsiaalvõrgustikke. Kuna vastanute hulka sattus vähe inimesi, kes reaalselt kasutavad järelvalve programme, siis ei saa teha põhjalikke ja usaldusväärseid järeldusi tarkavara kasutamispraktikate kohta.

3.3 Lapsevanemate nägemus vanemliku järelevalve tarkvara rolli võrreldes teiste järelevalvestrateegiatega

Internetiohutuse tagamisel peavad lapsevanemad esmatähtsaks laste harimist ja internetikasutamise reeglite kehtestamist (diagramm 8). Järelevalve tarkvara roll on märgatavalt väiksem. Näiteks 81% lastevanematest peab „väga tähtsaks" lapse harimist, 66% peab „väga tähtsaks" reegleid, mis reguleerivad lapse internetikasutamist, ning tehnilisi vahendeid peab „väga tähtsaks" 47% lapsevanemaist. Peaaegu sama tähtsaks internetiohutuse tagamisel peetakse vastavaid seadusi (45%), mis kaitsevad last internetis.

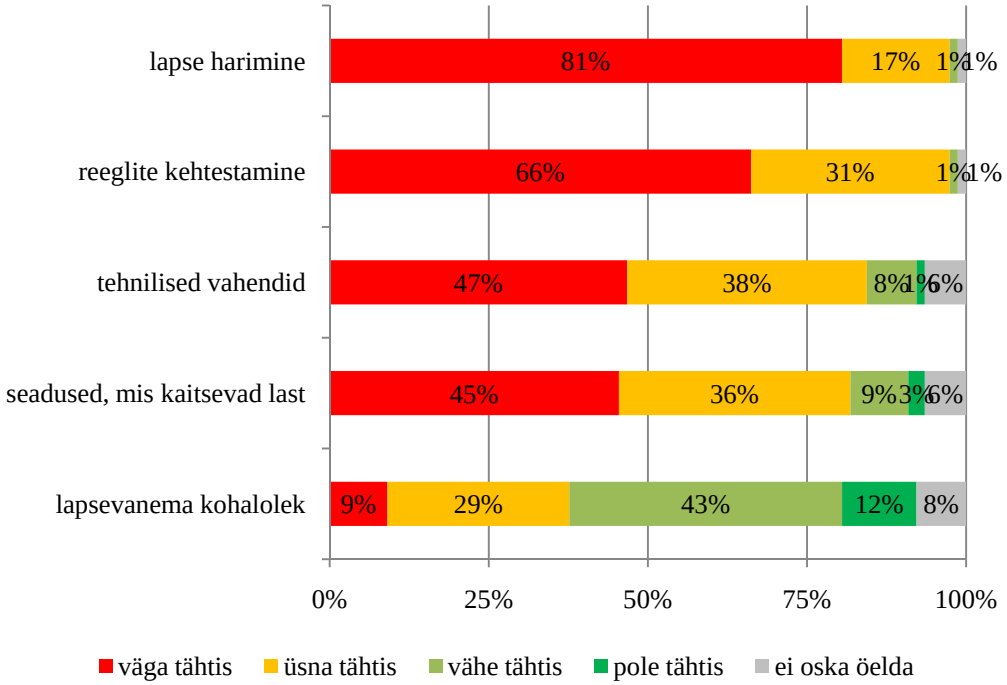


Diagramm 8. Lapsevanemate hinnangud erinevatele internetiohutuse strateegiatele (kõik vastajad).

Diagrammilt 8 on näha, et küsitluses osalenud lapsevanemad annavad eelistuse pedagoogilistele meetoditele – lapse valgustamisele internetiturvalisuse teemadel ja reeglite kehtestamisele. Tehnilistesse vahenditesse suhtuvad vanemad üldiselt positiivselt, enamus (85%) usub, et need vahendid võivad olla abiks laste *online*-riskide eest kaitsmisel. Samas reaalselt neid vahendeid siiski ei kasutata.

Vanemate (10–12-aastate) laste vanemad näevad tehnikas rohkem kasu (42% peab tehnikat „väga tähtsaks"), kui eelkooli (4–6-aastaste) laste vanemad (38%). Aga kõige suuremat potentsiaali tehnilises järelevalves näevad 7–9-aastaste laste vanemad, 65% nendest peab tehnilise järelevalve rolli „väga tähtsaks".

Uurimus on välja toonud, et **järelevalve tarkvara mittekasutamise peamine põhjus on vajaduse puudus** – 43% vanemaist ei näe oma peres selliste programmide vajalikkust (diagramm 9). Suur osa lapsevanematest põhjendavad vajaduse puudust sellega, et laps on liiga väike ja nad jõuavad ise teda kontrollida: „*pean oma lapsi veel piisavalt väikesteks, et suudan nende vähestel tegemistel arvutis ka ilma programmita silma peal hoida*" või „*laps on veel väike. Kuid kindlasti tulevikus pean seda programmi vajalikuks*". Tuuakse ka põhjuseks, et vajadus puudub, kuna laps ei tee keelatuid asju: „*olen kindel ,et mu laps ei ole pornograafiast ja muust sellisest huvitatud. Olen sellest teemast temaga rääkinud.*" või „*laps saab aru, mida tohib ja mida ei tohi teha.*" Lastevanemate seas on ka levinud

seisukoht, et usaldus on parem meetod kui kontrollimine – „*last tuleb usaldada ja seni pole ta seda kuritarvitanud. Olen selgitanud ohtusid*”.

Teine põhjus, miks järelevalve programme ei kasutata, on vähene teadlikkus – 40% vanematest tunnistasid, et ei ole sellistest programmidest kunagi midagi kuulnud.

35% lapsevanemaist tunnistasid, et neil ei jätku tehnilisi oskusi sellise programmi töölepanemiseks: „*pole leidnud aega sobiva programmi otsimiseks ja samas kardan, et ei oska seda ise kasutada*.” Ning üsna väike lapsevanemate protsent (6%) ei usu, et need programmid võivad olla laste kaitsmisel efektiivsed.

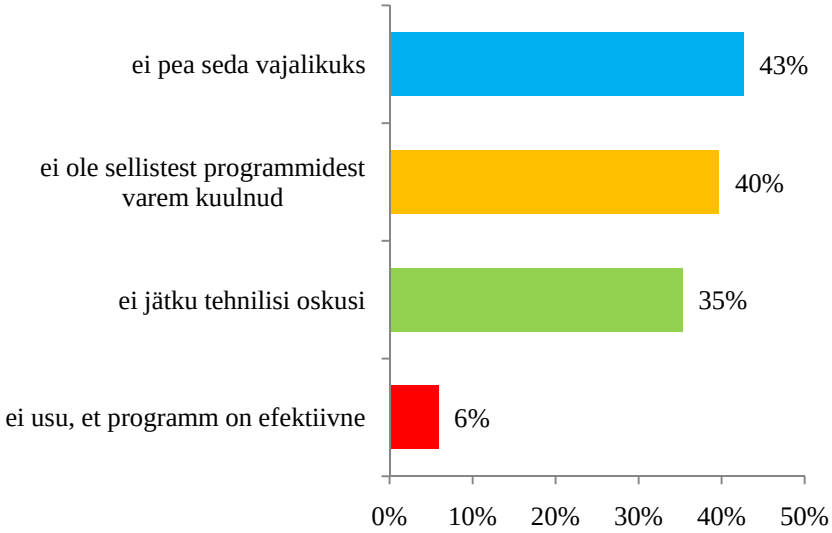


Diagramm 9. Vanemliku järelevalve tarkvara mittekasutamise põhjused (vastajad, kes ei kasuta järelevalve tarkvara).

Väärib mainimist, et enamus lapsevanematest usub, et järelevalve tarkavara kasutamine ei pea negatiivselt mõjutama suhetele lapsega ega tekitada konflikti. Selle, et kontrolliprogramm võiks rikkuda suhteid lapsega, toob välja ainult 17% vastanutest.

Vaadates tulemusi laste vanuse lõikes võib märgata, et järelevalve tarkvara mittekasutamise põhjused erinevates vanusegruppides on erinevad. Näiteks eelkooli lastega vanemate hulgas on peamiseks põhjuseks, miks järelevalve tarkvara ei kasutata, vajaduse puudumine (53%). Tarkvara ebavajalikkust seletavad vanemad sellega, et koolieelikud kasutavad arvutit vähe ja lapsevanemad üritavad asuda laste kõrval. 7–9-aastaste laste lapsevanemad nimetavad järelevalve vahendite mittekasutamise peamiseks põhjuseks tehniliste oskuste puudumist (50%). Ning 10–12-aastaste laste lapsevanemate grupis peamine takistus on madal teadlikkus – 52% vanemaist nentis, et ei ole järelevalve tarkvarast kuulnud. Analüüs näitas,

et teadlikkuse tase sõltub vastajate vanusest. Üle 40-aastaste hulgas oli 54%, kes ei teadnud varem järelevalve tarkvarast. Nooremates vanusegruppides (kuni 30 a ja 31–40 a) oli see näitaja ligi 36%.

Kui võrrelda lapsevanemate vastusi hariduse lõikes, siis ilmneb huvitav eripära, et haritumad inimesed suhtuvad tehnikasse tunduvalt kriitilisemalt – tehnilist järelevalvet ei pea oma perele vajalikuks 48% kõrgharidusega vanematest, samas kui kutseharidusega lapsevanemate hulgas on see protsent vaid 28%. Kutseharidusega vanemate peamine põhjus, miks järelevalve tarkvara ei kasutata, on tehniliste oskuste puudus (67%).

Väärib mainimist, et võrreldes naistega peavad mehed tehnilist järelevalvet oma perele vähem vajalikuks (vastu oli 56% isadest ja 36% emadest). Kuna aga isadest vastajaid oli vähe, siis tegelikkuses ei saa sellest kaugeleulatuvat järeldust siiski teha.

Kui lapsevanem valib vanemliku kontrolli tarkvara, siis **kõige olulisemaks funktsionaalsuseks** peetakse ebasobiva sisu filtreerimist ja ajalimiidi seadmise võimalust (diagramm 10). Tähtsaks loetakse ka *online*-ostude blokeerimist, valitud programmide keelamist, külastatud veebilehtede statistika jälgimist. Vähemoluliseks peetakse mängude blokeerimist, voogvideo filtreerimist, avatud failide loendi jälgimist, suhtlusvõrgustike piiramist.

Funktsioonid, mida peetakse oluliseks, toetavad interneti ohtude ja riskides välja tulnud probleemide olemasolu. Selles valguses diagramm 10 viitab sellele, et lapsevanemad muretsevad kõige rohkem ebasobiva veebisisu ja arvuti liigkasutamise pärast. Probleemid, nagu suhtlusvõrgustike kasutamine või autoriõigusi rikkuvad failide jagamise programmid (nt BitTorrent), ei paista küsitlus osalejatele probleemina.

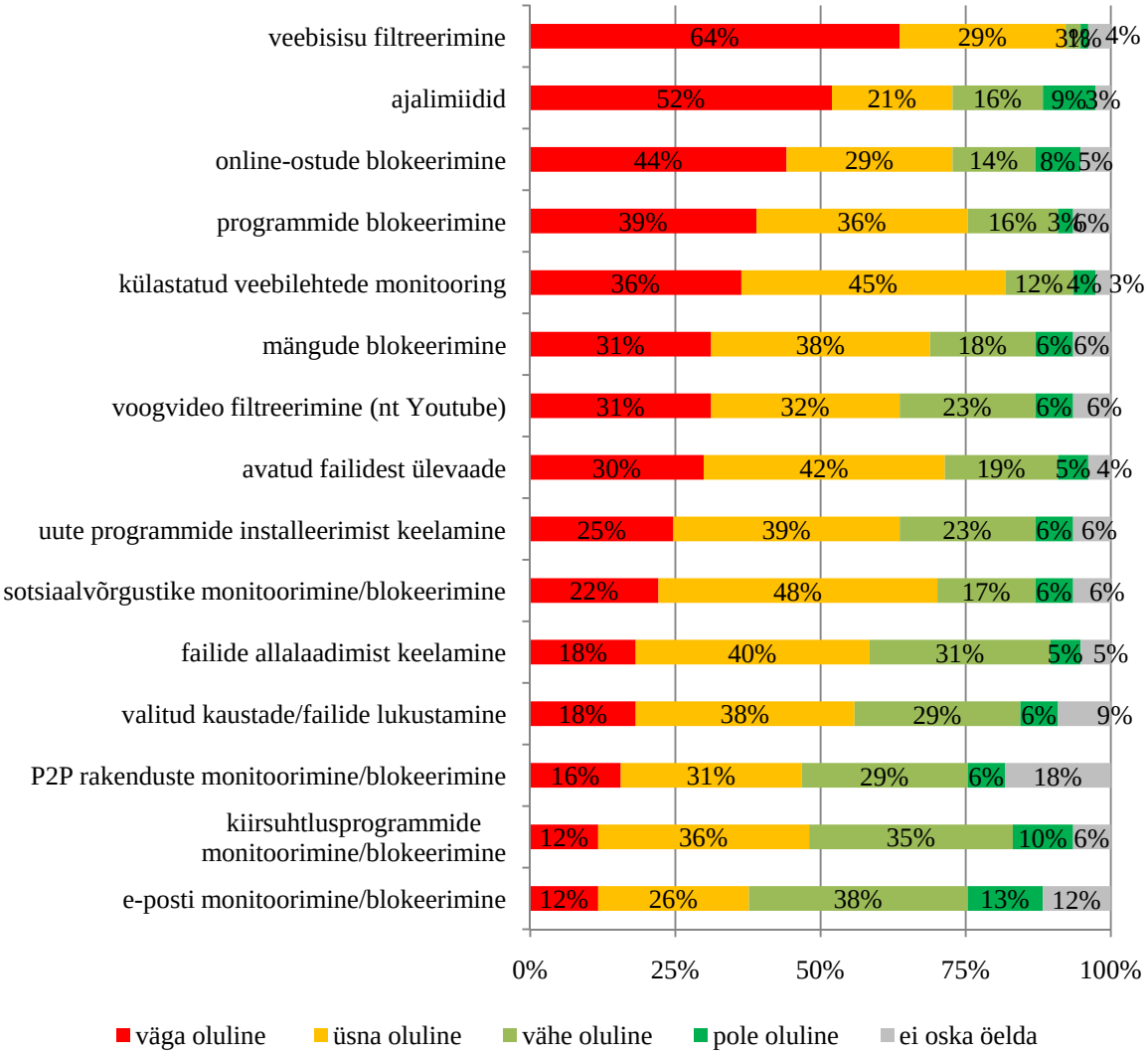


Diagramm 10. Milliseid järelevalve tarkvara funktsioone peate oma perele oluliseks?

Kui vaadata tulemusi laste vanuse lõikes, siis selgub, et vanemas grupis (10–12-aastaste laste lapsevanemad) peetakse järelevalve funktsioone oma perele vähem oluliseks kui nooremates gruppides (4–6- ja 7–9-aastased). Seega 10–12 aastaseid lapsi peetakse tihti piisavalt arukaks ja iseseisvaks ning vanemad on juba vähem huvitatud järelevalve tarkvara kasutamisest.

Nii emad kui ka isad pidasid tähtsaimaks järelevalve tarkvara funktsiooniks ebasobiva veebisisu filtreerimist. Isade arvates on aga olulised külastatud veebilehtedele nii ajalimiitide seadmine kui ka nendest ülevaate omamine. Emad hindavad aga enim võimalusi blokeerida valitud programme ja keelata *online*-ostude sooritust.

Järelevalve programmis oli **kasutatavuse osas** kõige tähtsam lapsevanematele see, et programm oleks piisavalt turvaline ja laps ei saaks sealsetest piirangutest mööda pääseda –

95% vastanutest peab seda „väga” või „üsna oluliseks”. Lapsevanemad sooviksid, et programmi töökeskkond oleks võimalikult lihtne ja arusaadav (94%), ning annaks välja ka põhjaliku raporti lapse tegevuste kohta (91%). Kindlasti on oluline programmi hind: 88% sooviks programmi kasutada pigem tasuta või maksta selle eest vähe. Mitte vähemoluline see, et installeerimine ja seadistamine oleks kasutajale jõukohane (87%). Kasutatavuse osas tuleb ka mainida, et 30% vanemaist arvab, et järelevalve programm peab olema lapsele nähtamatu, 70% arvates ei ole see aga oluline. Vanemate poolt tuli ka ettepanek, et programm peaks olema osaliselt nähtav ehk kasutaja võiks ise valida, millised funktsioonid töötavad piiratule nähtavas või nähtamatus režiimis. Autori andmetel selline funktsionaalsus järelevalve programmides hetkel puudub ning seesugune ettepanek võiks huvi pakkuda vastava tarkvara arendajatele.

Lapsevanemate arust on keskmine vanus, kui laps on piisavalt küps, et tegutseda internetis iseseisvalt ilma vanemate järelevalveta, 14,5 eluaastat. Sellest saab järeldada, et põhikooli lõpuks on laps jõudnud vanema meelest ikka, kus järelevalve kasutamine ei ole enam mõistlik ning laps peaks suutma iseseisvalt otsuseid teha, probleeme lahendada ja ise abi küsida, kui ta seda peaks vajama. Uuring näitas, et kutseharidusega vanemad pooldavad lapse kontrollimist kuni 15,3 eluaastani ja kõrgharidusega vanemad kuni 14,2 eluaastani. Samuti selgus, et lapsevanemate meelest poisid küpsevad internetis varem kui tüdrukud, seega planeeritakse järelvalvet poiste suhtes kasutada keskmiselt kuni 13,4 eluaastani, ja tüdrukute järele kuni 15,1 eluaastani.

4. Järeldused ja arutelu

Üldine kokkuvõte saadud andmetest annab huvitava, kuid keerulise vaatenurga, kuidas lapsevanem oma last internetis kasvatab, ohtudest eemale püüab hoida ja kontrollib. Vanemlik järelevalve internetis peaks toimima sellest hetkest, kui laps asub esimesi samme arvutis või internetis tegema, ja kestab enamasti keskmiselt 14,5 eluaastani, kui noor inimene peaks olema valmis ise oma käitumise kohta internetis otsuseid tegema.

Internetti peavad ohtlikuks 96% lapsevanematest ning enamik neist peab ennast ka vastutavaks selle eest, kuidas tema laps selles keskkonnas hakkama saab. Ligi neljandik vastanud vanematest toob välja, et nende peres on toimunud viimase kuue kuu jooksul mõni intsident, mis on neile interneti ohtlikkust kinnitanud. Suurimad väljatoodud riskid on seotud suhtlemisega suhtlusvõrgustikes ja jututubades. Samamoodi mainitakse ära nii ohtlike failide allalaadimist, nende avamist, veebikaamera kasutamist kui ka niisama veebis surfamist. Internetti peetakse tüdrukutele ohtlikumaks kui poistele. Ohtlikuks veebisisuks peetakse seksuaalse alatooniga materjale, enesevigastamisele ja suitsiidile õhutavaid materjale, vägivalda ja ka narkootikumide kasutusele suunavaid veebe.

Kuigi enamik vanemaid peab ennast peavastutajaks oma lapse hea käekäigu eest internetis, on suur osa vanemaid nõus vastutust jagama internetiteenuse pakkuja, veebiportaalide haldajate ja tarkvara loojatega. See näitab, et vanemad vajavad abi, mis lahendaks juba eos ära interneti ohutusega olevad probleemid, näiteks teenusepakkuja ja veebilehe looja peaks blokeerima ligipääsu lastele ebasobivale sisule.

Lapsi puudutavad järelevalvestrateegiad jagunevad neljaks: aktiivne ehk meetod otse lapsega suhtlemisel ja nii tema otsuste mõjutamisel; monitoorimise meetod – lapsevanem kontrollib hiljem lapse internetikasutust, et teada saada, mida tema laps internetis teeb; kolmas metoodika on piirav järelevalvestrateegia, milles keelatakse käsu või perereegliga oma lapse arvuti- ja internetikasutust; neljas strateegia puudutab tehnilise programmi kasutamist piirangute seadmiseks.

- Aktiivse järelevalve metoodikast kasutavad lapsevanemad kõige enam vestlust lapsega, julgustavad last rääkima oma probleemidest või viibivad ise lapse vahetus läheduses, et teda kontrollida või vajadusel aidata. Mõned vanemad teevad lastega ka teavitustööd, kuidas internetis käituda, kuid seda pigem vanemate lastega kui noortematega. Tüdrukutega vesteldakse interneti teemadel enam kui poistega,

samamoodi kui lapsevanem on ise kõrgharidusega, siis kasutab ta seda metoodikat veidi vähem kui need, kellel oli kutseharidus. Vestlusi interneti teemal viivad enamasti läbi emad.

- Monitoorimise metoodikat kasutab ligi 75% lapsevanematest. Enamasti on see veebilehitseja ajaloo kontrollimine, uuritakse lapse sotsiaalvõrgustiku profiile ja kontaktide loendit otsesuhtlusprogrammides. E-kirjavahetust uuritakse harva. Eelnimetatud metoodikad on küsitavad juba seepärast, et nendega võidakse rikkuda oma lapse põhiõiguseid ja isikuvabadust. Tulemused näitavad, et keskharidusega vanemad kontrollivad oma lapsi rohkem. Emad uurivad veebiajalugu ja isad hoiavad pigem silma peal sotsiaalvõrgustikes.
- Piirava järelevalve strateegia juures piiratakse kõige enam just meelelahutuse kasutust internetis. Piiravaid reegleid kasutavad enam kõrgharidusega vanemad ning poistele on kehtestatud rohkem piiranguid kui tüdrukutele. Kõige sagedamini kasutatud piirang on aja- ja sisupiirang meelelahutuse tarbimisele. Kuna vanemad seostavad meediakasutuse võimaldamist hea õppeedukusega, siis enamasti on internet ja arvuti kasutamine lubatud siis kui „*asjad on koolis korras*“ või „*on õpitud*“.
- Tehnilist järelevalvet tunnevad küsimustikule vastanud lapsevanemad kõige vähem, mainiti ainult operatsioonisüsteemi limiteeritud kasutamist ja kaht järelevalve programmi. 40% küsitluses osalenutest tunnistasid, et ei ole varem kuulnud järelevalve tarkvara vahenditest.

Kuigi enamus lapsevanematest ei kasutanud vastamise ajal erinevat tarkvara oma lapse ohjamiseks internetis, siis see ei takistanud neil vastava tarkvara kohta arvamuse avaldamist. Vastustest tuli välja, et kõige olulisemaks peetakse oma lapse harimist ja reegleid, siiski üsna suur hulk vanemaid oli huvitatud ka vastavast tehnilisest võimalusest enda harimisel. Suurimat kasu näevad järelevalve tarkvarast pigem kooliõpilaste vanemad ning pigem emad kui isad.

Põhjustena, miks järelevalve tarkvara ei kasutata, pakuti järgmist: *ei näe vajadust, kuna laps on liiga väike ja jõuan ise kontrollida; ei tea sellest programmist midagi; puuduvad vajalikud tehnilised oskused programmi kasutamiseks*; üsna väike protsent usub, et programmid on ebaefektiivsed. Järelevalve tarkvara kasutamise suhtes kriitilisemad on pigem kõrgharitud vanemad. Tarkvara olulisemad funktsioonid on järgmised: ebasobiva

sisu filtreerimine, ajalimiidi panemise võimalus, *online*-ostude blokeerimine, programmide käivituse keelamine, külastatud lehtede statistika. Samas ei ole vanemad maininud vajadust saada abi suhtlusvõrgustiku kasutamise keelamiseks ning ka autoriõiguste temaatika vanemaid eriti ei huvita.

Tarkvara kasutuse üle igas konkreetses olukorras tuleb otsustada eraldi, võttes arvesse lapse vanust ja arvuti kasutamisharjumusi, lapsevanemate kasvatusväärtusi ning eesmärki, milleks tarkavara kasutada kavatsetakse. Enne tarkvara rakendamist oleks soovitatav uurima tehnilise strateegia eeliseid ja puuduseid. Näiteks oluline on mõista, et järelevalve tarkvara kaitseb last *online*-ohtude eest, kuid ei suurenda laste meediakirjaoskust ja oskust probleemidega iseseisvalt toime tulla. Teatud määral rikub programm laste privaatsust ning piirab võimalusi internetti täisväärtuslikult kasutada. Samuti ei arenda programm lapsevanema oskust lapsega suhelda internetiturvalisuse teemadel, suunata ja õpetada last võrgumaailmas turvaliselt käituma. Programmi kasutamine võib tekitada tunde, et laps on piisavalt kaitstud ning lapsevanem ei pea midagi juurde õpetama. Tegelikult ei suuda ükski arvutiprogramm asendada lapsevanema otsest tähelepanu ja juhendamist. Selles valguses tuleb parimaks strateegiaks pidada ikkagi piisavat ennetustööd – lapse harimist ja õpetamist internetiohutuse valdkonnas, ning järelevalve tarkvara võib olla rakendatud vaid lisameetmena.

Oluline on silmas pidada, et järelevalve programmide efektiivsus varieerub sõltuvalt funktsionaalsusest, näiteks veebisisu filtreerimine on veel ideaalist kaugel. Internetis leiduva ebatsensuursete materjalide hulk on nii mahukas ja mitmekesine ning ühtlasi ka mitmekeelne, et filtreerimise kõrgele efektiivsusele loota ei maksa. Samal ajal näitasid vanemate vastused, et ohtlik veebisisu on peamine lapsevanemate mure ning selle filtreerimine on kõige vajalikum funktsionaalsus. Need vanemad, kelle jaoks see funktsioon on kriitiline, võivad järelevalve tarkavaras kergesti pettuda. Teiselt poolt, terve rida ülesandeid täidab järelevalve tarkvara väga hästi – näiteks ajalimiidid, erinevate rakenduste blokeerimine, sotsiaalvõrgustike monitoorimine, *online*-ostude keelamine, lapse internetiaktiivsuse jälgimine on üsna hästi väljaarendatud. Need vanemad, kes on nimetatud funktsioonidest huvitatud, võivad järelevalve programmi kasutuselevõtmisel olla sellega rahul.

Tuleb arvestada, et programmi valimine, installeerimine ja töölesaamine võib olla keeruline ja aeganõudev protsess – 35% lapsevanemaist nentisid, et nende kasinad arvutioskused on

üks vanemliku kontrolli mittekasutamise põhjustest. Need vanemad, kel ei ole häid arvutioskusi, peavad programmi valikul silmas pidama seda, et valitav rakendus oleks võimalikult lihtne nii installeerimisel kui ka kasutamisel, vajadusel peaks neid toetama vajaliku infoga ka programmi edasimüüja, kui see on näiteks tasuline toode.

Uuring näitas, et lisaks tehnilistele raskustele tekivad lapsevanematel ka psühholoogilised barjäärid – näiteks hirm sattuda lapsega konflikti või kaotada usaldus. 17% uuringus osalenud lastevanematest nõustus, et tarkvara kasutamine võib rikkuda suhteid lapsega. Järelevalve programmi rakendamisel peaks lapsevanem kindlasti oma lapsele seletama, miks sellised piirangud on valitud ja arutama lapsega, millistel veebilehtedel ta käia sooviks ja miks ning siis koos otsustama, mida piirata ja mida mitte. Piirangute panemine ei tohi olla lapsevanema võimu demonstreerimine, vaid peaks toimuma dialoogis lapsega, kellele piirang kohaldatakse. Tähtis on see, et laps mõistaks piirangute eesmärke ja oleks nendega nõus, see aitab vältida konflikti ja arusaamatusi.

Järelevalve vahenditele on omased ka töökindluse- ja turvalisuseprobleemid – programmi piirangutest möödahiilimine on tihti üsna lihtne, kui näiteks internetist abi otsida. Internetist saab leida õpetusi, kuidas mööda minna tarkvara paroolidest või neid lahti murda. Lapsevanem peab arvestama, et järelevalve tarkvara on efektiivsem nooremate laste puhul, kes pole veel nii osavad, et suudavad piiranguid tühistada. Seega valides programmi vanematele lastele, peab lapsevanem arvestama programmi töökindlust ja vastupidavust. Kindlasti ei piira kodus arvutile peale pandud piirang võimalust kasutada piiranguteta arvutit kas koolis, sõprade juures või avalikus kohas, näiteks raamatukogus, mis viib lapse palju ohtlikumasse situatsiooni, sest seal võib puududa täiskasvanu järelevalve või on see nõrk.

Eelkooliealiste laste puhul, kelle interneti kasutamine piirdub vaid mõne veebilehega, on hea idee kasutada valget nimekirja (*white list*), mis kindlalt kaitseb last ebasobiva sisu eest, blokeerides kõik veebilehed, välja arvates lapsevanema lubatud.

Vanemad võivad kaaluda järelevalve programmi kasutamist ka siis, kui otsene kontroll on raskendatud või võimatu – arvuti asub näiteks lapse magamistoas või vanemad veedavad palju aega kodust väljaspool näiteks kaua tööl või tööl võõrriigis. Järelevalve tarkvara võib olla lapsevanemale ka abiks, kui suulised kokkulepped ei tööta efektiivselt, näiteks laps

ignoreerib reegleid. 37% küsitluses osalenud lapsevanematest nentisid, et suulised reeglid ei anna alati oodatud tulemusi ning nad vajaks lisaabi kokkulepitud reeglite kehtestamisel.

Kuigi järelevalve programmi kasutamine võib paljudel juhtumitel olla tulemuslik ning Euroopa Liidu tasemel võetakse ette samme selle tarkvara liikmesriikides levitamiseks, ei tasu siiski tehnilist kontrolli rakendada, kui selline meetod on lapsevanema kasvatusväärtustega vastuolus. Uuringutulemused näitasid, et enamus lastevanematest ei taha delegeerida lapse kasvatamist tehnikale. Küsitluses osalenud lapsevanemad eelistavad oma laste harimist tehnilisele järelvalvele. Vanemliku kontrolli vahendid ei ole lapsevanemate seas populaarsed, neid kasutab 12% vastanuist. Kuigi peamiseks põhjuseks tarkvara mittekasutamiseks oli nimetatud vajaduse puudumine, näitasid küsitluse tulemused, et järelevalve vahendite mittekasutamise taga on pigem vanemate madal teadlikkus – 40% vastanuist nentis, et ei ole sellistest programmidest varem kuulnud, seega tarkvaratootjatel ja müügimeestel Eestis veel suur töö tegemata.

Et lapsevanemad võiksid teadlikult otsustada järelevalve vahendite üle, tuleb pakkuda neile rohkem informatsiooni vastavate programmide kohta, nende funktsionaalsustest, tööpõhimõtetest, valiku kriteeriumidest. Hetkel on vähestel või puuduvad täiesti eestikeelsed õppematerjalid ja manuaalid, millist tarkvara valida, kuidas järelevalve programme seadistada ja kasutada. Eestikeelse kasutajaliidesega järelevalve programmide valik on piiratud. Autori andmetel on eesti keeles kättesaadavad vaid Kaspersky Internet Security, WhiteNet, Windows operatsioonisüsteemi integreeritud vanemlik kontroll ja F-Secure Internet Security 2014 rakendus. Unustada ei tohi ka lapsevanemate üldise teadlikkuse tõstmist internetiohutuse valdkonnas – 48% vanemaist tunnistasid, et nende teadmised internetiturvalisuse osas on kasinad, seega võib sisuliselt väita, et pooled vanematest ei ole oma lapsele parimad partnerid interneti ohutuse vallas ja vajavad ise abi.

Abi lapsevanematele järelevalve tarkavara valimisel, installeerimisel ja seadistamisel võiksid osutada internetiteenuse pakkujad – pakkudes oma klientidele vanemliku järelevalve tarkvara rakendamist näiteks võrgu tasemel. Huvitatud lapsevanemad võiksid seda teenust oma perele tellida, mis oleks kiire ja mugav võimalus alustada järelevalve programmi kasutamist. Järelevalve tarkavara võiksid kasutada ka Eesti koolid, integreerides vanemliku kontrolli funktsioone oma lokaalsesse võrku. Õpetusi järelevalve vahendite kasutamise kohta saaksid koostada koolitusega tegelevad asutused ja firmad ning välja pakkuda lapsevanematele vastavaid arvutikoolitusi. Ning lõpetuseks peaks erinevad e-ohutuse

teavitust läbiviivad programmid nagu „Targalt Internetis”, „Päriselt ka või?” jt oma programmi võtma samamoodi vastava tarkvara võimaluste tutvustamine, et vanemad saaksid teha oma laste suhtes oskuslikumaid ja teadlikumaid valikuid.

Kokkuvõte

Käesoleva magistritöö eesmärgiks oli välja selgitada millisena tajuvad lapsevanemad vanemliku järelevalve tarkvara rolli laste interneti turvalisuse tagamisel.

Töö tutvustab mitmetele huvigruppidele tarkvaralisi võimalusi laste kaitsmiseks internetis ja tõstab esile probleeme, mis on seotud järelevalve tarkvara kasutamisega. Uuring kutsub üles erinevaid osapooli koos mõtlema selle üle, kuidas neid vahendeid vastutustundlikult rakendada, et tagada lastele maksimaalne kaitse, samal ajal aga võimaldada neil täisväärtuslikult internetti kasutada.

Selleks, et sügavamalt mõista järelevalve tarkvara rolli, on töö teoreetilises osas seda nähtust vaadeldud kolmel dimensioonil ehk triangulatsiooni põhimõttel. Esiteks on töös toodud välja ja uuritud aktuaalseid ohte ning riske internetikeskkonnas viibivatele lastele, mis annab ülevaade sellest, milliste probleemidega järelevalve tarkvara peab olema suuteline toime tulema. Teiseks on kirjeldatud võimalikke kaitsestrateegiaid ja toodud välja nende eelised ning puudused. Kolmandaks on antud põhjalik ülevaade tehnilisest strateegiast – millised järelevalve vahendid eksisteerivad, kui lai on nende funktsionaalsus, kui efektiivselt nad toimivad.

Magistritöö raames on läbi viidud veebipõhine ankeetküsitlus, et välja selgitada:

1. Milliseid riske lapsevanemad tajuvad ja peavad probleemseks seoses laste internetis viibimisega?
2. Milliseid järelevalvestrateegiaid kasutavad lapsevanemad, et kaitsta oma last *online*-riskide eest?
3. Millisena näevad lapsevanemad vanemliku järelevalve tarkvara rolli võrreldes teiste järelevalvestrateegiatega?

Uurimistöö näitas, et kõige ohtlikumaks veebisisuks peetakse pornograafiat, vägivalda, enesevigastamise ja suitsiidi propageerivaid materjale. Lapsevanemad näevad ohtu oma lastele võõraste inimestega suhtlemises, eriti kui see toimub jututubades või suhtlusvõrgustikes veebikaamera vahendusel. Suur osa lapsevanematest on mures laste üleliigse internetikasutamise pärast; koolilaste puhul lisandub sellele murele ka hirm, et lapse õppeedukus võib kannatada.

Uuringu tulemustel võin väita, et küsitluses osalenud vanemad tunnevad oma laste tegevuste vastu internetis huvi, ning riskide maandamiseks kombineerivad erinevaid järelevalvestrateegiaid. Kõige populaarsem on aktiivne järelevalve, lapsevanemad küsivad last nende internetikasutamise kogemustest, selgitavad lastele veebisisu ja julgustavad rääkima häirivatest asjadest. Samal ajal on enamus peredest kehtestanud arvuti- ja internetikasutamise piiravad reeglid. Monitoorimise strateegia on mõnevõrra vähem populaarne, seda kasutab umbes kolm neljandikku lapsevanemaist.

Kõige vähem levinud on tehniline strateegia, järelevalve programme kasutab 12% küsitluses osalenud lapsevanematest. Kuigi tarkvara tegelik kasutamine on madal, suhtuvad tehnilisse järelevalvesse lapsevanemad positiivselt. Enamus usub, et need vahendid võivad olla abiks laste kaitsmisel *online*-riskide eest ning ei kahtle programmide efektiivsuses, kuid lapsevanemad ei kiirusta oma peres tehnilise järelevalve praktilise kasutamisega. Peamised põhjused järelevalve tarkvara mittekasutamiseks on vajaduse puudumine ja madal teadlikkus järelevalve vahenditest – vastused näitasid, et 40% lapsevanematest ei ole järelevalve programmidest varem kuulnud. Kõige rohkem kasu oma perele järelevalve tarkavaras näevad 7–9-aastaste laste vanemad. Koolieelikute vanemad väidavad, et jõuavad laste järele valvata ise, ilma tarkvarata, aga suuremaid lapsi (10–12 a) peavad lapsevanemad tihti piisavalt arukaks ja iseseisvaks, et tarkvara mitte kasutada.

Edasised uuringud võiksid detailsemalt keskenduda sellele, kuidas Eestis vanemliku järelevalve programme tegelikult kasutatakse, millised funktsioonid leiavad kõige rohkem rakendamist, milliseid ohtlikke veebisisu kategooriaid lapsevanemad blokeerimiseks valivad, milliseid märksõnu ja veebiaadresse lisavad musta nimekirja. Põhjalikumalt tuleb vaadelda mobiilse järelevalve tarkvara spetsiifikat. Tähelepanu võiks pöörata ka sellele, kuivõrd järelevalve tarkvara kasutamine rikub laste õigusi privaatsusele, eraelule, informatsioonile, sõnumisaladusele. Oluline on teada saada, kuidas tajuvad lapsed järelevalve tarkvara rolli internetiohutuse tagamisel ja milline on nende suhtumine tehnilisse järelevalvesse.

Summary

Title: The Role of Parental Control Software in Ensuring Children's Internet Safety – A Parents' View.

Keywords: parental mediation, parental control software, internet safety.

The aim of this master thesis is to find out, how the parents sense the role of the parental control software in order to maintain their children's internet safety. The role of parental control tools in ensuring children's internet safety is currently an actual debate theme both in Europe and in the world. The information technology provides us with more and more opportunities for work, entertainment, learning and now the children's upbringing. In order to ensure the safe internet usage, parents can choose a variety of mediation strategies, first of all this is an education and explanations, rules of online-safety and restrictions. But more attention is attracted such technical solutions that are able to identify potentially dangerous web-content and block this, – parental control software.

The early researches indicated that Estonian children are more unprotected, compared to kids from other European countries, in the matter of sexual materials, cyberbullying, interacts with online-strangers and meeting with them in the real life. Estonian children are at the forefront of excessive internet use in Europe as well. Estonian kids use computers in a relatively independent with little guidance or totally unsupervised, and the parents' awareness of the online-risks are low. In this light the parental control tools might be an appropriate solution for Estonian parents in order to maintain their children's internet safety.

The theoretical part of master thesis gives an overview about the actual risks that might threat children in the internet, describes the possible parental mediation strategies and brings out their advantages and disadvantages. The theoretical part also gives a thorough overview about the technical mediation – what kind of a parental control software does exist, how functional these are and how effectively they work.
In the context of the master thesis i have conducted a web-based questionnaire to find out the following:

- What kind of risks the parents sense and estimate as problematic about their children's internet usage?
- What kind of parental mediation strategies the parents use in order to keep their children away from the online-risks?

- What the parents think about the role of the parental control software compared to the other mediation strategies?

This master thesis is a quantitative descriptive research, where for data collecting was used the internet survey. The study sample consisted of 77 parents. The poll was conducted using the snowball sampling method during two months between December 2012 - January 2013. Survey questions were divided into five sections: issues children's computer and internet usage, parents worries and fears about online-threats, parents mediation strategies, parents opinions and expectations of the parental control software and the demographic questions.

The research showed that the most dangerous web-contents are considered to be the materials that promote pornography, violence, self-harm and suicide. Parents see threat to their children in communicating with strangers, especially when it happens in the chat rooms or in the social networks via webcams. Most of the parents are concerned about the excessive use of the internet and computers. When it comes to schoolchildren, there is also a fear that a pupil's progress in the studies might suffer. The parents also fear material damage due to their children's internet use.

In order to reduce online-risks, parents combine different mediation strategies. The most popular is active mediation – parents ask from their children, what kind of a experiences they have had in the internet, explain the web-content and encourage them to talk about the disturbing issues. At the same time most of the families have set the restrictive rules of the computer and internet usage. Monitoring strategy is a bit less popular than active and restrictive strategies – it is used by three-fourths of the parents and its key method is to control the browser's history.

The least spread is a technical strategy, parental control programs are used by 12% of the parents. The biggest advantage of the control software is seen by these parents, whose children are 7–9 years old. The parents of a preschool children claim that they can supervise their children by themselves, without using any software, and the parents of more grown-up children (aged 10–12) consider them often sufficiently wise and independent, and see no need to use the software. Although the real usage of this software is low, practically all the parents admit that control software programs have functions that are potentially very useful to their families. Most people believe that the parental controls can help to keep the children away from the online-risks and they do not doubt the efficiency of these programs. But on

the other hand they are not in a hurry to start really using these technical tools. The main reasons not to use parental controls is the lack of necessity and knowledge about these control measures – the answers showed that 40% of the parents have never heard about such programs.

The survey found that the Estonian parents feel an interest in their children's online-activities and try to reduce online-risks for their kids. But the parents prefer to use pedagogical methods of mediation – an instructions, explanations, dialogs. Concerning the parental control software parents need more information about this tools – about their functionality, work principles and criteria, what to choose.

Kasutatud allikad

American Academy of Pediatrics (1999). *Understanding the Impact of Media on Children and Teens*. Loetud aadressil: http://www.thepediatriccenter.net/docs/brudenell/UnderstandingtheImpact.pdf (05.10.2013)

Apple Inc (2013). iOS: Understanding Restrictions (parental controls). Loetud aadressil: http://support.apple.com/kb/ht4213 (12.10.2013)

Bazaarvoice (2012). *Talking to Strangers: Millennials Trust People over Brands.* Loetud aadressil: http://resources.bazaarvoice.com/rs/bazaarvoice/images/201202_Millennials_whitepaper.pdf (2.11.2013)

Baumrind, D. (1991). The Influence of Parenting Style on Adolescent Competence and Substance Use. *Journal of Early Adolescence*, 11 (1), 56-95. Loetud aadressil: http://mltei.org/cqn/Adolescent%20Development/Resources/Family/Baumrind,%20The%20influence%20of%20parenting%20style%20on%20adolescent%20competence%20and%20substance%20use.pdf (2.12.2013)

BitDefender (2012). *Parental Control User's Guide.* Loetud aadressil: http://download.bitdefender.com/resources/media/materials/parental-control/en/Parental_Control_User_Guide.pdf (8.11.2013)

Bond, E. (2012). *Virtually Anorexic – Where's the harm? A research study on the risks of pro-anorexia websites.* Loetud aadressil: http://www.nominettrust.org.uk/sites/default/files/Virtually%20Anorexic%20-%20Where%27s%20the%20harm.pdf (2.10.2013)

Boyd, D., Ryan, J., Leavitt, A. (2011). *Pro-Self-Harm and the Visibility of Youth - Generated Problematic Content.* Loetud aadressil: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/boyd.pdf (21.09.2013)

Burt, D. (2002). *The Facts on Filters.* Loetud aadressil: http://www.ntia.doc.gov/legacy/ntiahome/ntiageneral/cipacomments/pre/aclj/ExhibitA.pdf (1.08.2013)

Caldwell-Stone, D. (2013). Filtering and the First Amendment. Loetud aadressil: http://www.americanlibrariesmagazine.org/article/filtering-and-first-amendment (4.10.2013)

CEOP (2013). *Annual Review 2012-2013.* Loetud aadressil: http://ceop.police.uk/Documents/ceopdocs/AnnualReviewCentrePlan2013.pdf (8.11.2013)

Chiapetta, M (2013). Make your PC kid-friendly with four custom operating systems. PCworld, Mar 14, 2013. Loetud aadressil: http://www.pcworld.com/article/2030685/make-your-pc-kid-friendly-with-four-custom-operating-systems.html (24.10.2013)

Clark, L.S. (2011). Parental Mediation Theory for the Digital Age. *Communication Theory* 21, 323 – 343. Loetud aadressil: https://portfolio.du.edu/downloadItem/217203 (3.10.2013)

Common Sense Media (2010). *Do Smart Phones = Smart Kids?* Loetud aadressil: http://www.itu.int/council/groups/wg-cop/second-meeting-june-2010/CommonSenseSmartPhonesSmartKidsWhitePaper.pdf (4.11.2013)

CYBERsitter (2013). How does CYBERsitter compare to other filtering software? Loetud aadressil: http://www.cybersitter.com/whycyb.htm (16.10.2013)

Daily Mail (2012). Amanda Todd: Canadian teen kills herself after desperate video. Loetud aadressil: http://www.dailymail.co.uk/news/article-2216543/Amanda-Todd-Canadian-teen-kills-desperate-video-plea-begging-bullies-stop.html (9.10.2013)

Daphne (2008). *Vägivald ja tehnoloogia.* Loetud aadressil: http://ec.europa.eu/justice_home/daphnetoolkit/files/others/booklets/07_daphne_booklet_7_et.pdf (2.03.2013)

Delfi (2012). Internetis levib koolitüdruku peksmise räige video: "Põlvili! Võta oma püksirihm ära!" Loetud aadressil: http://www.delfi.ee/news/paevauudised/eesti/internetis-levib-koolitudruku-peksmise-raige-video-polvili-vota-oma-puksirihm-ara.d?id=65130944 (21.11.2013)

Duerager, A. & Livingstone, S. (2012). *How can parents support children's internet safety?* EU Kids Online, London, UK. Loetud aadressil: http://eprints.lse.ac.uk/42872/1/How%20can%20parents%20support%20children%E2%80%99s%20internet%20safety%28lsero%29.pdf (1.02.2013)

EMT (2009). EMT ja rate.ee algatavad noorte turvalise internetikäitumise projekti (pressiteade) Loetud aadressil: https://www.emt.ee/uudised/-/uudisvoog/uudis/16820 (7.08.2013)

Euroopa Komisjon (2012). Komisjoni teatis euroopa parlamendile, nõukogule, euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele. *Lastele parema interneti*

loomise Euroopa strateegia. Loetud aadressil: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:ET:PDF (21.05.2013)

Euroopa Komisjon (2013). Turvalise interneti päev 2013 – „Respekt!" (pressiteade) Loetud aadressil: http://europa.eu/rapid/press-release_IP-13-86_et.htm (21.09.2013)

FamilyPC, (1997). FamilyPC`s Second Annual Survey Of Parents On The Internet. Loetud aadressil: http://list.uvm.edu/cgi-bin/wa?A3=ind9712A&L=COMMUNET&E=0&P=70476&B=--&T=text%2Fplain (10.10.2013)

Faulkner, M. (2012). Libraries and Internet Filtering Software. Loetud aadressil: http://webjunction.org/documents/webjunction/Filter_Schmilter_Libraries_and_Internet_Filtering_Software.html (1.12.2013)

Flash Eurobarometer (2008). *Towards a saferuse of the Internet forchildreninthe EU– a parents' perspective.* The Gallup Organisation upon the request of European Commission. Loetud aadressil: http://www.saferinternet.eu/c/document_library/get_file?uuid=52338038-5fef-4ba4-a8cf-4f421d618d5d&groupId=12160 (1.02.2013)

Foltz, R. (2011). Parental Monitoring or an Invasion of Privacy? *Reclaiming children and youth.* 20 (3), 41-42. Loetud aadressil: http://reclaimingjournal.com/sites/default/files/journal-article-pdfs/20_3_Foltz.pdf (10.06.2013)

Fricker, R.D., Jr. (2012). The SAGE Handbook of Online Research Methods. *Sampling Methods for Web and E-mail Surveys.* Chapter 11, 195-216. London: SAGE Publications. Loetud aadressil: http://faculty.nps.edu/rdfricke/docs/5123-Fielding-Ch11.pdf (6.10.2013)

Gizmo's Freeware (2013). Best Free Parental Filter. Loetud aadressil: http://www.techsupportalert.com/best-free-parental-Filter.htm (14.11.2013)

Google (2013).Google'i ohutustööriistad. Loetud aadressil: http://www.google.com/intl/et/goodtoknow/familysafety/tools/(10.10.2013)

Haddon, L., Livingstone, S. (2012). *EU Kids Online: national perspectives.* EU Kids Online, The London School of Economics and Political Science, London, UK. Loetud aadressil: http://eprints.lse.ac.uk/46878/1/EU%20Kids%20Online%20national%20perspectives%20%28lsero%29.pdf (1.02.2013)

Harris Interactive (2007). *Trends and Tudes: Cyberbullying*. Loetud aadressil: http://www.harrisinteractive.com/news/newsletters/k12news/HI_TrendsTudes_2007_v06_i04.pdf (12.10.2013)

Hart Research Associates (2011). *Who Needs Parental Controls? A Survey of Awareness, Attitudes and Use of Online Parental Controls.* Loetud aadressil: http://www.fosi.org/images/stories/research/fosi_hart_survey-report.pdf (22.09.2013)

Hasebrink, U., Görzig., Haddon, L., Kalmus, V.,Livingstone, S. (2011). *Patterns of risk and safety online: in-depth analyses from the EU Kids Online survey of 9- to 16-year-olds and their parents in 25 European countries.* EU Kids Online, Deliverable D5. EU Kids Online Network, London, UK. Loetud aadressil: http://eprints.lse.ac.uk/39356/1/Patterns_of_risk_and_safety_online_%28LSERO%29.pdf (22.05.2013)

Heins, M., Cho, K., & Feldman, K. (2006). *Internet Filters. A Public Policy Report.* Loetud aadressil: http://www.fepproject.org/policyreports/filters2.pdf (2.09.2013)

Hirsjärvi, S., Remes, P., Sajavaara, P. (2005). Uuri ja kirjuta. Tallinn: Medicina.

Insafe (2013a). Filtering, monitoring and parental controls. Loetud aadressil: http://www.saferinternet.org/online-issues/parents-and-carers/filtering-monitoring-and-parental-controls (19.10.2013)

Insafe (2013b). *Insafe Good Practice Guide: Insafe resources on mobile devices.* http://www.saferinternet.org/c/document_library/get_file?uuid=b9b0915b-3387-4271-82fb-ec79246ab878&groupId=10137 (19.10.2013)

Jigsaw Research (2012). *Parents' views on parental controls.* Loetud aadressil: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/Annex_1.pdf (13.02.2013)

Johns, R. (2010). *Likert Items and Scales.* Loetud aadressil: http://surveynet.ac.uk/sqb/datacollection/likertfactsheet.pdf (12.10.2013)

K9 Web Protection (2013). Product Features. Loetud aadressil: http://www1.k9webprotection.com/aboutk9/product-features (1.11.2013)

Kalmus, V. (2013). *Ebasündsad pildid ja vilkuvad bännerid: mis häirib lapsi internetis?* Loetud aadressil: http://www.ut.ee/sites/default/files/www_ut/taiendusope/veronika_kalmus.pdf (10.11.2013)

Kalmus, V., Keller, M., Pruulmann-Vengerfeldt, P. (2009). Lapsed ja noored tarbimis- ja infoühiskonnas. M. Lauristin (Ed.), *Eesti Inimarengu Aruanne 2008*. Eesti Koostöö Kogu: Tallinn, 115-122. Loetud aadressil: http://www.kogu.ee/public/EIA08_est.pdf (8.10.2013)

Karu, K. (2010*). I klassi õpilaste teadlikkus online-riskidest ning vanemate käitumispraktikad lasteinterneti kasutuse kujundamisel Tartu koolide näitel (bakalaureusetöö).* Loetud aadressil: https://dspace.utlib.ee/dspace/bitstream/handle/10062/15310/Karu_Kersti.pdf (30.10.2013)

Kaspersky Lab (2012a). The top Internet dangers for kids. Loetud aadressil: http://www.kaspersky.com/about/news/virus/2012/The_top_Internet_dangers_for_kids (30.10.2013)

Kaspersky Lab (2012b). Statistics on Parental Control alerts for various countries. Loetud aadressil: http://www.securelist.com/en/blog/727/Statistics_on_Parental_Control_alerts_for_various_countries (4.9.2013)

Kaspersky Lab (2012c). How to control personal data transfer using Parental Control in Kaspersky PURE 2.0. Loetud aadressil: http://support.kaspersky.com/8078 (4.11.2013)

Kidrex.org (2013). What is KidRex and how does it work? Loetud aadressil: http://www.kidrex.org/parents/about.html (14.11.2013)

Kirna, A. (2012). Jälgida või mitte? Loetud aadressil: http://www.arvutikaitse.ee/jalgida-voi-mitte/ (9.11.2013)

Legal Information Institute (2003). United States v. American Library Assn., Inc. Loetud aadressil: http://www.law.cornell.edu/supct/html/02-361.ZS.html (24.09.2013)

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet:* The*perspective of Europeanchildren*. London: EU Kids Online. Loetud aadressil: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/D4FullFindings.pdf (1.06.2013)

Livingstone, S., Ólafsson, K., O'Neill, B., Donoso, V. (2012) *Towards a better internet forchildren: findings and recommendationsfrom EU Kids Online to inform the CEO coalition.* EU Kids Online , The London School of Economics and PoliticalScience, London, UK. Loetud aadressil:

http://eprints.lse.ac.uk/44213/1/Towards%20a%20better%20internet%20for%20children%28LSERO%29.pdf (1.12.2013)

Lobe, B., Livingstone, S., Ólafsson, K., Vodeb, H. (2011).*Cross-national comparison of risks and safety on the internet.* London: EU Kids Online. Loetud aadressil: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/D6%20Cross-national.pdf (1.03.2013)

Luik, P. (2009). *Sotsiaalsed probleemid virtuaalmaailmas.* Loetud aadressil: http://dspace.utlib.ee/dspace/bitstream/handle/10062/9127/?sequence=1 (1.09.2013)

Mandre, E. (2011). Mida teha meie noorte arvutipiraatlusega? *Õpetajate leht*, 4. Reede, 11. november, Nr. 41. Loetud aadressil: http://opleht.ee/arhiiv/?archive_mode=article&articleid=6348 (17.09.2013)

McAfee (2009). *A Parent's Guide to Social Networking Sites.* Loetud aadressil: http://promos.mcafee.com/en-US/PDF/SocialNetworkinge-guide.pdf (29.10.2013)

McAfee (2012). *The Digital Divide: How the Online Behavior of Teensis Getting Past Parents.* Loetud aadressil: http://www.mcafee.com/us/resources/misc/digital-divide-study.pdf (15.10.2013)

Mendoza, K. (2009). Surveying Parental Mediation: Connections, Challenges and Questions for Media Literacy. *Journal of Media Literacy Education*. 28-41. Loetud aadressil:http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1002&context=jmle (5.09.2013)

Microsoft (2007). Windows Vista and 2007 Microsoft Office system launched – largest product launch from Microsoft in over a decade. Loetud aadressil: http://www.microsoft.com/australia/presspass/post/Windowsc2ae-Vista-and-2007-Microsoft-Officee284a2-system-launched-e28093-largest-product-launch-from-Microsoft-in-over-a-decade (6.10.2013)

Microsoft (2013). Mida saab vanemliku järelevalve abil kontrollida? Loetud aadressil: http://windows.microsoft.com/et-ee/windows/what-can-control-parental-controls#1TC=windows-7 (15.10.2013)

MTAC (2012). *Report on Internet Filters.* Loetud aadressil: http://media-aware.net/resources/internet_filter_report/MTAC%20Filter%20Testing%20report%20-%202012-08-14.pdf (15.11.2013)

National Center for Education Statistics (2001*). Internet Access in U.S. Public Schools and Classrooms: 1994 – 2000*. Loetud aadressil: http://nces.ed.gov/pubs2001/2001071.pdf (14.10.2013)

National Center for Missing and Exploited Children (2001). *Online Victimization: A Report on the Nation's Youth*. Loetud aadressil: http://www.unh.edu/ccrc/pdf/Victimization_Online_Survey.pdf (18.10.2013)

National Computer Board (2012). *Guideline on Windows 7 Parental Controls*. Loetud aadressil: http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Windows%207%20Parental%20Controls.pdf (15.09.2013)

Net Nanny (2013). *Net Nanny 6.5 User Guide*. Loetud aadressil: http://www.netnanny.com/assets/documentation/nn/cpuserguide-current.pdf (1.10.2013)

O'Brien, N. & Moules, T. (2010). *The impact of cyber-bullying on young people's mental healt.* Loetud aadressil: http://www.ncb.org.uk/media/111007/cyber-bullying_report.pdf (30.08.2013)

OECD (2012).*The protection of children online. Recommendation of the oecd council.* Loetud aadressil: http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf (9.10.2013)

Ofcom (2013). *Children and Parents: Media Use and Attitudes Report.* Loetud aadressil: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf (22.11.2013)

Oja, E. (2011). *Lapsevanemate arvamused telemeedia negatiivsest mõjust väikelapsele (bakalaureusetöö).* Loetud aadressil: http://dspace.utlib.ee/dspace/bitstream/handle/10062/18024/oja_egle.pdf (15.10.2013)

Open DNS (2013). Protect your family on computers, gaming consoles, mobile devices and more. Loetud aadressil: http://www.opendns.com/parental-controls (2.11.2013)

Parental Control Software (n.d). In *Wikipedia*. Loetud aadressil: http://en.wikipedia.org/wiki/Parental_controls (20.11.2013)

PCWorld (2009). Keep Kids Safe Online: The KIDO'Z Browser. Loetud aadressil: http://www.pcworld.com/article/165348/Keep_Kids_Safe_Online_The_KIDOZ_Browser.html (3.11.2013)

Perry, J. (2012). *Digital stalking: A guide to technology risks for victims.* Loetud aadressil: http://www.rapecrisisscotland.org.uk/workspace/publications/Digital_stalking_A_guide_to_technology_risks_for_victims_2012.pdf (2.12.2013)

Pew Research Center (2011). *Teens, Kindness and Cruelty on Social Network Sites.* Loetud aadressil: http://www.pewinternet.org/~/media//Files/Reports/2011/PIP_Teens_Kindness_Cruelty_SNS_Report_Nov_2011_FINAL_110711.pdf (12.09.2013)

PhoneSheriff (2013). Child Monitoring Facts. Loetud aadressil: http://www.phonesheriff.com/parental.html (8.11.2013)

Politsei- ja Piirivalveamet (2011). *Tuttav Internet (voldik).* Loetud aadressil: https://www.politsei.ee/dotAsset/227910.pdf (28.09.2013)

Postimees (2012). Internetis ringleb järjekordne peksmisvideo. Loetud aadressil: http://www.postimees.ee/1012096/internetis-ringleb-jarjekordne-peksmisvideo (11.09.2013)

Päriselt ka või?(2013). Täiskasvanutele. Loetud aadressil: http://päriseltkavõi.ee/taiskasvanule (29.10.2013)

Sharma, S. (2013). *How to Access Blocked Websites* Loetud aadressil:. http://kyatechnologyhai.com/how-to-access-blocked-websites/ (12.09.2013)

SIP-Bench (2013). *Benchmarking of parental contro ltools for the online protection of children. Assessment results and methodology 5th Cycle.* Loetud aadressil: http://www.sipbench.eu/transfer/Report_5th_cycle.pdf (2.05.2013)

Thierer, A. (2009). *Parental Controls & Online Child Protection: A Survey of Tools & Methods.* The Progress & Freedom Foundation. Washington. Loetud aadressil: http://www.pff.org/parentalcontrols/Parental%20Controls%20&%20Online%20Child%20Protection%20[VERSION%204.0].pdf (15.10.2013)

Toompalu, S. (2010). *Statistika ja tõenäosusteooria (loengu konspekt).* Loetud aadressil: http://www.e-ope.ee/_download/euni_repository/file/796/ST-Loeng-01-0-Statistika-olemus-ja-tegevusvaldkonnad.pdf (2.12.2013)

Top Ten Reviews (2013a). CYBERsitter 11 review. Loetud aadressil: http://parental-software-review.toptenreviews.com/cybersitter-review.html (15.10.2013)

Top Ten Reviews (2013b). Parental Software Review. Loetud aadressil: http://parental-software-review.toptenreviews.com/ (15.10.2013)

Top Ten Reviews (2013c). Cell Phone Parental Control Software Review. Loetud aadressil: http://cell-phone-parental-control-software-review.toptenreviews.com/ (5.11.2013)

Turu-uuringute AS (2006). Lapsed ja Internet. Loetud aadressil: http://www.adm.ee/presentations/microsoft/uuringu_kokkuvote2006.pdf (5.11.2013)

Tuuling, T. (2013). *Küberkiusamise toimetulekustrateegiad 14-15 aastaste õpilaste hinnangul kolme Tartu kooli näitel (bakalaureusetöö).* Loetud aadressil: http://dspace.utlib.ee/dspace/bitstream/handle/10062/30986/tuuling_tiia.pdf (15.10.2013)

Whitby, P. (2012). *Turvalise internetikäitumise käsiraamat lapsevanematele.* Tallinn: Valgus.

Vinter, K. (2013). *Digitaalse ekraanimeedia tarbimine 5–7-aastaste laste seas ja selle sotsiaalne vahendamine eestis. Pedagoogiline vaatekoht (doktoritöö).* Loetud aadressil:http://e-ait.tlulib.ee/318/1/vinter_kristi.pdf (1.01.2013)

Vinter, K. (2011). *Esimesed sammud väikeste laste meediakasvatuses Eestis: Uurimistulemusi ja soovitusi õpetajakoolituse arendamiseks.* AS Atlex. Loetudaaressil: http://eduko.archimedes.ee/files/Esimesed%20sammud%20v%C3%A4ikeste%20laste%20meediakasvatuses%20Eestis_MEVA%20bro%C5%A1%C3%BC%C3%BCr.pdf (1.03.2013)

Üksikvanem (2013). Statistika. Loetud aadressil: http://www.yksikvanem.com/statistika/ (1.09.2013)

Lisa 1. Ohtlike materjalide kategooriad

(K9 Web Protection rakendus)

Lisa 2. Vanemliku kontrolli programmide hindamise edetabel

(Sip-Bench, 2013)

Programm	**Funktsionaalsus**	**Efektiivsus**	**Kasutatavus**	**Turvalisus**	**Koondhinnang**	**Maksumus****
1. PureSight Owl	3.41	2.3	3.04	4	2.67	46.00
2. Norton Online Family	1.78	2.3	3.05	4	2.54	Free
3. Telekom Kinderschutz Software	2.07	2.2	2.5	4	2.39	Free
4. Kaspersky Pure	3.41	2	2.69	3	2.33	60.00
5. Net Nanny	2.67	1.6	2.46	4	2.05	30.00
6. Trend Micro Online Guardian	1.93	1.6	2.86	3	1.99	23.00
7. K9 Web Protection	1.63	1.5	2.56	4	1.92	Free
8. AVG Family Safety	2.52	1.5	2.83	1	1.81	14.95
9. Windows Live Family Safety*	2.81	1.5	2.68	1	1.80	Free
10. Profil Parental Filter 2	3.41	1.2	2.44	3	1.77	39.99
11. Safe Eyes	2.96	1	2.39	4	1.68	38.00
12. McAfee Family Protection	2.67	1	2.3	4	1.63	36.95
13. F-Secure Internet Security*	1.33	1.2	2.52	3	1.62	49.95
14. Enologic Net Filter	1.48	1.5	2.23	1	1.60	40.00
15. Xooloo	1.48	1.4	2.47	1	1.59	29.99
16. Mac OS X Parental Controls	2.37	0.9	2.6	3	1.53	Free
17. Mobicip	2.07	0.9	2.15	4	1.49	7.75
18. CyberSitter	2.37	1.1	2.28	1	1.43	30.00
19. WhiteNet*	1.19	1.3	1.84	1	1.37	24.95
20. CyberSieve	2.81	0.6	2.17	4	1.36	27.00
21. CyberPatrol	2.22	0.6	2.58	2	1.24	30.00

*kättesaadav Eesti keeles

Lisa 3. Ankeet

KÜSIMUSTIK LAPSEVANEMALE

1 / 3

Lugupeetud lapsevanem!

Kui teie peres on olemas laps(ed) vanuses 4 kuni 12 aastat, siis palun leidke aega, et vastata allolevale ankeedile. Küsitluse eesmärgiks on uurida milliseid turvameetmeid kasutavad lastevanemad, et kaitsta oma last online-riskide eest, ning kui suurt rolli selles mängivad vanemliku kontrolli programmid? (*vanemliku kontrolli programmi abil saab filtreerida lapsele mittesobiva veebisisu, blokeerida valitud programme ja tegevusi ning monitoorida lapse toiminguid veebis). Ankeet koosneb 3 lehest ja võtab aega umbes 20 minutit.

1. Mitu last on teie peres vanuses 4 kuni 12 aastat?

NB! Kui teie peres on rohkem kui üks laps vanuses 4 kuni 12, siis palun vastake ankeedile mõeldes lapsest kelle sünnipäev on tänase kuupäevale kõige lähemal.

2. Kui vana teie laps on?

3. Lapse sugu:

- Poiss
- Tüdruk

4. Kui vana oli teie laps kui hakkas kasutama arvutit?

5. Mitu tundi keskmiselt päevas teie laps viibib arvuti taga kodus?

6. Kas laps kasutab arvutit administraatori õigustes (saab ise arvutisse programme installeerida ja kustutada)?

- Jah
- Ei
- ei tea

7. Kui sageli teie laps kasutab interneti (ükskõik millises kohas: kodus, koolis, sõprade juures)?

- iga päev
- 4-5 korda nädalas
- paar korda nädalas
- kord nädalas või harvem

8. Milliste vahenditega kasutab/ühendub laps kodus internetti? Märkige kõik sobivad variandid.

- pere arvuti/sülearvuti
- isiklik arvuti/sülearvuti
- tahvelarvuti
- mobiiltelefon
- mängukonsool

9. Kas teie laps omab negatiivset kogemust seoses interneti kasutamisega viimasel poolel aastal? (kogemus mille peale laps oli nukker või masendunud)

- jah, mitu korda
- paar korda
- üks kord
- ei

10. Kui sageli teie laps sooritab järgmisi tegevusi arvutis/internetis?

1-mitte kunagi 2-harva 3-mõnikord 4-üsna sageli 5-regulaarselt

	1-mitte kunagi	2-harva	3-mõnikord	4-üsna sageli	5-regulaarselt	ei oska öelda
teeb kodutöid, õpib	○	○	○	○	○	○
mängib	○	○	○	○	○	○
kuulab muusikat	○	○	○	○	○	○
otsib erinevat infot	○	○	○	○	○	○
kasutab suhtlusvõrgustikke (rate.ee, Facebook, Orkut jm)	○	○	○	○	○	○
vaatab videot (nt YouTube)	○	○	○	○	○	○
installib uusi programme	○	○	○	○	○	○
alla laadib faile (filmid, muusika, pildid jm)	○	○	○	○	○	○
üles laadib fotosid või videoid internetti	○	○	○	○	○	○
suhtleb kiirsõnumi programmides (Skype,MSN jm)	○	○	○	○	○	○
kasutab veebikaamerat	○	○	○	○	○	○
kasutab e-maili	○	○	○	○	○	○
kasutab P2P programmi (nt Torrent)	○	○	○	○	○	○
surfab meelelahutuslikult veebis	○	○	○	○	○	○
loeb uudiseid, raamatuid, ajakirju	○	○	○	○	○	○
peab oma blogi/ loeb blogisid	○	○	○	○	○	○
kasutab internetipanka	○	○	○	○	○	○
sooritab ostusid internetis	○	○	○	○	○	○

Kas soovite lisada veel mõne tegevuse, mida teie laps teeb üsna sageli või regulaarselt?

11. Kuidas jälgite oma lapse tegutsemist internetis? Märkige kõik sobivad variandid.

- ☐ suhtlen lapsega, küsin temalt mida ta tegi
- ☐ püüan olla lapse lähedal, et näha mis laps teeb online'is
- ☐ kontrollin hiljem veebilehed, mida laps on külastanud
- ☐ kasutan spetsiaalset „vanemliku kontrolli" tarkavara (näiteks viirusetõrje, operatsioonisüsteemi või brauseri lisavõimalused)
- ☐ ei kontrolli last
- ☐ kontrollin teisiti:

12. Kas teie peres on olemas mõned kokkulepped, reeglid või piirangud seoses lapse ... (Märkige kõik sobivad variandid)

- ☐ arvuti ja interneti kasutamisega
- ☐ nuti- või mobiiltelefoni kasutamisega
- ☐ mängukonsooli kasutamisega
- ☐ televiisori vaatamisega
- ☐ reegleid/piiranguid ei ole

13. Kirjeldage palun, millised need põhilised reeglid/kokkulepped on:

14. Kuidas teile tundub, kui palju abi on nendest reeglitest?

- ei ole abi
- pigem vähe
- pigem palju
- palju abi

15. Millist kokkulepet või reeglit kõige sagemini tuleb tihedasti uuesti selgitada?

16. Kui ohtlikud teie arust järgmised laste toimingud veebis ilma vanemate järelevalveta?

1-ei ole ohtlik 2-väheohtlik 3-mõõdukalt ohtlik 4-väga ohtlik

	1-ei ole ohtlik	2-väheohtlik	3-mõõdukalt ohtlik	4-väga ohtlik	ei oska öelda
infootsing					
veebis surfamine					
suhtlusvõrgustikes suhtlemine					
kiirsuhtlusprogrammide kasutamine (nt Skype)					
failide allalaadimine (muusika, filmid, programmid)					
veebikaamera kasutamine					
e-posti kasutamine					
foorumites suhtlemine					
jututoad					
mängud internetis					
video online'is (nt YouTube)					

Kas soovite lisada veel mõne tegevuse, mida sooviksite jälgida, mis on teie meelest mõõdukalt või väga ohtlik?

17. Millised teemad/valdkonnad peate teie lapse jaoks ohtlikuks, teemad mida sooviksite lapse arvutis blokeerida?

1-ei ole ohtlik 2-väheohtlik 3-mõõdukalt ohtlik 4-väga ohtlik

	1-ei ole ohtlik	2-väheohtlik	3-mõõdukalt ohtlik	4-väga ohtlik	ei oska öelda
pornograafia					
narkootikumide propageerimine					
vägivald, julmus					
rassism, vaenu õhutamine					
ropendamine, ebatsensuurne tekst					
relvad					
suitsiid, enesekahjustamine					
häkkerlus					
piraatlus, illegaalne tarkvara					
hasartmängud					

Teised teemad, mis on teie arust mõõdukalt ohtlikud või väga ohtlikud lastele internetis

18. Kui mõelda vanemliku kontrolli tarkvarast, milline funktsionaalsus teie perele oleks oluline?

1-pole oluline 2-väheoluline 3-üsna oluline 4-väga oluline

	1-pole oluline	2-väheoluline	3-üsna oluline	4-väga oluline	ei oska öelda
ajalimiidi seadmine (nt arvuti/interneti kasutamine 2 tundi päevas)	○	○	○	○	○
jätab meelde ja annab ülevaate kõigist külastatud veebilehtedest	○	○	○	○	○
jätab meelde ja annab ülevaate kõigist avatud failidest	○	○	○	○	○
mittesobiliku/ohtliku sisuga veeblehtede tuvastamine ja blokeerimine	○	○	○	○	○
valitud programmide blokeerimine	○	○	○	○	○
valitud mängude blokeerimine	○	○	○	○	○
online-ostude blokeerimine	○	○	○	○	○
uute programmide installeerimist keelamine	○	○	○	○	○
failide allalaadimist keelamine	○	○	○	○	○
suhtlusvõrgustike monitooring ja vajadusel blokeerimine	○	○	○	○	○
suhtlusprogrammide (nt Skype) monitooring ja vajadusel blokeerimine	○	○	○	○	○
P2P (nt Torrent) programmide monitooring ja vajadusel blokeerimine	○	○	○	○	○
e-posti monitooring	○	○	○	○	○
voogvideo filtreerimine (nt YouTube)	○	○	○	○	○
valitud kaustade/failide lukustamine	○	○	○	○	○

19. Millistele tingimustele peab vastama hea vanemliku kontrolli programm kasutatavuse osas?

1-pole oluline 2-väheoluline 3-üsna oluline 4-väga oluline

	1-pole oluline	2-väheoluline	3-üsna oluline	4-väga oluline	ei oska öelda
lihtne installeerimine	○	○	○	○	○
lihtne ja selge töökeskkond	○	○	○	○	○
eestikeelse kasutajaliidesega	○	○	○	○	○
peab omama kaitset, et laps ei saa seda kustutada või välja lülitada	○	○	○	○	○
arusaadav ja põhjalik raport laste tegutsemisest internetis	○	○	○	○	○
peab olema tasuta või madala hinnaga	○	○	○	○	○

Mida veel ootate vanemliku kontrolli tarkvarast, milliseid muid funktsionaalsuseid vajaksite?

20. Lõpetage lause: Hea vanemliku kontrolli programm peab olema pigem...

- ○ nähtamatu lapsele, laps ei tea, et tema tegevust kontrollitakse/piiratakse, dialoogiaknad ei ilmu.
- ○ nähtav lapsele, annab lapsele selgelt teada (dialoogiakendega) et teatud veebileht või rakendus on keelatud.

21. Kas arvutisse, mis teie laps kodus kasutab, on installeeritud vanemliku kontrolli programm või mõni sarnane tarkvara?

- Jah
- Ei

Kui valisite „EI" siis palun liikuge edasi küsimuse number 24 juurde!

22. Kui „jah", siis palun täpsustage millist programmi kasutate (programmi nimi):

23. Mida olete selle programmiga piiranud/blokeerinud? Märkige kõik sobivad variandid.

- blokeerisite veebilehekülgi
- monitoorisite laste poolt külastatud veebilehti
- piirasite arvuti kasutamisaega
- piirasite/blokeerisite suhtlusvõrgustike kasutamist
- blokeerisite programmide kasutamist
- midagi veel:

24. Kui teie ei kasuta vanemliku kontrolli programmi, siis palun täpsustage miks? Märkige kõik sobivad variandid.

- ei pea seda vajalikuks
- ei oma tehnilisi oskusi programmi seadistamiseks
- ei usu, et see programm on efektiivne
- ei ole sellistest programmidest varem kuulnud
- muu põhjus:

25. Kuivõrd olete nõus järgmiste väidetega?

1-ei ole üldse nõus 2-pigem ei ole nõus 3-pigem nõus 4-täiesti nõus

	1-ei ole üldse nõus	2-pigem ei ole nõus	3-pigem nõus	4-täiesti nõus	ei oska öelda
mina hästi tunnen arvutit ja internetti					
hästi valdan internetiturvalisuse teemat					
lapsed vajavad vanemate toetust internetis sama palju kui reaalelus					
lapsevanemal peab olema täielik kontroll selle üle, mida laps teeb internetis					
internetiturvalisuse alaseid materjale lapsevanematele veebis on palju					
minu laps veedab internetis liiga palju aega					
minu laps oskab arvutit paremini kui mina					
internetis on palju potentsiaalseid ohtusid lapsele					
vanemliku kontrolli programmi kasutamine rikub suhteid lapsega					

26. Palun vastake, kui tihti teie...

1-mitte kunagi 2-harva 3-mõnikord 4-üsna sageli 5-regulaarselt

	1-mitte kunagi	2-harva	3-mõnikord	4-üsna sageli	5-regulaarselt	ei oska öelda
surfate internetis koos oma lapsega	○	○	○	○	○	○
küsite lapselt mida tema teinud, näinud Internetis	○	○	○	○	○	○
asute lapse kõrval, kui ta kasutab arvutit või internetti	○	○	○	○	○	○
räägite lapsega internetiturvalisust, kuidas ohutult käituda internetis	○	○	○	○	○	○
kontrollite veebilehed mida laps külastanud on	○	○	○	○	○	○
kontrollite lapse postkasti, kellega laps suhtleb	○	○	○	○	○	○
kontrollite lapse suhtlusvõrgustike profiile ja sõbralisti	○	○	○	○	○	○
kontrollite lapse kontaktlisti suhtlusprogrammides	○	○	○	○	○	○
julgustate oma last online-muredest teiega rääkida	○	○	○	○	○	○

27. Laste internetiturvalisuse tagamiseks on esmatähtis ...

1 -pole tähtis 2-vähe tähtis 3-üsna tähtis 4-väga tähtis

	1-pole tähtis	2-vähe tähtis	3-üsna tähtis	4-väga tähtis	ei oska öelda
et lapsevanem oleks alati lapse juures, kui laps online'is	○	○	○	○	○
lapse harimine internetiturvalisuse teemadel	○	○	○	○	○
selged reeglid ja piirangud peres, - mida laps tohib veebis teha ja mida mitte	○	○	○	○	○
tehnilised vahendid - vanemliku kontrolli programmid	○	○	○	○	○
vastavad seadused, mis kaitsevad last internetis	○	○	○	○	○

28. Kes teie arust peab lapse internetiturvalisuse eest hoolitsema?

1-ei pea hoolitsema 2-pigem ei pea 3-pigem peab 4-kindlasti peab hoolitsema

	1-ei pea hoolitsema	2-pigem ei pea	3-pigem peab	4-kindlasti peab hoolitsema	ei oska öelda
laps ise	○	○	○	○	○
lapsevanem	○	○	○	○	○
kool ja haridusasutused	○	○	○	○	○
lastekaitseorganisatsioonid	○	○	○	○	○
riik (politsei, ministeeriumid)	○	○	○	○	○
interneti teenusepakkujad	○	○	○	○	○
tarkvara arendajad, IT firmad	○	○	○	○	○
portaalid, veebilehed	○	○	○	○	○

29. Kuidas arvate, mis vanusest laps on piisavalt küps, et iseseisvalt kasutada interneti ilma vanemate järelevalveta? *

VASTAJA ANDMED

Teie vanus

- ○ 0-30
- ○ 31-40
- ○ 41-50
- ○ >50

Teie sugu

- ○ M
- ○ N

Teie haridus

- alusharidus
- keskharidus
- keskeriharidus
- kõrgharidus

Mitu täiskasvanut inimest elab teie leibkonnas?

Kes on teie peres tunneb arvutit kõige paremini, kellelt küsitakse nõu IT-probleemide lahendamisel?

Kas soovite tutvuda uurimuse tulemustega (kevad 2013)?

Kui soovite, siis palun jätke oma e-mail:

Kas olete nõus osalema intervjuus, et oma vastuseid kommenteerida?

(mõnede vastajatega võtame ühendust, et esitada täiendavaid küsimusi). Kui olete nõus, siis palun jätke oma kontakt (nimi, e-mail või telefon). Kui ei soovi osaleda, siis jätke see lahter tühjaks.

saada