VILNIAUS UNIVERSITETAS
KAUNO HUMANITARINIS FAKULTETAS

INFORMATIKOS KATEDRA

MANTAS LUKOŠEVIČIUS

MAGISTRO BAIGIAMASIS DARBAS

VAIKŲ SAUGUMO INTERNETE UŽTIKRINIMO ĮGŪDŽIŲ SERTIFIKAVIMO PROGRAMOS TYRIMAS

Leidžiama ginti _____

Magistrantas _____
(Parašas)

Darbo vadovas doc. dr. Eugenijus Telešius
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

(parašas) _____

Darbo įteikimo data 2009 06 02

Registracijos Nr. _____

Kaunas 2009

VILNIAUS UNIVERSITETAS
KAUNO HUMANITARINIS FAKULTETAS
INFORMATIKOS KATEDRA

Verslo informatikos studijų programa
Kodas 62109P101

MANTAS LUKOŠEVIČIUS

MAGISTRO BAIGIAMASIS DARBAS

VAIKŲ SAUGUMO INTERNETE UŽTIKRINIMO ĮGŪDŽIŲ SERTIFIKAVIMO PROGRAMOS TYRIMAS

Kaunas 2009

TURINYS

SANTRUMPŲ SĄRAŠAS

AQTB – angl. Automated Question and Test Base;
MQTB – angl. Manual Question and Test Base
ECDL – angl. European Computer Driving Licence
ECDL-F – angl. European Computer Driving Licence Foundation
ICDL – angl. International Computer Driving Licence
CEPIS – angl. Council of European Professional Informatics Societies
CAD – angl. Computer Aided Design
EUCIP – angl. European Certification of Informatics Professionals
CTP - angl. Certified Training Professional - Sertifikuotas mokymo profesionalas.
ICT – angl. Information and Communications Technology
EQTB – angl. European Question Test Base
GIS – angl. Geographic Information System
CITS – angl. Croatian Computer Society
ITI – "Informacinių technologijų institutas"
SYL – angl. Syllabus – liet. Klausimynas - sertifikavimo programos turinį glaustai apibūdinantis žinių ir įgūdžių sričių rinkinys.

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Internetas vis giliau ir plačiau skverbiasi į mūsų kasdienį gyvenimą. Juo naudodamiesi skaitome naujienas, gauname įvairiausias paslaugas, bendraujame, tvarkome finansinius reikalus, ieškome profesinės ir pomėgių informacijos. Tačiau ar mokame patys saugiai naudotis internetu ir apsaugoti nuo galimų jo grėsmių savo artimuosius? Kartu su interneto nauda neišvengiamai tenka aptarti ir interneto keliamus pavojus ypač vaikams [29]. Internetu naudojasi ne tik geranoriškai nusiteikę žmonės. Kaip ir realiame gyvenime, čia pasitaiko piktavalių asmenų, siekiančių neteisėtai pasipelnyti, apgauti, piktam pasinaudoti įgytu pasitikėjimu. Kai kuriems žmonėms tiesiog patinka įsibrauti į kitų žmonių kompiuterius, visaip kenkti, platinti virusus, vogti ir gadinti duomenis. Nedori verslininkai interneto paslaugas naudoja nepageidaujamiems laiškams bei reklamai platinti, nekalbant jau apie pornografijos verslą, kuris internetą tiesiog užtvindė vaikams netinkamu turiniu. Bendravimas su kitais žmonėmis internetu gali būti ne tik malonus. Anonimai gali įsijungti į pokalbį ir išreikšti agresiją ar kitaip įskaudinti. Blogiausia, kai taip nutinka nepilnamečiams, kurie į tai jautriai reaguoja, bei dažniausiai negali ar nenori apie tai pasikalbėti su suaugusiais ar netgi draugais.

Internete gausu smurtinės, pornografinės ir kitokios žalingos informacijos. Vaikai, naršydami internete, anksčiau ar vėliau gali su tokia informacija susidurti. Todėl turime būti pasirengę ne tik tokią informaciją riboti techninėmis priemonėmis, bet ir kalbėtis su vaikais, kad jie žinotų, kaip tinkamai į ją reaguoti. Nors vaikai ir jaunimas dažnai yra interneto technologijų žinovai ir supranta apie grėsmes ir būdus jas apeiti, tačiau jie ne visi pakankamai subrendę, kad tinkamai įvertintų situacijas ir galimas pasekmės, su kuriomis susiduria. Tuo metu, jie retai kada pasidalina patirtimi su tėvais ar globėjais ir kreipiasi pagalbos į juos tik paskutiniu atveju [1]. Tarp tėvų ir vaikų yra didelė žinių spraga apie augančias interneto grėsmes ir jų supratimą. Ir vaikus, ir suaugusius būtinai reikia daugiau informuoti, kaip imtis priemonių prieš interneto pavojus, nes vaikų ir nepilnamečių tarp interneto vartotojų vis labiau gausėja.

Šiuo metu kvalifikacijos kėlimo ir sertifikavimo rinkoje atsirado niša, kuri turėtų būti kuo greičiau užpildyta. Lietuvos ECDL atstovybė numatė sukurti naują sertifikavimo programą, kurios pagrindinis tikslas – tiesiogiai padėti organizacijų, susijusių su vaikų ugdymu, darbuotojams bei tėvams gauti žinias, reikalingas apsaugoti vaikus nuo grėsmių virtualiame pasaulyje ir tas žinias patvirtinti ECDL sertifikatu. Šios programos idėja - ne kiekvieno iš mūsų moralinių normų nagrinėjimas. Programa skirta suteikti žinias, reikalingas suprasti situaciją, veiksmų galimybes ir įrankių tiems veiksmams atlikti naudojimą.

ECDL fondas siūlo daug kompiuterių vartotojų įgūdžių sertifikavimo programų. Iš pradžių ECDL fondas skleidė tik bazines kompiuterinio raštingumo sertifikavimo programas. Vėliau buvo

sukurtos specializuotos programos skirtos atskirų informacinių technologijų sričių žinioms sertifikuoti. Pastaruoju metu, pagal ECDL fondo standartus, skirtingų šalių ECDL atstovybės gali kurti ir kuria sertifikavimo programas, atitinkančias iškilusius poreikius. Lietuvos ECDL atstovybė pradėjo darbus realizuojant sertifikavimo programą e-Guardian, kuri skirta patvirtinti žinias apie vaikų apsaugą internete.

Iki šiol, nėra spręsta **problema**, ar kompiuterinėmis sistemomis ir internetu besinaudojantys, su vaikais dirbantys asmenys žino ir moka tinkamai apsaugoti duomenis, kompiuterinę programinę ir aparatūrinę įrangą bei vaikus, naudojančius minėtas kompiuterines sistemas. Todėl labai naudinga sukurti naują sertifikavimo programą, kurios atsiradimas leistų su vaikais dirbančių organizacijų atstovams ir norintiems gauti sertifikatą tėvams patvirtinti savo žinias atitinkamo sertifikato išlaikymu.

Tokio pobūdžio sertifikavimas ECDL / ICDL organizacijoje nebuvo sukurtas. Apie kitų pasaulinių sertifikavimo organizacijų sukurtas tokios klasės sertifikavimo programas (susijusias su saugiu darbu kompiuteriu ir vaikų apsauga) informacijos nerasta. Todėl palyginti ir išanalizuoti informaciją apie padarytus darbus nėra galimybės. Dar vienas šio magistrinio darbo **naujumas** yra suformuluotas siūlymas ECDL fondui modifikuoti produktų patvirtinimo standartus automatizuoto testavimo atvejui. Šio darbo **objektas** - vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo sistema, apimanti taip pat ir bendrus informacijos saugos įgūdžius. Darbo **tikslas** - anglų kalba sukurti vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programą e-Guardian, turint tikslą ją autorizuoti ECDL fonde. Darbo tikslui pasiekti suformuluoti tokie uždaviniai:

- Išnagrinėti esamas ECDL sertifikavimo programas orientuojantis į specializuotų programų turinį.
- Išnagrinėti naujų ECDL programų kūrimo standartus.
- Sukurti, kiek galima labiau nuo aparatūrinės platformos ir PĮ nepriklausomą e-Guardian sertifikavimo programos klausimyną (syllabus).
- Sukurti e-Guardian sertifikavimo programos testų klausimų bazę automatizuotam testavimui (AQTB).
- Įkelti e-Guardian sertifikavimo testo klausimų bazę naudojimui ECDL Lietuva testavimo sistemoje.
- Ištirti e-Guardian klausimyno ir testo klausimų bazės atitikimą ECDL fondo kokybės valdymo sistemos reikalavimams.

Tyrime bus taikomi tokie **tyrimo metodai** – mokslinės literatūros analizė ir apibendrinimas, anketinė apklausa, eksperimentiniai matavimai, statistinės analizės metodai. Remiantis pirmuoju

metodu buvo rašoma darbo teorinė dalis. Teorinėje dalyje nagrinėjamos ECDL sertifikavimo programos, ECDL programų kūrimo standartai, e-Guardian programos vieta ECDL fondo programų tarpe. ECDL produkto kūrimo metodai nagrinėjami antroje dalyje. Čia aprašomas ECDL produkto standartizavimas ECDL fonde, sertifikavimo programos klausimyno ir klausimų sudarymo metodai. Trečioje - dviejų tyrimų aprašymas. Pirmajame – atliekama literatūros analizė, sudaromas e-Guardian klausimynas ir testo klausimai automatizuotam testavimui, antrajame - anketinės apklausos pagalba atlikto tyrimo apie e-Guardian testo klausimų bazės koregavimą aprašymas. Eksperimentiniai rezultatai naudojami klausimų bazės tobulinimui, pateikus bandomąją programos versiją vartotojams ir ekspertams. Pagrindiniai darbo rezultatai ir praktinė reikšmė:

1. Atlikta esamų specializuotų ECDL sertifikavimo programų apžvalga.
2. Išnagrinėti naujų specializuotų ECDL fondo programų kūrimo standartai ir jų kokybės valdymo sistema bei apibrėžta e-Guardian programos vieta ECDL fondo programų tarpe.
3. Sukurtas vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programos e-Guardian klausimynas.
4. Pagal sudarytą klausimyną sudaryta testo klausimų bazė automatizuotam testavimui.
5. Paruošta patvirtinimo paraiškos forma ir pateikta ECDL fondui, kuris patvirtino, jog e-Guardian svarba yra ypač didelė.
6. Sertifikavimo programos bandomoji versija patalpinta ECDL Lietuva testavimo sistemoje, siekiant nustatyti testavimo charakteristikas ir vertinimo kriterijus. Atlikti tyrimai, patvirtinantys sertifikavimo programos klausimyno ir testo klausimų bazės kokybę.

Rezultatų aprobavimas:

- 2008 metų birželio 21 d. vykusioje tarptautinėje mokslinėje konferencijoje “Strategies, Media, and Technologies in European Education Systems” kartu su bendraautoriumi Eugenijumi Telešiumi pristatytas straipsnis “E-Guardian Programme – The new ECDL Endorsed Product Proposal from ECDL Lithuania” [34] (1 priedas).
- 2009 metų balandžio 3 d. tarptautiniame forume „Baltic IT&T 2009: eBaltics“ Rygoje, Latvijoje, sekcijoje “Secure Future Internet Solutions” kartu su bendraautoriumi Eugenijumi Telešiumi buvo padarytas pranešimas “e-Guardian Certification Programme Pilot in Lithuania” [36] (4 priedas).
- 2009 metų gegužės 8 d. VUKHF vykusioje 14-oje magistrantų ir doktorantų mokslinėje konferencijoje „IT 2009“, sekcijoje „Informacinės technologijos mokyme“ pristatytas straipsnis

„E-Guardian – the New Certification Programme on Skills of Ensuring Children Safety Using Internet“ [35] (2 priedas).

Magistrinio darbo apimtis yra 82 puslapiai, kuriuos sudaro įvadas, trys pagrindinės dalys ir išvados. Pagrindinėse dalyse yra 1 lentelė ir informaciją grafiškai pateikiantys 9 paveikslai. Prie darbo pateikiami 7 priedai.

1. ECDL PROGRAMŲ IR PATVIRTINTŲ PARTNERINIŲ PROGRAMŲ KŪRIMO TEORINIAI ASPEKTAI

Šiame skyriuje pateikiama teorinė medžiaga apie ECDL fondą. Aprašomos ECDL fondo sukurtos ir patvirtintos partnerinės programos, apžvelgiant jų turinį. Pristatoma naujai kuriama e-Guardian sertifikavimo sistema, nustatant jos vietą ECDL fondo programų portfelyje.

1.1. ECDL fondas

ECDL programą propaguoja ir sklaidos procesą prižiūri ECDL fondas (ECDL-F – European Computer Driving Licence Foundation). Šio fondo paskirtis – remti ir koordinuoti ECDL koncepcijos plėtrą. ECDL-F yra ECDL standarto garantas [35]. Fondas užtikrina, kad ECDL būtų administruojamas tolygiai visoje Europoje ir pasaulyje. Fondas siekia sukurti Tarptautinį kompiuterio vartotojo pažymėjimą (ICDL – International Computer Driving Licence) ir tapti pasauline informacinių technologijų žinias sertifikuojančia ir standartizuojančia organizacija.

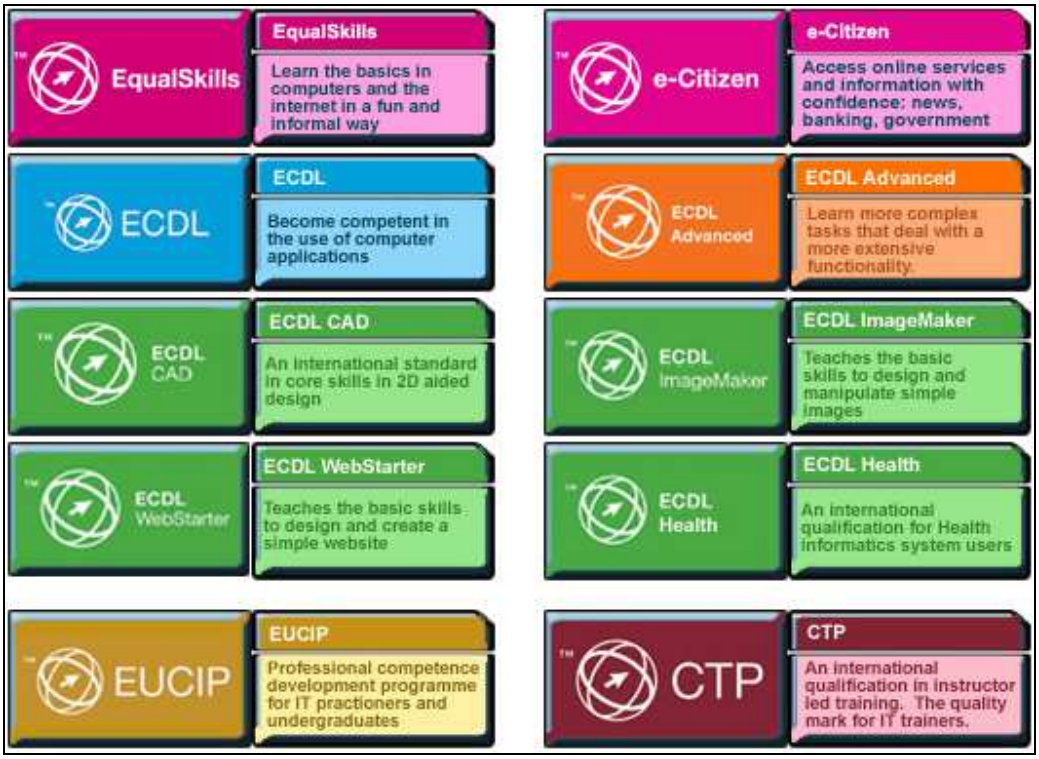
ECDL fondas buvo sukurtas siekiant koordinuoti ECDL koncepcijos atsiradimą ir plėtrą visoje Europoje. ECDL fondas yra pelno nesiekianti organizacija, kuri suteikia licenciją konkrečiai bet kurios šalies organizacijai – (licencijos turėtojui) naudotis ECDL koncepcija ir sukurti savo programą ECDL sklaidai toje šalyje. Europos šalyse nacionalinis licencijos turėtojas turi būti Europos profesinių informatikos sąjungų tarybos (CEPIS – Council of European Professional Informatics Societies) nariu. Ne Europos šalyse ECDL fondas suteikia licenciją organizacijoms, kurias CEPIS nurodo kaip licencijos turėtojas [13].

1.2. ECDL Programos

Sparčiai plėtojantis kompiuterinio raštingumo reikalavimams (tiek valstybinės, tiek privačios įmonės kelia vis aukštesnius reikalavimus kompiuterinėms darbuotojų žinioms), todėl didėja poreikis objektyviai įvertinti šių žmonių sugebėjimus. Taigi reikalinga vieninga sistema (apmokymo/ paruošimo, testavimo bei įvertinimo), kuri būtų pripažinta tarptautiniu mastu. Šiuo metu populiariausia ir labiausiai pripažįstama kompiuterinio raštingumo sertifikavimo sistema – ECDL (European Computer Driving Licence).

ECDL siekiantys asmenys – visi žmonės, kurie nori sumaniai naudotis asmeniniais kompiuteriais. ECDL kvalifikacija leidžia dirbantiesiems, studentams ir kitiems asmenims formaliai įrodyti ir patvirtinti, kad jie turi pagrindines žinias apie asmeninius kompiuterius ir sugeba jais naudotis. Pavyzdžiui, raštinės darbuotojai, norintys, kad formaliai būtų pripažinti ir dokumentu patvirtinti jų darbo kompiuteriu įgūdžiai, turėtų išlaikyti ECDL testus ir gauti atitinkamą pažymėjimą. Formalus darbo kompiuteriu kompetencijos patvirtinimas reikšmingas ir darbdaviams, norintiems įvertinti jų darbuotojų ar pretenduojančių įsidarbinti įgūdžius [13].

ECDL fondo produktų portfelyje yra 10 pagrindinių produktų (1 pav.), nuo pradinio lygio EqualSkills iki profesionalių programų IT specialistams.



Šaltinis: ECDL Foundation (2009) [žiūrėta 2009 01 06]. Prieiga per internetą: <http://www.ecdl.org/products/index.jsp>

Pav. 1 ECDL fondo produktų portfelis

Visos ECDL fondo sertifikacijos pasižymi ne tik aukštais produktų patvirtinimo, bet ir nuolatinio administravimo standartais. Tarptautiniu mastu pripažintas 148 šalyse ir pritraukęs 8 milijonus kandidatų į savo sertifikatų programas, ECDL fondas yra pasaulinis etalonas tarp eilinių vartotojų kompiuterių įgūdžių sertifikavimo programų.

1.2.1. ECDL Core programa

ECDL yra informacinių technologijų įgūdžių patvirtinimo pažymėjimas visiems piliečiams. Jis skirtas tiems, kam reikia arba kurie nori žinoti, kaip naudotis kompiuteriu. Jis tinka visų specialybių darbuotojams, tinka tik žengiantiems į darbo rinką, tinka ir bet kokio amžiaus žmonėms [13].

Europos kompiuterio vartotojo pažymėjimas (ECDL) – dokumentas, rodantis, kad jo savininkas turi pakankamai žinių apie informacijos technologiją ir sugeba naudotis asmeniniu kompiuteriu bei dažniausiai naudojama taikomąja programine įranga. Praktiniu požiūriu ECDL liudija, kad jo savininkas išlaikė teorinį egzaminą, įvertinantį informacijos technologijos pagrindų žinias, ir šešis praktinius testus, įvertinančius jo gebėjimus naudotis asmeniniu kompiuteriu bei jo taikomąja programine įranga [13].

ECDL yra visame pasaulyje pripažįstamas dokumentas. Jis skirtas palengvinti įdarbinimo procedūras ir užtikrinti darbdavį, kad pretendentai į darbo vietą ir jau dirbantys asmenys sugeba dirbti kompiuteriu ir naudotis įprastomis programomis. ECDL yra žinias ir kompetenciją patvirtinantis pažymėjimas, kuris remiasi vieninga Europoje pripažinta ECDL programa.

Pagrindinis ECDL programos tikslas – bendrasis pagrindinių žinių apie informacijos technologiją ir asmeninių kompiuterių bei jų taikomosios programinės įrangos panaudojimo kompetencijos lygio tobulinimas visoje Europoje ir pasaulyje [13].

ECDL standartas remiasi tuo, ką kompiuterio vartotojas turi žinoti apie informacijos technologiją ir asmeninius kompiuterius bei kokius asmeninių kompiuterių ir dažniausiai reikalingos jų taikomosios programinės įrangos panaudojimo įgūdžius jis turi įgyti. ECDL standarto numatytos būtinos žinių sritys ir įgūdžių grupės yra aprašytos ECDL programoje. Dar vienas ECDL programos tikslas – išvardinti faktus, kuriuos reikia žinoti, bei įgūdžius, kuriuos reikia įgyti pagal standarto reikalavimus [13].

ECDL Core yra praktinių įgūdžių ir kompetencijų testas, susidedantis iš septynių atskirų modulių, apimančių kompiuterinę teoriją ir praktiką. Norint gauti ECDL sertifikatą kandidatas turi išlaikyti visų septynių modulių testą. ECDL modulis 1 yra pagrindinių teorinių žinių apie kompiuterius testas, o moduliai 2-7 yra praktinių sugebėjimų testai.

1 modulis. Pagrindinės informacijos technologijos sąvokos. Reikalaujama, kad kandidatas žinotų, kaip sudarytas asmeninis kompiuteris, ir suprastų pagrindines informacijos technologijos koncepcijas: duomenų saugojimą pagrindinėje ir išorinėje atmintinėje, taikomosios programinės įrangos vietą visuomenėje, informacinių tinklų panaudojimą. Kandidatas turi suprasti, kokią vietą

kasdieniame gyvenime užima informacijos technologija, kokią įtaką asmeniniai kompiuteriai gali turėti žmogaus sveikatai. Kandidatas taip pat turi išmanyti pagrindinius informacijos saugos dalykus ir teisinius kompiuterių naudojimo aspektus.

2 modulis. Naudojimasis kompiuteriu ir bylų (angl. *file*) **tvarkymas.** Reikalaujama, kad kandidatas parodytų žinias ir gebėjimą naudotis pagrindinėmis asmeninių kompiuterių ir jų operacinių sistemų funkcijomis. Kandidatas turi sugebėti efektyviai tvarkytis kompiuterio darbo terpėje. Jis turi mokėti tvarkyti bylas ir katalogus (aplankus), mokėti kopijuoti, perkelti ir šalinti bylas ir katalogus (aplankus). Kandidatas taip pat turi parodyti, kad jis moka manipuliuoti darbo lauko piktogramomis ir langais. Jis turi parodyti, kad moka naudotis paieškos galimybėmis, operacinėje sistemoje esančiomis paprasčiausiomis redagavimo ir bylų spausdinimo valdymo priemonėmis.

3 modulis. Tekstų tvarkymas. Reikalaujama, kad kandidatas parodytų sugebąs naudotis asmeninio kompiuterio tekstų apdorojimo (angl. *word processing*) programine įranga. Jis turi suprasti ir mokėti atlikti pagrindinius veiksmus, reikalingus norint sukurti tekstinį dokumentą, jį tvarkyti ir užbaigti darbą, kad sukurtasis dokumentas būtų tinkamas platinti. Kandidatas taip pat turi parodyti sugebąs naudoti sudėtingesnes teksto apdorojimo operacijas – standartinių lentelių kūrimą, paveikslų ir kitų grafinių vaizdų įterpimą, objektų importavimą ir susiejimo su elektroniniu paštu priemones.

4 modulis. Skaičiuoklės. Reikalaujama, kad kandidatas suprastų pagrindines skaičiuoklių (angl. *spreadsheets*) sąvokas ir principus, mokėtų pasinaudoti asmeniniame kompiuteryje esančia skaičiuoklių programine įranga. Jis turi suprasti ir mokėti atlikti pagrindinius veiksmus, reikalingus sukurti, tvarkyti ir naudoti lentelę. Kandidatas turi sugebėti atlikti standartines matematines ir logines operacijas, panaudodamas pagrindines formules ir funkcijas. Kandidatas taip pat turi parodyti sugebąs naudoti kai kurias sudėtingesnes skaičiuoklių operacijas – objektų importavimą, grafikų ir diagramų kūrimą.

5 modulis. Duomenų bazės. Reikalaujama, kad kandidatas suprastų pagrindines duomenų bazių (angl. *database*) sąvokas ir principus, mokėtų pasinaudoti asmeniniame kompiuteryje esančia duomenų bazių programine įranga. Modulis padalintas į dvi dalis; pirmojoje dalyje patikrinami kandidato gebėjimai suprojektuoti paprastą duomenų bazę, naudojantis standartiniu duomenų bazių paketu, o antrojoje dalyje patikrinama, ar kandidatas gali gauti informaciją iš turimos duomenų bazės, naudodamas užklausas, pasirinkti ir surikiuoti duomenų bazėje esančius duomenis. Jis turi sugebėti kurti ataskaitas ir jas modifikuoti.

6 modulis. Pristatymai. Reikalaujama, kad kandidatas mokėtų panaudoti asmeniniame kompiuteryje esančias pristatymų (angl. *presentations*) rengimo priemones. Kandidatas turi sugebėti

atlikti pagrindinius veiksmus: sukurti pristatymą, jį tvarkyti ir paruošti demonstruoti bei platinti. Kandidatas turi parodyti gebąs sukurti įvairią pristatymų medžiagą, skirtą skirtingoms auditorijoms arba skirtingoms situacijoms. Kandidatas taip pat turi parodyti gebąs atlikti pagrindines operacijas su grafiniais vaizdais ir diagramomis, mokąs naudoti įvairius skaidrių demonstravimo efektus.

7 modulis. Informacija ir komunikacija. Modulis padalintas į dvi dalis. Pirmojoje dalyje (informacija) patikrinami kandidato gebėjimai atlikti pagrindines paieškos Internete užduotis ir panaudoti turimas paieškos priemones, pasižymėti paieškos rezultatus bei atspausdinti tinklalapius ir paieškos ataskaitas. Antrojoje dalyje (komunikacija) patikrinama, ar kandidatas sugeba naudotis elektroninio pašto programine įranga laiškams išsiųsti ir gauti, prijungti dokumentus ir bylas kaip laiškų priedus, kurti ir tvarkyti aplankus bei katalogus laiškams saugoti [13].

1.2.2. ECDL Advanced programa

ECDL / ICDL *Advanced* yra aukštesnio lygio programa sukurta tiems kas sėkmingai pasiekė ECDL Core žinių lygį ir nori toliau kelti savo kompiuterinę kvalifikaciją. ECDL / ICDL *Advanced* apima šiuos modulius:

- Advanced Word Processing
- Advanced Spreadsheets
- Advanced Database
- Advanced Presentation

ECDL / ICDL *Advanced* moduliai suteikia kandidatams galimybę tapti ekspertais naudojantis minėtomis aplikacijomis. Kiekvienas *Advanced* modulis sukurtas kaip atskiras sertifikavimas atitinkamoje srityje. Kandidatai, sėkmingai įsisavinę ir išlaikę kiekvieną modulį, sertifikuojami kaip konkrečios aplikacijos *Advanced* vartotojai. Kiekvieno modulio testavimo pasiruošimui paprastai reikia 30 valandų, nors, jei kandidatai turi reikiamas žinias, galima ir aplenkti pasiruošimo etapą. Yra išleista įvairios ECDL fondo patvirtintos pasiruošimo medžiagos, pagal kurią kandidatas gali ruoštis savo laisvu laiku.

Kiekvieno modulio testas trunka po 1 valandą. Sėkmingai išlaikę kiekvieną *Advanced* testą, kandidatai gauna *Advanced* sertifikatą iš atitinkamo modulio. Kandidatai, pasirinkę baigti visus keturis *Advanced* modulius, gauna naują ECDL / ICDL *Expert* sertifikatą, liudijantį ekspertinio lygio ECDL / ICDL kompetenciją.

1.2.3. e-Citizen programa

Kompiuteriai ir internetas dabar yra kasdieninio gyvenimo dalis ir mums visiems reikia sugebėti jais naudotis, kad atliktume dalį kasdieninių užduočių. Internetas tai ne tik naudingas bendravimo ir informacijos paieškos įrankis, bet vis daugiau organizacijų ir vyriausybės departamentų naudoją internetą tiekti informaciją ir paslaugas. Tie, kurie neturi interneto įgūdžių, rizikuoja būti atskirtais nuo informacinės visuomenės. Net jei atrodo, kad esame susipažinę su internetu, vis tik yra ir tokių žmonių, kuriems jis svetimas. e-Citizen yra išeitis tiems, kurie nemoka ir nesinaudoja internetu. e-Citizen - tai sprendimas, kuris leidžia kandidatams sužinoti apie internetą, neturint prieš tai įgytų kompiuterinių žinių.

e-Citizen sukurtas padėti žmonėms gauti kiek įmanoma daugiau apie internetą, supažindindamas kaip jis veikia ir parodydamas, kad jis gali būti naudojamas daugybei tikslų. Tai gali būti veikla susijusi su vyriausybinėmis organizacijomis, informacijos paieška, prekių pirkimu ar bendravimu su šeima ir draugais. e-Citizen sertifikavimas sukurtas specialiai žmonėms su ribotomis žiniomis apie kompiuterius ir internetą. Programa prieinama visiems, nepriklausomai nuo šeimyninės padėties, išsilavinimo, supratimo ir gabumų, nors šiokios tokios žinios apie kompiuterius būtų naudingos prieš pradedant įsisavinti šią programą.

e-Citizen programa sukurta kaip įmanoma paprastai. Klausimyne yra užduotys suteikiančios praktinės interneto galimybių patirties. Programa susideda iš nepriklausomų mokymosi skyrių su mokomosiomis pagalbomis kiekvienai daliai.

Programa yra lanksti ir leidžia mokytis norimu tempu, bet paprastai reikia 30 mokymosi valandų. e-Citizen mokymosi pabaigoje yra nesudėtingas 45 minučių testas.

1.2.4. EqualSkills programa

EqualSkills yra laisva ir nesudėtinga įžanga apie kompiuterius ir internetą pradedantiesiems. Programa suteikia supratimą apie kompiuterius ir internetą, kad įgyti pasitikėjimo ir paskatinti kelti įgūdžius šioje srityje.

EqualSkills apima šias keturias sritis:

- Pagrindinės žinios apie kompiuterius (kompiuterių sandara, įjungimas, naudojimasis klaviatūra ir pelyte).
- Supažindinimas su darbalaukiu (darbalaukis, langai, dokumentų kūrimas, failų tipai).

- Internetas (WWW, interneto naršyklė, paieška).
- Elektroninis paštas (elektorinio pašto vartotojas, elektroninės žinutės).

Su EqualSkills gaunamas supratimas apie tai, ką galima padaryti kompiuteriu ir kokias užduotis galima atlikti naudojantis internetu. Baigęs programą kandidatas moka siųsti elektorinius laiškus, naudotis kai kuriomis paprastomis programomis ir naršyti internete, kad surastų informacijos apie naujienas, orus, hobius, t.t.

Programos mokymosi kursas trunka nuo 8 iki 15 valandų, priklausomai nuo besimokančiojo. Programa lanksti ir todėl leidžia mokytis norimu tempu. Nėra formalaus EqualSkills egzamino. Programa neskirta sertifikuotis, turint tikslą kažkur įsidarbinti, tačiau suteikia besimokančiajam pagrindines kompiuterių žinias ir atskleidžia technologijų vaidmenį kasdieniniame gyvenime. Baigus EqualSkills programą galima pereiti prie sudėtingesnių programų, gal net prie pilno ECDL sertifikavimo.

1.2.5. ECDL CAD programa

Visiems, kas naudojasi kompiuterinėmis technologijomis kuriant 2 matavimų objektus (CAD), svarbu turėti pagrindinius 2D CAD programinės įrangos naudojimosi įgūdžius ir pademonstruoti tuos įgūdžius darbdaviams arba būsimiems darbdaviams. ECDL Computer Aided Design (CAD) siūlo galimybę sertifikuoti pagrindinius 2D CAD įgūdžius tarptautiniu standartu.

ECDL CAD yra nepriklausomas tarptautinis pagrindinių 2D kompiuterinio dizaino įgūdžių standartas. Naujausia ECDL CAD klausimyno versija 1.5 atnaujino sertifikavimą iki dabartinių 2D CAD industrijos standartų. Tai leidžia ECDL fondui teikti išsamų ir sklandų, dabartį atitinkantį, 2D CAD pagrindinių įgūdžių sertifikavimą.

ECDL CAD skirtas studentams ir profesionalams, kurie siekia tarptautiniai pripažįstamo kvalifikacijos pripažinimo sertifikato, liudijančio CAD įgūdžius. Šis sertifikavimas duoda pagrindą tolimesnėms studijoms arba profesionaliam tobulėjimui su CAD susijusioje srityje. ECDL CAD sertifikatas rodo, kad jį išlaikę žmonės, turi įgūdžius ir žinias naudotis daugumos CAD aplikacijų standartine programine įranga ir savybėmis.

1.2.6. ECDL WebStarter programa

ECDL fondo sukurta ECDL WebStarter, yra nauja sertifikavimo programa skirta suteikti įgūdžius reikalingus modeliuoti, kurti ir prižiūrėti internetinę svetainę. Programa specialiai sukurta norintiems gauti įgūdžių kuriant ir prižiūrint internetines svetaines ir yra trumpesnė bei pigesnė, nei profesionalaus lygio Web dizaino programa.

ECDL WebStarter sertifikavimui reikia apie 20-30 valandų mokymo, po kurio seka 45 minučių paprastas testas. ECDL WebStarter sertifikatas liudija, kad kandidatas:

- Supranta pagrindines Web leidybos sąvokas
- Turi pagrindinius įgūdžius reikalingus sukurti internetinį puslapį
- Supranta esminius HTML principus
- Gali parašyti paprastą HTML programinį kodą
- Moka naudotis Web redaktorių kuriant internetinius puslapius, kurti formas ir lenteles, naudotis karkasais ir formuoti tekstą
- Gali dirbti su internetinių puslapių vaizdiniais objektais
- Gali publikuoti puslapį internete
- Turi gerą supratimą apie saugumo objektus ir įstatymus susijusius su Web leidyba.

ECDL WebStarter yra tinkamas produktas smulkiam verslui, kai reikia internetinio puslapio, bet nenorima skirti resursų finansuoti didelės apimties puslapius. Taip pat bendruomenėms, kurioms reikia bendrauti su savo nariais, naudojantis mažais resursais; studentams, norintiems dalintis informacija tarpusavyje; individams, norintiems turėti asmenines internetines svetaines.

1.2.7. ECDL ImageMaker programa

Atsiradus skaitmeniniams fotoaparatams, kompiuteriams, skaneriams, mobiliesiems telefonams su fotokameromis ir skaitmeninio vaizdo manipuliavimo programinei įrangai, visi dabar turi galimybę dirbti su skaitmeniniais vaizdais įvairiais tikslais. Galimybės neribotos – jei suprantate pagrindines skaitmeninių vaizdų idėjas ir turite įgūdžių manipuliuoti ir redaguoti juos. Iki šiol, norint įgyti tokius sugebėjimus, reikėjo įsisavinti profesionalias aukšto lygio programas.

ECDL ImageMaker sukurtas žmonėms, norintiems gauti įgūdžių dirbant su skaitmeniniais vaizdais, neskiriant pernelyg daug laiko ir išlaidų, kaip kad reikia profesionalaus lygio skaitmeninių vaizdų redagavimo sertifikavimui. ECDL fondo sukurtas ECDL ImageMaker yra naujas sertifikavimas,

skirtas suteikti žinias, reikalingas naudotis ir manipuliuoti skaitmeniniais vaizdais. Programa suteikia praktinių įgūdžių tam, kad gauti maksimalią naudą iš skaitmeninių vaizdų. ECDL ImageMaker tinkamas sertifikavimas studentams, smulkiam verslui, bendruomenėms ir individualiems namų vartotojams.

ECDL ImageMaker sertifikavimui reikia apie 20-30 valandų mokymo, po kurio seka 45 minučių trukmės testas.

1.2.8. ECDL CTP programa

Sertifikuotas mokymo profesionalas (Certified Training Professional - CTP) yra tarptautinė ICT mokymo kvalifikacija. Nepaisant griežtų tarptautinių ECDL administravimo standartų, iki CTP sukūrimo grupinio ir individualaus mokymo organizacijos buvo mažai kontroliuojamos. Kaip vienas iš fondo ne galutinių vartotojų sertifikavimų, CTP suteikia mokytojams ir mokymo organizacijoms objektyvų kokybės standartą, kuris atsispindės jų pačių mokymo paslaugose.

Programa sukurta siekiant tenkinti profesionalaus IT mokymo poreikius. Sertifikavimas yra nepriklausomas nuo prieš tai įgytos kvalifikacijos ir kiekvienas CTP kandidatas turi pademonstruoti savo kompetenciją.

Norint tapti sertifikuotais mokymo profesionalais, individualiems mokytojams nereikia sėdėti ir laikyti egzaminų. Reikia pateikti įrodymus, kad jie atitinka programos žinių reikalavimus. Įrodymai klasifikuojami kaip:

- Dokumentiniai įrodymai: mokymo planai, sesijų tvarkaraščiai, analitinės formos, vertinimo formos, t.t.
- Darbų įrodymai: mokymų vaizdo medžiaga, pagrindinių žinių įvertinimas, apimantis komunikavimą, instrukcijas, klausimus ir atsakymus.

Darbų įrodymai yra būtini programai, nes nėra kitos alternatyvos įsitikinti mokytojo aktyvumu mokyme. Sertifikuoto mokymo profesionalo programos tikslai:

- Naudoti gerąją praktiką ICT mokyme.
- Pripažinti ir sertifikuoti gerąją praktiką individualiems mokytojams.
- Suteikti mokytojams galimybę kelti kompetenciją.
- Suteikti mokymo organizacijoms objektyvų ir pripažintą ICT mokymo lygio ženklą.
- Sukurti sertifikuotų mokytojų bendruomenę, kuri padėtų individualiems mokytojams.

1.2.9. EUCIP programa

EUCIP (European Certification of Informatics Professionals), Europos informatikos profesionalo sertifikatas yra profesionalaus sertifikavimo ir kompetencijos vystymo schema skirta IT specialistams ir paskutinio kurso studentams.

Daugeliui žmonių, dirbančių su informacijos komunikavimo technologijų pramonėje, nelengva patenkinti ambicijas ir progresuoti iš bazinės kvalifikacijos į pilnai profesionalią sertifikaciją. EUCIP suteikia netradicinį kelią tokiems specialistams į pilną profesionalo pripažinimą. Žmonės, dirbantys kitose specializuotose srityse, turi skubų informacijos komunikavimo technologijų įgūdžių poreikį suprasti ir valdyti informacijos komunikavimo technologijų projektus savo organizacijose.

EUCIP, kaip ir ECDL, sukurtas CEPIS (Council of European Professional Informatics Professionals), t.y. Europos informatikų profesionalų tarybos. Programos objektas yra informacijos komunikavimo technologijų, vidurinio lygio kompetencija, užtikrinanti bendruosius pramonės, valdymo ir viešųjų organizacijų standartus.

1.2.10. ECDL Health programa

ECDL Health yra galutinio vartotojo kvalifikacija sveikatos informatikos sistemų vartotojams, įskaitant gydytojus, seseles ir kitus sveikatos profesionalus, palaikančius sistemas, naudojančias pacientų duomenis. Programa orientuojama į pripažinimą ir poreikį visose šalyse, kurios naudoja sveikatos informacijos sistemas ir įgalina nacionalines sveikatos sistemas tapti efektyvesnėmis bei našesnėmis.

ECDL Health klausimynas buvo sukurtas tarptautinės ECDL fondo ekspertų grupės ir patvirtintas vienu metu trijose šalyse: Italijoje, Didžiojoje Britanijoje ir JAV.

ECDL Health pripažįsta, kad nacionaliniai reikalavimai, įskaitant praktikos būdus, kultūrą, kalbą ir įstatymų rėmus, skiriasi priklausomai nuo šalies, todėl specifiniai sertifikavimai buvo sukurti kartu su sveikatos informatikos ekspertais Italijoje, Didžiojoje Britanijoje, JAV ir Suomijoje. Sertifikavimo įrankiai, kuriuos sukūrė šios šalys, duoda platesnę naudą ir gali būti naudojami kitose šalyse.

1.3. ECDL fondo patvirtintos partnerinės programos (Endorsed Programmes)

Iki šiol ECDL fondas kūrė ir leido programas tik savo iniciatyva, tačiau nuo 2008 metų fondas pakeitė požiūrį, nusprendė, kad iniciatyva turi būti iš žemesnių lygių ir atskiroms šalims, t.y. partneriams, suteikė galimybes, kurti savo programas. ECDL fondo partneriai skirtingose šalyse, atsižvelgdami į savo šalies ar naujai atsiradusius globalius poreikius, gali pasiūlyti fondui naują sertifikavimo programą.

Patvirtinti produktai yra lokaliai kuriamos sertifikavimo programos, kurios tvirtai laikosi aukštų turinio ir veiklos administravimo standartų. Tvirtas šių standartų laikymasis leidžia kūrėjui naudoti "Endorsed by ECDL Foundation" logotipą prie savo produkto. Nors patvirtinti produktai nėra ECDL fondo nuosavybė, tačiau struktūra ir palaikymo metodai patvirtinami pagal ECDL fondo produktų patvirtinimo kokybės užtikrinimo standartus [35]. Šiuo metu ECDL fondo patvirtinti produktai yra naudojami tik tose šalyse, kurios juos sukūrė.

Norint gauti ECDL fondo leidimą sukurti ir paleisti naują patvirtintą partnerinę sertifikavimo programą, reikia atlikti standartizuotas procedūras, kurios plačiai aprašomos šio darbo 2 dalyje. ECDL standarto laikymąsi ir ECDL sklaidos darbus stebi ir koordinuoja ECDL fondas. ECDL standartą sudaro:

- ECDL programa – detalus standarto apimamų žinių sričių ir įgūdžių aprašas;
- Europos klausimų ir testų bazė (European Question and Test Base – EQTB), kurioje saugomi klausimai ir testai, naudojami vertinimo metu
- ECDL vertinimo metodiniai nurodymai

ECDL standartui palaikyti kiekvienoje šalyje turi būti organizacija, kurią ECDL fondas paskiria atsakinga už tai, kad visi testai atitiktų ECDL programą. Skirtingose šalyse naudojamos mokymo ir egzaminavimo procedūros gali skirtis, tačiau ECDL fondas reikalauja, kad visuose patvirtintuose testavimo centruose būtų naudojamas teisingas ir gerai apibrėžtas egzaminavimo procesas kartu su patikimai veikiančiu testavimo procesu. ECDL pažymėjimo įteikimo proceso auditą atlieka ECDL fondas.

ECDL pagrindu yra ECDL programa anglų kalba. Ši programa apibrėžia pažymėjimui reikalingas žinių sritis ir praktinius įgūdžius. Įvairiose šalyse standartiniai testai lokalizuojami, tačiau naudojama ta pati programa, todėl išlaikomas toks pats žinių ir įgūdžių lygis. Lokalizuotos Europos klausimų ir testų bazės auditą atlieka ir ją registruoja ECDL fondas.

ECDL sklaidos programa skiriasi nuo daugumos nacionalinių ir tarptautinių švietimo programų, nes ji remiasi standartiniais testais ar egzaminais, o ne standartizuotu mokymu. ECDL visada patvirtina tą patį žinių ir įgūdžių lygio standartą, nepriklausomai nuo asmenų tautybės, išsilavinimo, amžiaus ar lyties. Vienoje šalyje išduotas ECDL pažymėjimas galioja ir kitose šalyse.

1.3.1. GIS programa

AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) Italijos licenzijos turėtojas [26], kartu su asociacija LABSITA, neseniai išleido ECDL fondo patvirtintą produktą pavadinimu GIS (Geographic Information System) – geografinę informacinę sistemą. GIS sertifikuoja profesionalus, kurie įrodo savo įgūdžius šiose srityse:

- Pagrindinės GIS naudojamos IT idėjos
- Geografinės informacinės sistemos komponentai
- Geodezijos ir topologijos GIS
- Skaitmeninė kartografija
- GIS analizavimo ir pristatymo technologijos

Šie įgūdžiai testuojami parinktais klausimais ir praktiniais testais, pritaikomais daugumos GIS programinės įrangos.

Sertifikavimas skirtas profesionalams, kurie nori parodyti savo GIS įgūdžius, įgydami pripažintą kvalifikaciją. Jis specialiai skirtas:

- Tiems, kurie nori turėti oficialiai pripažintą nacionalinį (ir tarptautinį) GIS įgūdžių sertifikatą.
- Mokykloms ir studijų programoms, kurios nori teikti papildomą profesionalią ir techninę įgūdžių ir pripažintą profesionalią kvalifikaciją, tam, kad padėtų ieškantiems darbo.
- Viešiesiems organams ir agentūroms, kurios reikalauja objektyvios bazinių ir praktinių žinių savo darbuotojų sertifikacijos.
- Privačioms kompanijoms, dirbančioms nuo GIS sektorių iki IT tinklų, kurios planuoja įdarbinti žmones, turinčius objektyvias žinias. GIS sertifikacija turi tris pagrindinius modulius, kuriuos reikia pabaigti norint gauti GIS sertifikatą.

Trys GIS sertifikavimo moduliai:

- Kartografija (1 modulis)
- GIS sistemos (2 modulis)

- GIS programinės įrangos naudojimas (3 modulis)

1.3.2. ECDL 3D CAD programa

AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) - Italijos licenzijos turėtojas [26], neseniai išleido ECDL fondo patvirtintą produktą pavadinimu 3D CAD. Sertifikavimas sukurtas sertifikuoti žmones, kurie įgijo 3D CAD kvalifikaciją, pademonstravę, kad turi standartinių 3D CAD aplikacijų savybių naudojimo žinias.

3D CAD sertifikuoja profesionalus, kurie įrodo savo įgūdžius šiose srityse:

- Bazinis 3D erdvės modeliavimas
- Pažangesnio lygio architektūros ir mechanikos 3D modeliavimas
- Vaizdavimo technologija ir koncepcija

Šie įgūdžiai testuojami praktiniais testais, taikomais daugumoje architektūros ir mechanikos 3D CAD programinėje įrangoje.

3D CAD sertifikavimas nepriklausomas nuo produkto ir apima daug skirtingų tipų 3D CAD/CAM programinės įrangos paketų. Nepriklausomumas nuo produkto yra reikalavimas, kurį turi atitikti ECDL fondo patvirtintas produktas.

Pagal patvirtintą klausimyną buvo sukurti dviejų tipų testai, tinkami specifiniams architektų ir mechanikų reikalavimams. Visos 3D CAD versijos turi po 20 klausimų. Testo objektas yra sukurti realų architektūrinio ir mechaninio modeliavimo modelį nuo pradžių iki reprezentacinio vaizdavimo.

1.3.3. E-KIDS programa

Kroatijos licenzijos turėtojas, Kroatijos kompiuterinė bendruomenė (CITS - Croatian Computer Society) [27], Kroatijos rinkoje išleido e-Kids kaip ECDL fondo patvirtintą produktą. E-Kids produktas yra reikalingas žingsnis diegiant kompiuterinį raštingumą vaikams ir jis susideda iš trijų pagrindinių komponentų:

- Multimedijos kompaktinis diskas (iki mokyklinio amžiaus vaikams)
- E-Kids paketas
- E-Kids žurnalas (mėnesinis)

Šis žingsnis ugdo kompiuterinį raštingumą ankstyvame amžiuje, tam, kad suteikti galimybę vaikams išmokti efektyviai naudotis informacinių komunikacijų technologijomis bet kokioje

gyvenimiškoje situacijoje: mokykloje, namuose, linksmybėms ir daug kitų tikslų. Tai daug daugiau nei kompiuterinių žaidimų žaidimas ar bendravimas mobiliųjų telefonų trumposiomis SMS žinutėmis. E-Kids paketą sudaro vadovėlis (parašytas kaip animacinis filmas ir iliustruotas keliais animaciniais herojais), kompaktinis diskas su dviem žaidimais (kurie interaktyviai moko informacinių komunikacijų technologijų) ir sertifikuota programa (kuri tikrina vaiko žinias).

Mokytojui reikia pasirašyti įgūdžių kortelę, kuri liudija, jog vaikas testą atliko pats, be jokios pagalbos. Mokytojas siunčia pasirašytas korteles CITS bendruomenei, kurie atspausdina sertifikatą ir/arba ID kortelę. Vaikai gali naudotis ID kortelėmis kaip savo kompiuterinio raštingumo patvirtinimais.

1.3.4. E-Learner programa

e-Learner yra ECDL fondo patvirtintas produktas Pietų Afrikoje, kuris aprūpina jaunesnius studentus solidžiu pagrindu keliant ECDL / ICDL kvalifikaciją. Tai sertifikuotas, modulinis progresyvių ICT įgūdžių kursas, panaudojantis Computers 4 Kids kurso medžiagą. Naudodamas unikalų ir integruotą požiūrį, e-Learner teikia galimybę gauti esminius ICT įgūdžius septyniuose dalyse.

E-Learner kursas yra sudarytas iš dalių ir yra dviejų skirtingų lygių (Silver ir Gold). Silver kursas susideda iš 5 dalių ir apima bazinio lygio įgūdžius. Gold kursas apima visas 7 dalis ir įgūdžius, kurie šiose dalyje jau yra aukštesnio lygio. e-Learner dalys lygiuojamos į tas, kurias kandidatui reikėtų turėti ECDL Core kurse, tokiu būdu jos yra kaip įvadas (Silver) ir progresyvus žingsnis (Gold) į ECDL Core. e-Learner kurso dalys yra šios:

1. IT pagrindai
2. Failai ir katalogai
3. Piešimas
4. Teksto redagavimas
5. Skaičiuoklės
6. Pateiktys
7. Naršymas internete ir elektroninis paštas

Kai reikalaujami įgūdžiai pasiekti visose dalyse (nesvarbu ar Silver ar Gold kurse), užpildyta įgūdžių įrašų kortelė, kartu su e-Learner administracinės sistemos kopija, perduodama į pagrindinį ofisą.

Po patvirtinimo, pripažinti sertifikatai išduodami kiekvienam mokiniui, kuris išpildė reikalavimus Silver arba Gold kursuose.

1.3.5. e-Guardian programa

Lietuvos ECDL sklaidos darbus koordinuoja Lietuvos kompiuterininkų sąjunga ir jos Kaune įkurta viešoji įstaiga "Informacinių technologijų institutas" (ITI). Ši viešoji įstaiga nuo 2000 metų sausio mėnesio yra oficiali ECDL fondo atstovybė Lietuvoje. 2007 metų gale ITI vadovo ir šio magistrinio darbo autoriaus iniciatyva gimė mintis sukurti naują sertifikavimo programą, pavadinimu e-Guardian, skirtą patvirtinti žinias apie vaikų apsaugojimą internete. e-Guardian programos vieta ECDL fondo produktų portfelyje pavaizduota 2 paveiksle.

Šaltinis: sudaryta autoriaus.

Pav. 2 e-Guardian programos vieta ECDL fondo produktų portfelyje

Iki šiol nebuvo spręsta problema, ar kompiuterinėmis sistemomis ir internetu besinaudojantys, su vaikais dirbantys asmenys žino ir moka tinkamai apsaugoti duomenis, kompiuterinę programinę ir aparatūrinę įrangą, bei vaikus naudojančius minėtas kompiuterines sistemas. Todėl būtų labai naudinga sukurti naują sertifikavimo programą, kurios atsiradimas leistų su vaikais dirbančių organizacijų atstovams ir norintiems tėvams patvirtinti savo žinias jas liudijančio sertifikato išlaikymu. Tokio pobūdžio sertifikavimas ECDL / ICDL organizacijoje nebuvo sukurtas. Apie kitų pasaulinių sertifikavimo organizacijų sukurtas tokios klasės sertifikavimo programas (susijusias su saugiu darbu kompiuteriu ir vaikų apsauga) informacijos nerasta. Šio darbo objektas - vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programa. Iškeltas tikslas - anglų kalba sukurti vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programą e-Guardian, turint tikslą ją patvirtinti ECDL fonde.

2008 metų balandžio mėnesį buvo sukurtas e-Guardian programos turinys ir pagal ECDL fondo reikalavimus suformuotas klausimynas. Šis klausimynas, kartu su partnerinės programos standartų patvirtinimo paraiškos forma pateiktas ECDL fondui. Gavus klausimyno patvirtinimą 2008 metų gale pagal šį klausimyną buvo sudaryta e-Guardian testo klausimų bazė, skirta automatizuotam testavimui. Sudaryta testo klausimų bazė pateikta ECDL fondo ekspertams, vėliau pagal jų pastabas pakoreguota ir patalpinta į ECDL Lietuva testavimo sistemą bandomajam testavimui. Šiuo metu sertifikavimo sistema yra pilotinio testavimo stadijoje. ECDL fondo ekspertų pageidavimu, pilotiniai testai yra vykdomi keliose Europos šalyse (Lietuva, Latvija, Bulgarija).

e-Guardian sertifikavimo testas susideda iš 5 dalių:

- Bendros saugumo užtikrinimo priemonės
- Kenkėjiškos programos (*malware*)
- Elektroninis bendravimas
- Saugus naršymas ir atsiskaitymai internete
- Vaikų saugumas

Sertifikato išlaikymui reikia teisingai atsakyti į bent 80% iš 30 pateikiamų klausimų, kurie pagal specialų atsitiktinio parinkimo algoritmą atrenkami iš automatizuoto testavimo klausimų bazės (AQTB). Klausimų bazėje klausimai iš visų penkių minėtų dalių.

Išlaikęs testą kandidatas gautų sertifikatą liudijantį, kad jis žino ir moka tinkamai apsaugoti duomenis, kompiuterinę programinę ir aparatūrinę įrangą bei vaikus, naudojančius kompiuterines (ypač bendravimui internete skirtas) sistemas.

2. ECDL PATVIRTINTŲ PARTNERINIŲ PRODUKTŲ KŪRIMO METODAI

Šiame skyriuje aprašomi metodai, kurie buvo naudojami magistrinio darbo tyrimams atlikti. Pirmasis metodas naudojamas gauti kuriamos sertifikavimo programos ECDL fondo patvirtinimą. Tai yra griežtai formalizuota procedūra, naudojanti specialias standartizuotas formas. Kitas metodas skirtas kuriamos sertifikavimo programos klausimynui sudaryti. Šioje dalyje taip pat aprašomi sertifikavimo produkto testo klausimų bazės klausimų sudarymo ir koregavimo metodai.

2.1. Produkto patvirtinimo standartai

Šiame skyriuje pateikiamas naujos sertifikavimo programos patvirtinimo pagal ECDL fondo standartus metodas. Atitikimas standartams, turi būti išreikštas specialia forma, taikomas visiems esamiems produktams ir visiems ECDL fondo patvirtinimo siekiantiems produktams [34]. Standartai grupuojami į tris kategorijas:

- Klausimyno standartai, kurie nustato sertifikacijos įgūdžių/žinių srities specifikacijas.
- Vertinimo standartai, kurie nustato pagrindines technologijas, skirtas priimti sprendimui apie kandidato sertifikavimą.
- Veikimo standartai, kurie yra kaip administravimo taisyklės ir turi užtikrinti sertifikacijos operacijų aukštą kokybę.

ECDL licenzijos turėtojas, siekiantis standartizavimo ir norintis gauti produkto patvirtinimą turi užpildyti formą, kuri detaliai aprašoma šiame skyriuje. Ar produktas atitinka visus formos standartus ir gali tapti standartizuotas, sprendžia ECDL fondas. Kadangi standartizavimo siekia skirtingų tipų produktai, todėl standartai pateikiami bendrai visiems tipams. Nepaisant to, standartai aiškiai nustato, kad sertifikacija turi turėti savo pagrindinius unikalius atributus, kad būtų pripažinta jų aukšta kokybė [10]. Prie kai kurių standartų pateikiami pavyzdžiai, iliustruojantys, kaip gali būti parodytas atitikimas. Pavyzdžiai pateikti anglų kalba, nes pati paraiškos forma pildoma būtent šia kalba.

Pagrindinis magistrinio darbo naujumas yra tai, kad produkto patvirtinimo standartai sudaryti rankinio testavimo atvejui ir juose nagrinėjamas MQTB sudarymas. e-Guardian programa yra pirmoji ECDL fondo patvirtintos partnerinės programos statuso siekianti programa, naudojanti testavimo

sistemą ir AQTB. Magistrinio darbo metu nebuvo galima aklai sekti ECDL fondo kokybės valdymo sistemos standartais, bet reikėjo taikyti juos kūrybiškai, derinant su ECDL fondo ekspertais.

2.1.1. Klausimynas

Esminiai sertifikacijos tikslai. Paraiškos formos pirmajame skyriuje pateikiami esminiai sertifikacijos tikslai, kurie apibūdina svarbiausius sertifikacijos įgūdžius ir žinias. Šiame skyriuje žinios ir įgūdžiai reikalingi kandidatui, pateikiami pagal panaudojimo sritis. Pateikiami bendrųjų reikalavimų sertifikavimo tikslai ir detalesni įgūdžių bei žinių srities reikalavimai.

Atitikimo reikalavimams pavyzdys:

The candidate should understand **Common means for safety assurance:**

The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas **Malicious software:**

The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas of **Securable web browsing and paying on internet:**

The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas **Children safety:**

Mokymosi medžiagos turinys. Mokymuisi reikalingi rezultatai turi būti aiškiai apibrėžti, kad kandidatas galėtų vienareikšmiškai nustatyti įgūdžių ir žinių sritis, kuriose atliekamas sertifikavimas [9].

Atitikimo reikalavimams pavyzdys:

Common means for safety assurance:

- Know how to follow, download and use updates for your operating system, additional software and security components. Understand the benefits of these updates.
- Know multiple user account. Understand what a personal user account is and how information of different users is separated.
- Understand the purpose of a user name, and the difference between user name and user password. Understand the meaning and importance of access rights.
- Know the necessity of login to system password, and that the usage of login passwords
- Be able to make complex password. Know the structure of a complex password and the rules for changing and keeping passwords.
- Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Defender, etc.).
- Be able to protect data on computer disk. Know about data encryption and password protection.

- Know how to find out whether a data media has a password protection possibility, used for protecting against unwanted data access. Be able to use these passwords for protection. Be able to protect CD, DVD, USB memory and other external data media.
- Understand the threat of malicious data spread in external data medias.
- Understand the benefits and purpose of data and software backups.
- Know who you should contact if you discovered or suspect that data can be classified as illegal or dangerous

Malicious software:

- Understand different malicious software (viruses, Trojan horses, spyware, dishonest adware, etc.) definitions and differences.
- Know when and how malicious software can get into computer system.
- Know what security software used to protect against malware.
- Be able to configure software to automatic and regular update
- Know what has to be done and it what order, if you suspect that computer system is infected. Understand the limitation of security software.
- Understand that an active version of security software should be running when downloading files or opening email attachments.
- Know that unknown and unwanted emails and their attachments should not be opened.
- Understand what is unsafe data media. Understand that unsafe CD, DVD, USB memory media should not be used
- Electronic messages:
- Know about email that is classified as spam, and email messages infected with malware.
- Be aware of privacy protection legal act
- Know how to redirect children email first to your account
- Know how to reject email from specific email addresses
- Know how to block private messages between a child and another user
- Know how to threat email messages from unknown senders.
- Know how to threat securable with instant messaging.
- Be aware of mobile phone capabilities
- Know who to contact if you discovered or suspect dangerous or illegal content

Securable web browsing and paying on internet:

- Know about tools that ensure safety when browsing the internet (blocking of cookies, ActiveX control, etc.).

- Know about advantages, disadvantages and dangers of internet cookies.
- Know about threats associated with the personal data disclosure
- Know about gaps and threats, such as possibilities for evel-minders to use or steal client information.
- Know about encryption keys used on internet, know about types of encryption keys and how to use them.
- Be able to distinguish safe/genuine online transaction/commerce sites from unsafe.
- Be able to perform online transaction using credit or debit cards.
- Know how to contact service administrator while required
- Know who to contact if you discovered or suspect dangerous or illegal content

Children safety:

- Understand that open communications between parent and children is important to keeping children safe.
- Know about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet.
- Know about system monitoring types and be able to monitor use of computer.
- Be able to access temporary internet files and browser history
- Be able to use software to control children use of internet, operating system and software.
- Know about children protection software.
- Be able to use internet content filtering tools integrated on web browsers.
- Know what defensive software is.
- Know what a quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use it.
- Be able to access the chat, instant messenger history
- Be able to contact service administrator
- Know about recommended kid directories, search sites geared for children and targeted at teenagers.
- Know who to contact if you discovered or suspect dangerous or illegal content

Tinkamų ekspertų patikrinimas. Mokymosi medžiaga turi būti kuriama naudojant formalius procesus, patikrintus tinkamų tos srities ekspertų. Turi būti pateikti klausimyno kūrimo žingsniai ir srities ekspertų informacija. Turi būti pastebėta, kad klausimynas bus tikrinamas ECDL fondo

reikalingų sričių ekspertų. Ši sritis sudaroma techniškai tiksliai ir pagal klausimyną, ryšium su apibrėžtais programos tikslais [8].

Atitikimo reikalavimams pavyzdys:

Please provide details of the relevant subject matter expertise:

Dr. Alfredas Otas, Chairman of the Lithuanian Computer Society; Chair of IT Expert Group at Ministry of

S Science and Education, Lithuania

Piotr Mrozinski, Regional Development Executive, ECDL Foundation

Dr. Marek Milosz, CEO of ECDL–Poland, Head of Division at Lublin University of Technology, Poland

Vaino Brazdeikis, Director of the Centre of Information Technologies of Education, Lithuania

Tomas Lygutas, Doctoral student, Institute of Informatics, Lithuania (Internet security)

Mantas Lukosevicius, Security administrator, Company Sekasoft, Lithuania

- Advice is sought at key points from teachers, significant individuals and organisations. In particular, professional teacher associations play an important role.
- A project manager employed by the Office of the Board of Studies manages the syllabus development project, developing the initial proposal, establishing consultative networks, managing consultation, and drafting and revising syllabus documentation.
- Project teams will, at various stages of the syllabus development process, include curriculum, assessment and publications officers.
- Contracted writers are, at times, also included in the project teams. The Expert Group maintains a register of writers. To be considered for appointment as writers, teachers from all syllabus areas with demonstrated writing expertise can submit an expression of interest to the Expert Group.

Klausimyno koregavimo metodai. Klausimyno priežiūrai ir koregavimui turi būti sukurtas ir dokumentuotas specialus metodas. Klausimyno koregavimas užtikrina, kad klausimynas atitinka dabartines žinias, sukurtas pagal technologinius pažangumus ir naujoves, reikalavimus kandidatui, kurie bus tinkami tuo metu kai produktas bus išleistas [7]. Rekomendacijos koregavimams turi būti gautos iš testuotojų ir iš kandidatų atsiliepimų, taip, kad sričių ekspertai į juos atsižvelgtų prieš produkto išleidimą.

Atitikimo reikalavimams pavyzdys:

Please provide details of a process for syllabus review and upgrade:

Phase 1 Syllabus (SYL) review

Purpose

A review of the existing syllabus provision and a plan for the revision or development of the syllabus.

Following consideration of relevant data the Licensee determines whether a review of existing syllabus provision will be conducted.

The review phase will typically involve

• establishment of a Expert Group to monitor the syllabus development process and provide advice throughout the project

• establishment of the project plan which includes consultation and a timeline

• informing Licensees and Test Centres of the project plan including the timeline for consultation

• evaluation of the existing syllabus against the syllabus criteria approved by the Licensee

• consultation with teachers and key groups regarding the existing syllabus and the general directions for the syllabus development

• research, including a review of literature and practice in Europe and overseas

• recommendation to the Expert Group of the broad directions for syllabus revision or development in response to the review findings to the Expert Group

• Expert Group endorsement of broad directions for syllabus revision or development

Outcomes

• endorsement by the Expert Group of the broad directions for syllabus revision or development

• information provided to the third parties

Phase 2: Writing brief development

Purpose

The development of a writing brief for the draft syllabus that takes account of the Expert Group directions established during the syllabus review phase.

This phase will typically involve

• preparation of a draft writing brief by a project team, taking into account information from consultation and research undertaken during the previous phase

• widespread consultation on the draft writing brief, involving:

- teachers

- key groups, including professional associations and school systems

- other relevant third partie committees

• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response

to those issues

• modification of the draft writing brief in response to consultation feedback

• consideration of the amended draft writing brief for the Expert Group with recommendation

• submission of the draft writing brief, consultation report and Licensee recommendation to the ECDL Foundation for endorsement

• Internet publication of the consultation report and endorsed writing brief.

Outcome

A writing brief which provides the detailed blueprint for the development of the syllabus, against which the final syllabus is judged.

Phase 3: Syllabus development

Purpose

The development of the syllabus package as defined by the project plan.

This phase will typically involve

• preparation of a draft syllabus package, by a project team, according to the endorsed writing brief

• distribution of a draft syllabus package for consultation (via the Internet) to:

- teachers

- key groups, including professional associations and school systems

- the Expert Group

- other relevant third parties committees

• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response

to those issues

• preparation of a report that describes the extent to which board criteria for approval of syllabuses have been met

• modification of the draft syllabus package in response to consultation feedback

• consideration of the amended draft syllabus package by the expert group for recommendation to the ECDL-F

• submission of the draft syllabus package, consultation report and expert group recommendation to

the ECDL-F for endorsement

• submission of the syllabus to the ECDL-F for approval

• Internet publication of the consultation report

• editing, design, layout and printing of the approved syllabus package

• briefing of school authorities to effect handover of syllabus package for implementation in schools

• distribution of the syllabus package to schools.

Outcomes

• A syllabus approved by the ECDL-F

• Publication and distribution of the syllabus package.

Phase 4: Implementation

Purpose

Implementation of the syllabus is conducted by the Test Centres and other Licensee. The LIKS role is the on-going collection of

data on the use of the syllabus to ascertain whether the intentions of the syllabus are being achieved.

This phase will typically involve

• collection, collation and analysis of data on the use of the syllabus

• routine reports to the Board and ECDL-F

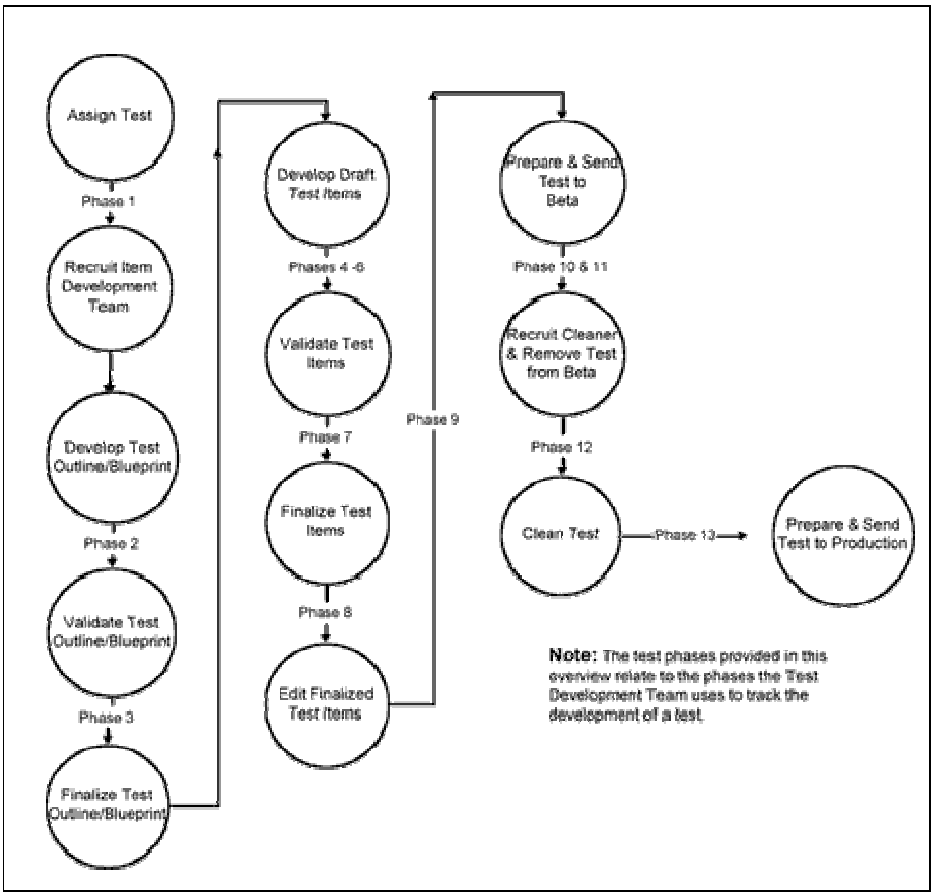
• identification and recording of issues that need to be taken into account in subsequent syllabus revision.

Outcome

Data on the use of the syllabus that can be used to inform a future syllabus review.

2.1.2. Vertinimas

Vertinimas. Vertinimas turi atitikti testavimo vertinimo teoriją (IRT – Item Response Theory). Turi būti tikslus vertinimo siūlymo paaiškinimas ir vertinimo metodo aprašymas. Vertinimas turi būti pateiktas formaliai. Atitikimo reikalavimams pavyzdys pateikiamas 3 paveiksle:



Šaltinis: ECDL (2009) [žiūrėta 2009 01 06]. Prieiga per internetą: <http://www.ecdl.org.ro/en/certificari_ecdl.php?id=26>

Pav. 3 Vertinimo moksliniu pagrindu atitikimas reikalavimams

Detali vertinimo specifikacija. Šiame magistriniame darbe vertinimo specifikaciją siūloma papildyti dviem punktais:

- Vertinimo formatas (rankinis arba automatizuotas)
- Klausimų formatas (pasirinkimas iš kelių galimų atvejų, spragtelėjimas grafiniame vaizde, imitavimas ar realios programos fragmento vykdymas)

Įvertinus siūlomus pakeitimus vertinimo specifikaciją turi sudaryti šios dalys:

- Klausimų skaičius
- Vertinimo formatas (rankinis arba automatizuotas)
- Klausimų formatas (pasirinkimas iš kelių galimų atvejų, spragtelėjimas grafiniame vaizde, imitavimas ar realios programos fragmento vykdymas)

- Laiko specifikacija (testams su laiko limitais, reikia atlikti tyrimą, kad nustatyti tinkamas ribas)
- Išlaikymo balas (naudojamos balų interpretavimo procedūros, reikia dokumentuoti)
- Testų administravimo procedūros – testų administracijai turi būti duoti nurodymai. Testų administravimo procedūrų dalis turi būti irgi pritaikyta automatizuoto testavimo atvejui.

Aukščiau minėti pakeitimai yra formuluojami kaip siūlymas ECDL fondui modifikuoti produktų patvirtinimo standartus automatizuoto testavimo atvejui.

Vertinimo kokybės stebėjimo procesai. Turi būti sukurti tokie vertinimo kokybės ir vertinimo koregavimo procesai, kurie užtikrintų tolimesnį validumą ir aktualumą. Procesai turi turėti valdymo ir atsakomųjų veiksmų iš tarpininkų, susijusių su sertifikacija, elementus, o taip pat ir formalų techninių sertifikavimo aspektų aprašymą.

Atitikimo reikalavimams pavyzdys:

Please provide a detailed process for reviewing and revising the assessment:

Phase 1 Existing MQTB review

Purpose

A review of the existing MQTB provision and a plan for the revision or development of the MQTB.

Following consideration of relevant data the Licensee determines whether a review of existing MQTB provision will be conducted. The review phase will typically involve

• establishment of Item review/development team

• establishment of the project plan which includes consultation and a timeline

• informing Licensees and Test Centres of the project plan including the timeline for consultation

• research, including a review of literature and practice in Europe and overseas

• Expert Group endorsement of broad directions for MQTB revision or development

Outcomes

• endorsement by the Expert Group of the broad directions for MQTB revision or development

• information provided to the third parties

Phase 2: MQTB blueprint development

Purpose

The development of a MQTB blueprint that takes account of the Expert Group directions established during the MQTB review phase.

This phase will typically involve

• preparation of a draft writing brief by a project team, taking into account information from consultation and research undertaken during the previous phase

• widespread consultation on the draft writing brief, involving:

- teachers
- key groups, including professional associations and school systems
- other relevant third partie committees

• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response to those issues

• modification of the draft writing brief in response to consultation feedback

• **Outcome**

A writing brief which provides the detailed blueprint for the development of the MQTB, against which the final MQTB is judged.

Phase 3: MQTB development and Validation

Purpose

The development of the MQTB as defined by the project plan.

This phase will typically involve

• preparation of a draft MQTB, by a project team, according to the blueprint

• distribution of a draft MQTB for consultation (via the Internet) to:

- teachers
- key groups, including professional associations and school systems
- the Expert Group
- other relevant third parties committees

• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response

to those issues

• modification of the syllabus package in response to consultation feedback

• consideration of the MQTB amended draft group for recommendation to

the ECDL-F

• submission of the MQTB, consultation report and expert group recommendation to the Expert Group for endorsement

• submission of the MQTB

• Internet publication of the consultation report

• editing, design, layout and printing of the approved MQTB

• briefing of school authorities to effect handover of MQTB package for implementation in TC

• distribution of the MQTB to Licensees and TC

Outcomes

• A MQTB approved by the Expert Group

• Publication and distribution of the MQTB

Phase 4: Implementation

Purpose

Implementation of the MQTB is conducted by the Test Centres and other Licensees.

This phase will typically involve

• collection, collation and analysis of data on the use of the syllabus and MQTB

• identification and recording of issues that need to be taken into account in subsequent MQTB revision.

Outcome

Data on the use of the MQTB that can be used to inform a future MQTB review.

2.1.3. Administravimas

Turi būti aiškiai dokumentuota sistema, užtikrinanti efektyvias ir teisėtas sertifikavimo sistemos operacijas. Pagrindinės sistemos funkcijos yra vientisumo palaikymas ir darbo organizavimas, vertinimo vientisumo palaikymas, efektyvių operacijų užtikrinimas.

Administravimo sistema turi būti sukurta taip, kad joje būtų saugoma visa pagrindinė, su sertifikavimu susijusi, informacija. Ši sistema privalo saugoti pagrindinę informaciją apie kandidatų registraciją, vertinimo rezultatus ir sertifikatus. Sistemos duomenys turėtų būti laikomi saugiai ir atitikti visus atitinkamus duomenų apsaugos reikalavimus.

Atitikimo reikalavimams pavyzdys:

Please describe the administration system that will support this endorsed product.

The same administration system will be used as for support of other ECDL Foundation products in Lithuania. The administration system is in full compliance with the QA Standards.

Jei į patvirtinto produkto operacijas yra įtraukti partneriai, turi būti aiškiai, naudojant formalius palaikymo procesų aprašymus, apibrėžti partnerių patvirtinimo reikalavimai. Jei į patvirtinamo produkto ruošimą įtrauktos kitos organizacijos, tai toms organizacijoms turi būti paruošti aiškūs reikalavimai, kuriuos jos turės atitikti. Jei partneris bus įtraukiamas į produkto vertinimo diegimą, turi būti pateikti aiškūs reikalavimai, susiję su organizacijos, įrangos ir personalo tinkamumu. Paprastai partneriai būna testavimo centrai, kurso medžiagos leidėjai, arba ATES tiekėjai.

Vykdomų veiklos procesų patvirtinimui įvertinti reikalingas formalus procesas. Formalus procesas reikalingas ir veiklos aprašymui, kad užtikrintų atitikimą veiklos standartams, ypatingai, jei partneriai yra įtraukti į vertinimą. Neatitikimams valdyti taip pat turi būti sukurtas atitinkamas procesas.

2.2. Klausimyno sudarymas

Klausimyno sudarymas yra pirmas ir bene svarbiausias naujos sertifikavimo programos kūrimo žingsnis. Klausimynas yra visos sertifikavimo programos turinį glaustai apibūdinantis žinių ir įgūdžių rinkinys. ECDL fondas yra standartizavęs klausimyno sudarymo procedūrą. Klausimyno struktūra pavaizduota 4 paveiksle. Klausimyne išskiriamos įgūdžių ir žinių kategorijos, tai kategorijai tinkamos žinių sritys su kiekvienos srities žinių ir įgūdžių apibūdinimo aprašymu [12]. Visos dalys numeruojamos pagal atitinkamą tvarką, kur pirmas skaičius nurodo modulio numerį (jei sertifikavimo sistema susideda ne iš vieno modulio), antras skaičius žymi kategoriją, trečias - sritį, o ketvirtas - aprašymą.

CATEGORY	SKILL SET	REF.	TASK ITEM
		6.3.3.3	Resize pictures, images in a presentation.
		6.3.3.4	Delete text, pictures, images in a slide.
6.4 Charts/ Graphs, Drawn Objects	*6.4.1 Using Charts/Graphs*	6.4.1.1	Input data to create, modify different kinds of built-in charts/graphs in a slide: column, bar, line, pie.
		6.4.1.2	Change the background colour in the chart/graph.
		6.4.1.3	Change the column, bar, line, pie slice colours in the chart/graph.
		6.4.1.4	Change the chart/graph type.
	6.4.2 Organisation Charts	6.4.2.1	Create an organisation chart with a labelled hierarchy. (Use a built-in organisation chart feature).

Šaltinis: ECDL (2009) [žiūrėta 2009 01 06]. Prieiga per internetą:
<http://www.ecdl.com/files/products/20060331035737_ECDLV4SWG110159.pdf>

Pav. 4 Klausimyno struktūra

Klausimyno turinys turi būti aiškiai apibrėžta informacija, kad kandidatas galėtų vienareikšmiškai nustatyti įgūdžių ir žinių sritis, kuriose atliekamas sertifikavimas. Klausimyno turinys turi būti kaip įmanoma mažiau priklausomas nuo kompiuterinės platformos, operacinės sistemos ar

konkrečios programinės įrangos bei aplikacijos. Klausimyno turinys turi atitikti laikui aktualias IT tendencijas, naujoves, bei žinias. Jis turi būti sudaromas sertifikuojamos srities ekspertų arba su jų pagalba kelių sričių ekspertų. Turi būti atliekamas klausimyno koregavimas, kad užtikrinti, jog klausimynas atitinka dabartines žinias, sukurtas pagal technologinius pažangumus ir naujoves, reikalavimus kandidatui, kurie bus tinkami tuo metu kai produktas bus išleistas. Rekomendacijos koregavimams turi būti gautos iš testuotojų ir iš kandidatų atsiliepimų, taip, kad sričių ekspertai į juos atsižvelgtų prieš klausimyno išleidimą.

2.3. Testo klausimų bazės sudarymas ir koregavimas

Sertifikavimo programos klausimyno sudarymas ir testo klausimų bazės sudarymas yra skirtingi, tačiau tiesiogiai susiję procesai, kadangi testo klausimai sudarinėjami tik iš klausimyne aprašytų kategorijų ir sričių, ir tik taip, kaip aprašyta klausimyno aprašomuosiuose dalyse. Testo klausimų bazė turi pilnai atitikti ir išpildyti sertifikavimo programos klausimyną. Testo klausimų bazės sudarymas yra taip pat standartizuotas ECDL fondo. Sertifikavimo programos testo klausimų bazės klausimai sudaromi taip, kad būtų skirti automatiniam arba rankiniam testavimui atlikti. Pastaruoju metu populiaresnis yra automatizuotas testavimas. Automatizuotam testavimui sudaromi klausimai talpinami į automatizuoto testavimo klausimų bazę (AQTB). Šie klausimai būna dviejų tipų:

- Klausimas su keturiais atsakymo variantais iš kurių vienas teisingas
- Klausimas su grafiniu vaizdu. Tai dažniausiai kokios nors aplikacijos lango vaizdas. Klausime nurodoma užduotis, o imitavimo lange reikia pažymėti vietą (ar vietas), kurios reikalingos pasiekti klausime nurodomą rezultatą [11].

Pirmojo tipo klausimų AQTB paprastai būna apie 85 %, antrojo - 15 %. Sudaromi klausimai, prieš talpinant į testavimo serverį, surašomi į standartizuotą formą, kurios pavyzdys pateikiamas 5 paveiksle. Tokioje formoje testo klausimų kūrimo ir koregavimo stadijose klausimai pateikiami ekspertams.

1.10. Understand the benefits and purpose of data and software backups.					
1	41.	1.10.	Why do you need to backup your data?	4	To be able to restore it in case of loosing it. To be able to restore after it has been damaged by a virus. To be able to restore previous state of changed data. All above are correct.
2	42.	1.10.	What should you choose on Control Panel, if you want to create backup?		

Šaltinis: Sudaryta autoriaus

Pav. 5 Klausimų surašymo standartinė forma

Kiekvienai ECDL fondo patvirtintos sertifikavimo programos klausimyno sričiai turi būti sudaryta bent po 4 klausimus. Testo klausimai negali kartotis, turi būti aiškūs, atsakymai nedviprasmiški, kad atsakantysis galėtų vienareikšmiškai suprasti. Testo klausimų turinys turi būti kaip įmanoma mažiau priklausomas nuo kompiuterinės platformos, operacinės sistemos ar konkrečios programinės įrangos bei aplikacijos. Klausimų turinys turi atitikti laikui aktualias IT tendencijas, naujoves, bei žinias. Jie turi būti sudaromi sertifikuojamos srities ekspertų arba su jų pagalba kelių sričių ekspertų. Turi būti atliekamas klausimų koregavimas, kad užtikrinti, jog klausimai atitinka dabartines žinias, sukurtas atitinkant technologinę pažangą ir naujoves, reikalavimus kandidatui, kurie bus tinkami tuo metu kai produktas bus išleistas. Rekomendacijos koregavimams turi būti gautos iš testuotojų ir iš kandidatų atsiliepimų, taip, kad sričių ekspertai į juos atsižvelgtų prieš klausimų išleidimą. Ekspertų sudaryti klausimai perduodami ECDL fondo paskirtiems ekspertams analizuoti. Atsižvelgiant į ekspertų pastabas, testo klausimai koreguojami ir pataisyta versija dar kartą siunčiama ekspertams. Paskui sertifikavimo programos testo klausimai talpinami į testavimo serverį bandomiesiems testavimams. Bandomuosius testus laiko vartotojai, turintys pakankamą kompetenciją sertifikuojamoje srityje. Iš vartotojų surenkami atsiliepimai, pagal kuriuos klausimų sudarymo ekspertai dar kartą koreguoja klausimus. Tokiu būdu turi būti pašalinama kiek įmanoma daugiau

netikslumų, klaidų ar dviprasmybių. Veikiančios sistemos klausimai taip pa gali būti koreguojami. Keičiantis situacijoms, klausimai papildomi, pakeičiami, į klausimų bazė talpinami nauji klausimai.

3. E-GUARDIAN KLAUSIMYNO, TESTO KLAUSIMŲ BAZĖS SUDARYMO IR MODIFIKAVIMO TYRIMAI

Šioje dalyje aprašomi du magistrinio darbo metu atlikti tyrimai. Pirmo tyrimo tikslas - pagal ECDL fondo standartus sudaryti e-Guardian sertifikavimo sistemos klausimyną ir automatizuoto testavimo testo klausimų bazę, bei paruošti e-Guardian standartizavimo patvirtinimo paraiškos formą ECDL fondui. Antro - nustatyti bei įvertinti e-Guardian sertifikavimo programos klausimyno ir testo klausimų bazės klaidas, modifikuoti klausimyną ir automatinio testavimo testo klausimų bazę.

3.1. E-Guardian klausimyno ir testo klausimų bazės sudarymo tyrimas

Tyrimo tikslas – pagal ECDL fondo standartus sudaryti e-Guardian sertifikavimo sistemos klausimyną ir automatizuoto testavimo testo klausimų bazę, bei paruošti e-Guardian standartizavimo patvirtinimo paraiškos formą ECDL fondui.

Tyrimas atliekamas trim etapais. Pirmajame etape, pagal ECDL fondo standartus, ruošiamas e-Guardian programos klausimynas. Antrajame etape pagal sudarytą klausimyną sudarinėjama testo klausimai automatizuoto testavimo klausimų bazei. Trečiasis etapas, tai e-Guardian standartizavimo ECDL fonde, paraiškos ruošimas.

Tyrimo tikslui pasiekti iškeliami tokie uždaviniai:

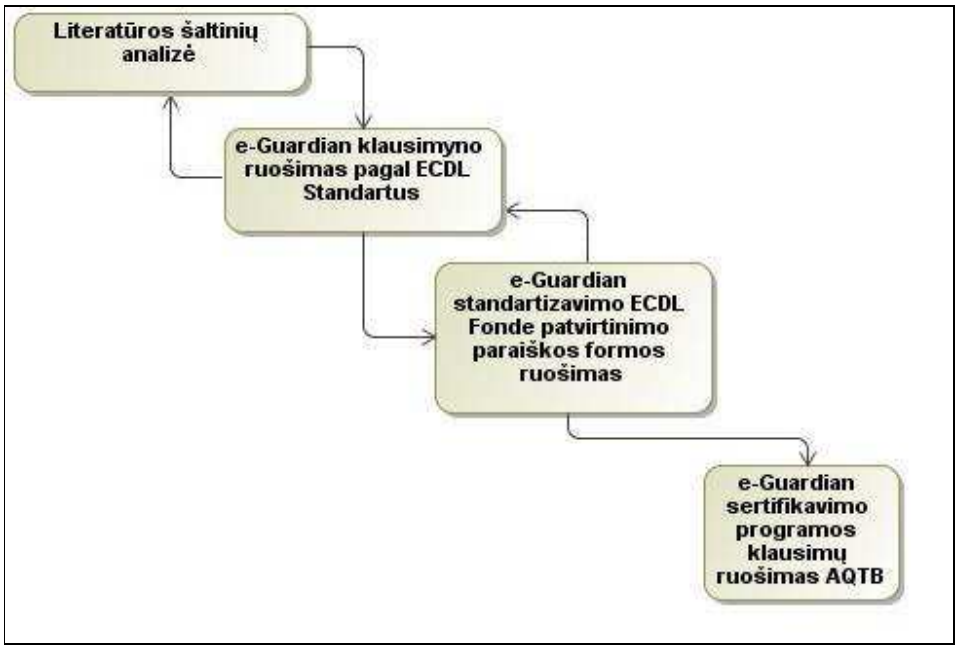
1. Atlikti literatūros analizę.
2. Pagal ECDL fondo standartus, paruošti e-Guardian sertifikavimo programos klausimyną.
3. Pagal sudarytą e-Guardian sertifikavimo programos klausimyną, paruošti automatizuoto testavimo klausimų bazei testo klausimus, atitinkančius ECDL fondo standartus.
4. Pagal ECDL fondo reikalavimus, paruošti e-Guardian sertifikavimo programos standartizavimo patvirtinimo paraiškos formą ir pateikti ECDL fondui.

Tyrimo metodai. Šiam tyrimui buvo taikoma literatūros analizė, palyginimo metodas. ECDL fondo kokybės valdymo standartai nusako metodus, kuriais reikia naudotis tyrime. Jie ir panaudoti sudarinėjant klausimyną, bei testo klausimų bazę. Metodai aprašyti 2.2. ir 2.3. darbo dalyse. Standartizavimo formos ruošimui buvo taikomas metodas aprašytas 2.1. darbo dalyje.

Tyrimo metu atliekama literatūros apie sertifikavimo programų kūrimą, vaikų apsaugą internete, interneto grėsmes, saugumą, apsisaugojimą nuo grėsmių, atsiskaitymus internetu, duomenų apsaugą analizė. Sudarinėjant sertifikavimo sistemos klausimyną ir programos testo klausimus buvo laikomasi ECDL fondo iškeltų standartų, pasinaudota darbo autoriaus darbo patirtimi sertifikuojamoje srityje.

Viso tyrimo metu bus konsultuojamasi su ECDL standartų, testo klausimų sudarinėjimo ekspertais, kompiuterinių sistemų saugumo specialistais.

Tyrimo organizavimas. Tyrimo, atlikus literatūros analizę, e-Guardian sertifikavimo programos klausimynas buvo pradėtas sudarinėti 2008 vasario mėnesį ir konsultuojantis ECDL su standartų, klausimyno ir testo klausimų sudarinėjimo ekspertais, kompiuterinių sistemų saugumo specialistais, baigtas 2008 balandžio mėnesį. Sudarius klausimyną buvo pradėta ruošti ECDL standartų atitikimo patvirtinimo paraiškos forma, kuri baigta 2008 gegužės mėnesį ir išsiųsta ECDL fondui. Lygiagrečiai, nuo pat klausimyno baigimo, buvo pradėti sudarinėti ir e-Guardian testo klausimai automatizuoto testavimo klausimų bazei. Klausimų pirmoji versija paruošta per pusę metų ir pirmą kartą siunčiama ECDL fondo ekspertams 2008 12 08. Tolimesnis klausimų redagavimas daromas antrojo tyrimo rėmuose. Tyrimo veiklos diagrama pateikiama 6 paveiksle.



Šaltinis: Sudaryta autoriaus

Pav. 6 Tyrimo veiklos diagrama

3.1.1. Literatūros analizės tyrimo rezultatai.

Tyrimo metu atlikta literatūros apie sertifikavimo programų kūrimą, vaikų apsaugą internete, interneto grėsmes, saugumą, apsisaugojimą nuo grėsmių, atsiskaitymus internetu, duomenų apsaugą analizė. Toliau šiame skyriuje pateikiama medžiaga apie pagrindinius apsaugos būdus, žinias, kurias

turi žinoti vartotojas norintis mokėti saugiai dirbti kompiuteriu, naršyti internete ir apsaugoti vaikus nuo grėsmių susijusių su internetu.

3.1.1.1. Vaikų apsauga internete

Saugiam vaikų darbui internete turi būti skirtas ypatingas dėmesys: pokalbių svetainėse ir elektroniniu paštu galimas kontaktas su nepažįstamaisiais (kartais vaikai sutinka susitikti su savo internetiniu pažįstamu, net nesuvokdami, kad jis gali būti ne toks, kokiu apsimeta). Kita grėsmė vaiko ar paauglio psichikai yra netinkamo (pornografinio, propaguojančio žiaurumą) turinio interneto svetainės, galinčios pakenkti vaiko asmenybės vystimuisi. Taip pat nepamirškime galimybės beveik viską nusipirkti internetu. Jeigu vaikas be tėvų ar globėjų priežiūros turės galimybę pirkti internetu, jis gali nebūtinai suvokdamas pasekmes tuo pasinaudoti.

Nustatyta, kad internetu naudojasi 73 proc. apklaustų Lietuvos vaikų. Tyrimai, atlikti kitose šalyse, rodo, kad bene pusė visų interneto vartotojų yra paaugliai nuo 8 iki 14 metų, o mažamečiai vaikai iki 5 metų sudaro net 25 proc. visų interneto vartotojų. Dauguma jaunųjų interneto vartotojų internetu naudojasi be jokių apribojimų ar kontrolės [18].

Pastaruoju metu žalingo turinio sklaidos internete reguliavimas yra viena iš aktualių žinių visuomenės plėtros problemų, kurios sprendimui vis daugiau dėmesio skiriama įvairiose Europos valstybėse. Pagal Lietuvos Respublikos Vyriausybės 2003 m. kovo 5 d. nutarimą Nr. 290 „Dėl viešo naudojimo kompiuterių tinkluose neskelbtinos informacijos kontrolės ir ribojamos viešosios informacijos platinimo tvarkos patvirtinimo", neskelbtina informacija yra ta, kurią paviešinti ir (ar) platinti draudžia Lietuvos Respublikos įstatymai, o ribojama viešoji informacija - kenkianti nepilnamečių fiziniam, protiniam ir doroviniam vystimuisi viešoji informacija, kurios platinimas ribojamas siekiant apsaugoti nepilnamečius. Internetas, jei juo vaikai ir paaugliai naudojasi be suaugusiųjų priežiūros, gali sukelti nemažai pavojų [18].

Pokalbių svetainėse ir elektroninio pašto žinutėmis vaikas dažnai bendrauja su nepažįstamaisiais, kurių siekiai neretai būna pavojingi vaikams, kartais vaikai sutinka susitikti su savo internetiniu „draugu“ nesuvokdami, kad jis gali būti ne tas, kuriuo apsimeta, arba susitikę patirti fizinį ir moralinį smurtą. Netinkamo turinio internetiniai tinklalapiai (pornografija, žiaurumai, baimės ir neapykantos kurstymas) žaloja vaiko ar paauglio psichiką, kenkia vaiko asmenybės vystimuisi. Kompiuteriniai virusai, šnipinėjimo programos, nepageidaujami e. pašto laiškai ir pan. dažnai plinta pasinaudodami vaikų smalsumu, naivumu ir nesupratimu. Jie gali

rimtai pakenkti kompiuteriams ar juose saugomai informacijai. Šiuolaikinės e. prekybos suteikiamos galimybės beveik viską nusipirkti internetu yra ne tik patogus ir greitas būdas įsigyti reikalingas paslaugas ir daiktus, bet ir gali būti rimtas išbandymas šeimos biudžetui, jei vaikas be tėvų ar globėjų priežiūros turės galimybę pirkti internetu [18].

Pirmas žingsnelis apsisaugant patiems ir apsaugant vaikus nuo grėsmių, susijusių su nesaugiu interneto naudojimu, - patiems turėti informaciją apie galimas grėsmes ir žinoti būdus, kaip jų išvengti. Būtina šviesti šia tema ne tik vaikus, bet ir jų tėvus ar globėjus. Antrasis - su vaikais būtina kalbėtis apie jų tykančius pavojus. Vaikams reikia išaiškinti ne tik interneto galimybes, bet ir jo trūkumus. Vaikas turi suvokti, kad internetas gali būti pavojingas tiek psichologiniu požiūriu, tiek ir fiziniu [18].

3.1.1.2. Interneto pavojai

Internetu naudojasi ne tik geranoriškai nusiteikę žmonės. Kaip ir realiame gyvenime, čia pasitaiko piktavalių asmenų, siekiančių neteisėtai pasipelnyti, apgauti, piktam pasinaudoti įgytu pasitikėjimu. Kai kuriems žmonėms tiesiog patinka įsibrauti į kitų žmonių kompiuterius, visaip kenkti, platinti virusus, vogti ir gadinti duomenis. Nedori verslininkai interneto paslaugas naudoja nepageidaujamiems laiškams bei reklamai platinti, nekalbant jau apie pornografijos verslą, kuris internetą tiesiog užtvindė vaikams netinkamu turiniu. Bendravimas su kitais žmonėmis internetu gali būti ne tik malonus. Anonimai gali įsijungti į pokalbį ir išreikšti agresiją ar kitaip įskaudinti. Blogiausia, kai taip nutinka nepilnamečiams, kurie į tai jautriai reaguoja, bet dažniausiai negali ar nenori apie tai pasikalbėti su suaugusiais ar netgi draugais. Kai internetu siunčiama specialiai neužkoduota informacija, ją gali sužinoti ir kiti žmonės. Tiek elektroninio pašto laiškus, tiek ir informaciją apie tai, kokiose svetainėse lankotės, gali stebėti darbdavys (darbovietėje), interneto paslaugų teikėjas (tiek darbovietėje, tiek ir namuose) ir visi interneto kompiuterių, per kuriuos keliauja Jūsų siunčiama informacija, valdytojai. Beveik visas tarptautinis interneto srautas yra įrašomas ir analizuojamas kai kurių šalių specialiųjų tarnybų. Dar didesnė rizika, jei naudojatės belaidžiu interneto ryšiu. Tuomet duomenis perimti gali bet kas, esantis signalo sklidimo nuotolyje.

Internetas yra laisva ir beveik nekontroliuojama informacijos erdvė, kurioje pilna kenksmingo ir nepriimtino turinio svetainių. Įvairios interneto turinį prižiūrinčios tarnybos kovoja daugiausia su jau įvykusiais elektroniniais nusikaltimais, todėl pirmiausia reikia saugotis patiems interneto vartotojams.

3.1.1.3. Saugumo mitai

Turiu antivirusinę programinę įrangą, taigi aš esu visiškai apsaugotas. Ne tik virusai kelia grėsmę saugumui, taigi tai panašu į atvejį, kai paradinės durys užrakinamos, bet langai paliekami atviri. Pavyzdžiui, antivirusinė programinė įranga neapsaugos nuo piktų kompiuterinių įsilaužėlių, nesustabdys šnipinėjimo programinės įrangos ir nesutrukdys jiems tiesiogiai prisijungti prie Jūsų kompiuterio [18].

Aš niekam neįdomus. Vėl klystate. Daugelis kompiuterinių įsilaužėlių ir nusikaltėliai dirba kartu. Pavogti Jūsų tapatybę daug pelningiau nei pavogti Jūsų televizorių. Anonimiškumas – tai ne apsauga. Nusikaltėliai naudojasi automatizuotais įrankiais, kad surastų potencialias aukas. Per valandą internetu jie gali iššvalgyti dešimtis tūkstančių kompiuterių. Tai panašu į telefonų knygos vartymą ir atsitiktinį skambinimą žmonėms, siekiant išsiaiškinti, ar jie namuose [18].

Darau atsargines informacijos kopijas. Vien tik informacijos kopijavimas Jūsų neapsaugos. Tai tas pats, kas kelyje sugedus mašinai džiaugtis, kad garaže turite kitą. Be to, galite nukopijuoti jau užkrėstus duomenis, nebent kopijas parengėte prieš užpuolant virusams [18].

Esu apsidraudęs. Paprastai draudimo bendrovės į kompensuojamų nuostolių sąrašą neįtraukia virusų atakų padarytos žalos. Bendrovės siūlo specialų draudimą verslui, bet dažniausiai reikalauja papildomos apsaugos kompiuteriams. Būna labai įvairių draudimo polisų, todėl pasigilinkite į savąjį ir išsiaiškinkite, kokie nuostoliai bus dengiami [18].

Virusus gauname tik elektroniniu paštu. Deja, yra daugybė būdų apkrėsti virusu savo kompiuterį. Pavyzdžiui, lankantis svetainėse, naršant internete, į kompiuterį įdedant keičiamus diskus, prijungiant USB atmintines, ar tiesiog įdiegiant užkrėstas programas [18].

Jei prarasiu pinigus, bankas ar kredito kortelę išdavusi bendrovė viską sutvarkys. Jei Jūs galėsite įrodyti, kad nesate atsakingas dėl skolos, kuri susikaupė apgaulingai pasinaudojus iš jūsų pavogta informacija, pinigai bus grąžinti. Tačiau kompensacijos už sugaištą laiką ir patirtą stresą negausite. Nėra malonu, kai nukenčia ilgus metus kurta nepriekaištinga kredito vartotojo reputacija. Įprastai vagystei išsiaiškinti reikia savaitės ar daugiau, bet yra ir tokių tapatybės vagystės pavyzdžių, kai vagystei išsiaiškinti reikia net kelių mėnesių [18].

„Interneto policija“ neleis, kad man atsitiktų kas nors bloga. Tokio dalyko kaip „interneto policija“ nėra! 2001 metais Lietuvos kriminalinės policijos biuro Nusikaltimų tyrimo vyriausiojoje valdyboje buvo įkurtas specializuotas Nusikaltimų elektroninėje erdvėje tyrimo

skyrius – NEETS. NEETS yra centrinės šalies kriminalinės policijos padalinys, kurio misija yra užtikrinti Konvencijos dėl elektroninių nusikaltimų reikalavimų įgyvendinimą, užkardyti, tirti ir atskleisti ruošiamus, daromus ar padarytus nusikaltimus elektroninėje erdvėje – pasauliniame interneto tinkle bei korporatyvinėse informacinėse sistemose – intranete, taip siekiant užtikrinti Lietuvos visuomenės ir informacinių technologijų saugumą šioje sferoje. Tačiau apsaugoti Jūsų prieš padarant nusikaltimą, ar garantuoti, kad nusikaltėliai bus išaiškinti neįmanoma. Internetas neturi sienų ir prisijungę nusikaltėliai gali naudotis jų tapatybę nuslepiančiomis technologijomis [18].

Kompiuterio apsauga atima daug laiko. Tapatybės vagystei išaiškinti reikia vidutiniškai 60 valandų ir dar poros dienų, kol kompiuteris išvalomas nuo virusų ir šnipinėjimo programinės įrangos. Daug geriau vagystei užkirsti kelią [18].

Mano interneto paslaugų teikėjas saugo nuo pavojaus, gresiančio naudojantis interneto ryšiu. Kai kurie interneto paslaugų teikėjai pateikia kai kurias apsaugos paslaugas, pavyzdžiui, virusų paiešką gaunamuose ir siunčiamuose elektroninio pašto laiškuose, aprūpina interneto užkarda, tačiau turite tą tiksliai žinoti. O dar svarbiau žinoti, kokios apsaugos jie neteikia. Kai kurie interneto paslaugų teikėjai nesuteikia jokių interneto saugumo paslaugų. Tą žinant, nesiimti saugumo priemonių būti brangi klaida [18].

Mano kompiuteryje veikia „Mac“ ar „Linux“ operacinė sistema, todėl esu saugus. Tiesa, kad *Mac* ir *Linux* operacinės sistemos puolamos mažiau nei *Windows* operacinė sistema, tačiau tai nereiškia, kad jos visiškai nepažeidžiamos. Visų šių operacinių sistemų kūrėjai reguliariai teikia programų atnaujinimus, lopančius kompiuterio saugumo spragas. Be to, dauguma internetinių sukčių naudojasi tokia pat įranga, kaip ir Jūs [18].

3.1.1.4. Kaip apsisaugoti?

Kompiuteryje esanti žalinga programinė įranga dažniausiai veikia nepastebimai, tačiau kartais dėl jos galite pastebėti neįprastą kompiuterio elgseną, pavyzdžiui:

- programų veikimas sulėtėja ir paprasti veiksmai trunka ilgiau nei įprasta;
- programoms pradeda nepakakti kompiuterio darbinės atmintinės;
- atveriami įvairūs reklaminiai langai netgi nepaleidus interneto naršyklės;
- be Jūsų žinios pakeičiamas interneto naršyklės pradinio tinklalapio adresas;

- interneto ar *Windows* naršyklėje rodoma nauja priemonių juosta, kuria sunku atsikratyti;
- programos be Jūsų žinios jungiasi prie interneto, ilgai ir intensyviai siunčia duomenis.

Nuo daugelio interneto ir kompiuterinių virusų keliamų grėsmių galima apsisaugoti specialiomis programinėmis priemonėmis - interneto užkardomis, antivirusinėmis ir šnipus naikinančiomis programomis, pašto filtrais ir kt. Tačiau vien to nepakanka. Būtina taip pat reguliariai naujinti antivirusinę ir visą likusią programinę įrangą, kopijuoti svarbius duomenis bei laikytis tam tikrų saugaus elgesio internete rekomendacijų.

3.1.1.5. Turinio filtravimo priemonės

Tam tikros interneto saugumu besirūpinančios organizacijos vertina interneto svetainių turinį ir jam priskiria vienokį ar kitokį reitingą. Kai kurios naršyklės (pavyzdžiui, *Internet Explorer*) turi vertinimus tikrinantį turinio filtrą, kurį įjungus svetainės turinys parodomas arba blokuojamas. Tačiau žalingas turinys pasitaiko ne tik tinklalapiuose, su juo susiduriama ir bendravimo kanaluose ar naudojantis e. paštu. Daug geresnis sprendimas - naudotis specialia filtruojančia programa. Jos veikia įvairiai. Kai kurios programos blokuoja žinomas netinkamo turinio svetaines. Kitos neleidžia vaikams naudotis bendravimo kanalais ar siųsti bei skaityti e. laiškus. Labai svarbu suvokti, kad vien filtravimo programos Jūsų vaiko negali apsaugoti nuo visų internete tykančių blogybių. Pirmiausia, nė viena programa nesugebės blokuoti absoliučiai visų netinkamų svetainių, o kai kuriais atvejais programa gali blokuoti svetaines, kurios yra tinkamos.

Filtravimo programos neatstoja tinkamo vaikų auklėjimo ką jie gali ir ko negali daryti internete. Nesvarbu, įdiegti filtrai ar ne, visi šeimos nariai turi nuovokiai elgtis tinkle ir bendradarbiauti vieni su kitais. Platinama gana daug įvairių filtravimo programų. Daugelis jų yra mokamos ar pritaikytos angliškai kalbantiems vartotojams (pastaruoju atveju jos dažniausiai nereaguoja į netinkamus kitų kalbų žodžius). Pats geriausias turinio filtravimo būdas - kai kontrolė vykdoma kompiuterių tinkle ir centralizuotai. Filtruojanti programa gali būti įdiegta interneto tiekėjo serveryje, įmonės ar švietimo įstaigos atstovaujančiame (angl. *proxy*) serveryje. Tuomet interneto vartotojus pasiekia tik maksimaliai saugus turinys.

3.1.1.6. Reklamų blokavimas

Nepageidaujamam ir žalingam interneto turiniui taip pat priskiriamos daugelis reklamų. Labiausiai įkyrios reklamos rodomos atskiruose iškylančiuose naršyklės languose, kurie gali taip sparčiai rastis, kad nespėsite jų užverti. Kai kuriose svetainėse tyčia sukuriamas toks turinys, kad užvėrus vieną reklaminį langą, jo vietoje būtų atverti keli. Reklamos ne tik blaško dėmesį, papildomai naudoja kompiuterio išteklius, bet ir pats jų turinys ar tematika skirti suaugusiems. Šiuolaikinės naršyklės gali blokuoti bet kokį turinį, gaunamą iš "juodajame sąraše" esančių adresų, taip pat nerodyti tam tikru formatu pateikiamų interneto dokumentų, pavyzdžiui, animacijos. Paprastai naudojama papildoma programinė įranga, kuri reklamas blokuoja pagal iš anksto sukurtus ir nuolat atnaujinamus "juoduosius sąrašus".

3.1.1.7. Susitarimas su vaikais

Kaip rodo pasaulinė praktika, nepakanka kalbėti vaikams apie galimas grėsmes, bandyti vienašališkai primesti savo valią, taikyti įvairias kontrolės ir sekimo sistemas, bet su vaikais reikia kalbėtis, pasiekti susitarimą, bendrai sudaryti interneto naudojimo taisykles ar net pasirašyti įsipareigojimų sutartį. Vaikų ir tėvų sutarties esmė yra tėvų įsipareigojimas saugoti nuo galimų pavojų savo vaiką, pripažinti jo gebėjimus, protingai kontroliuoti jo veiklą internete ir prireikus ištiesti pagalbos ranką. Vaikai įsipareigoja saugiai naudotis internetu ir apie visas kilusias grėsmes pranešti tėvams.

Organizacija „Langas į ateitį“ siūlo pavyzdinę sutarties tarp tėvų ir vaikų sutartį [25]:

Tėvų sutarties dalis

Žinau, kad internetas gali būti puiki vieta mano vaikams naršyti. Taip pat žinau, kad turiu atlikti savo pareigą ir padėti jiems saugiai naršyti internete. Suvokdamas, kad mano vaikai gali man padėti, sutinku su šiomis taisyklėmis:

1. Žinosiu, kokiomis paslaugomis ir tinklalapiais naudojasi mano vaikas.
2. Savo vaikams nustatysiu saikingas kompiuterio naudojimo taisykles ir gaires, aptarsiu jas ir pakabinsiu šalia kompiuterio kaip priminimą.
3. Nereaguosiu pernelyg jautriai, jei vaikas man pasakytų apie ką nors „bloga“, ką jis rado ar daro internete.

4. Stengsiuosi žinoti, kas yra mano vaiko „internetiniai bičiuliai“ ir bičiulių sąraše esantys kontaktiniai asmenys. Taip pat stengsiuosi žinoti, kas yra jo draugai.

5. Stengsiuosi užtikrinti, kad namų kompiuteris būtų vietoje, kur renkasi visa šeima.

6. Pranešiu apie įtartiną ir nelegalią veiklą bei tinklalapius kompetentingoms įstaigoms.

7. Sudarysiu ar rasiu vaikams rekomenduojamų tinklalapių sąrašą.

8. Dažnai tikrinsiu, kur mano vaikai lankėsi internete.

9. Ieškosiu būdų filtruoti ir blokuoti netinkamą interneto medžiagą, kad ji nepasiektų mano vaikų.

10. Kalbėsiuosi su vaikais apie jų atradimus internete ir kiek įmanoma dažniau pats kartu su jais ieškosiu nuotykių internete.

Vaiko sutarties dalis

Žinau, kad internetas gali būti puiki vieta naršyti. Taip pat žinau, kad man svarbu laikytis šių taisyklių, kurios padės man saugiai naršyti internete. Sutinku su šiomis taisyklėmis:

1. Pasirinksiu saugų ir protingą slapyvardį, kuriame neatsiskleistų asmeninė informacija apie mano šeimą ar mane.

2. Saugosiu savo slaptažodį paslaptyje, bet tik ne nuo tėvų. Nesiregistruosiu elektroninio pašto dėžutėms sukurti be mano tėvų sutikimo.

3. Nenurodysiu savo asmeninės informacijos savo aprašyme, tai yra vardo, pavardės, adreso, telefono numerio, amžiaus ar mokyklos pavadinimo bei kitos informacijos. Nesidalysiu savo asmenine informacija, mano tėvų ar kitų šeimos narių informacija jokiu būdu ar forma internete ir neteiksiu jos niekam, su kuo susipažinsiu internetu.

4. Elgsiuosi internete su kitais taip, kaip noriu, kad būtų elgiamasi su manimi.

5. Elgsiuosi internete mandagiai, kalbėsiu gražia kalba ir rodysiu pagarbą. Nepradėsiu ginčų ir nevartosiu grasinančių ar netinkamų žodžių.

6. Mano asmeninis saugumas bus mano prioritetas, nes žinau, kad tinkle gali būti žmonių, apsimetančių kitokiais, nei yra iš tikrųjų.

7. Sąžiningai bendrausiu su tėvais ir papasakosiu jiems apie žmones, su kuriais susipažįstu internete, nebūtinai tik tėvams prašant. Neatsakysiu į jokius elektroninius laiškus ar žinutes, kuriuos siunčia tėvų nepatvirtintas asmuo.

8. Jeigu matysiu ar perskaitysiu dalykus, kurie yra blogi, bjaurūs ar nedori, atsijungsiu ir papasakosiu tėvams, kad jie galėtų užtikrinti, jog tai nebepasikartos.

9. Papasakosiu tėvams gavęs nuotraukas, nuorodas į blogus tinklalapius, elektroninius laiškus ar žinutes, kur vartojama netinkama kalba, arba apie pokalbių svetainę, kur žmonės vartoja keiksmažodžius ar nedorą ir bjaurią kalbą.

10. Nesiųsiu nieko žmogui, su kuriuo susipažinau internete, be mano tėvų pritarimo. Gavęs ką nors iš žmogaus, su kuriuo susipažinau internete, iš karto pasakysiu tėvams (nes tai reiškia, kad tas asmuo gali turėti mano asmeninę informaciją).

11. Nedarysiu nieko, ko manęs prašo mano internete sutiktas asmuo, ypač jei žinau, kad mano tėvams tai nepatiktų ar jie tam nepritartų.

12. Neskambinsiu, nerašysiu paprastų laiškų ar nesusitiksiu asmeniškai su žmonėmis, su kuriais susipažinau internete, tėvams nepritarus ar neinat kartu su manimi.

13. Suprantu, kad tėvai prižiūrės, kiek laiko leidžiu internete, ir naudos programinę įrangą mano naršymui internete stebėti ar riboti. Jie tai daro, nes mane myli ir nori apsaugoti.

3.1.1.8. Interneto užkarda

Prie kiekvieno kompiuterio, kuris įjungtas į kompiuterių tinklą, gali prisijungti kiti žmonės, gauti kompiuteryje esančius duomenis, adresus bei slaptažodžius ar netgi valdyti kompiuterį. Interneto programišiai nuolat žvalgo kompiuterių tinklus ir radę neapsaugotą kompiuterį stengiasi įsibrauti, įrašyti jame kenksmingą programinę įrangą, kuri ne tik išsiųstų norimus duomenis, bet ir prireikus perimtų kompiuterio valdymą. Jei kompiuteris kuriuo nors būdu prijungtas prie interneto, tai jis atakuojamas maždaug porą kartų per minutę, o jei internetą gaunate iš didžiųjų interneto tiekėjų, turinčių tūkstančius vartotojų - net kas kelias sekundes.

Nuo įsibrovėlių kompiuterį gali apsaugoti interneto užkarda (angl. *firewall*). Daugelis operacinių sistemų (pavyzdžiui, *Microsoft Windows XP* ar *Vista*) turi nuosavą užkardą, kurią tereikia įjungti. Užkarda tikrina iš interneto ir į jį siunčiamas informacijos užklausas. Nekenksmingos užklausos praleidžiamos, o įtartinos blokuojamos. Tinkamai nustačius užkardą, interneto įsibrovėliai tiesiog negalės aptikti Jūsų kompiuterio. Pačiam kompiuterio vartotojui naršyti internete užkarda praktiškai netrukdo. Tačiau įvairių programų mėginimai be vartotojo žinios išsiųsti kokią nors informaciją į išorę ar kitaip susisiekti su interneto kompiuteriais bemat sustabdomi.

Kai kurie kompiuterinio tinklo prietaisai (pavyzdžiui, maršrutizatoriai) taip pat turi interneto užkardas, tik nepatyrusiems ne visuomet paprasta jas tinkamai sureguliuoti. Svarbiausi maršrutizatoriaus derinimo veiksmai aprašyti vartotojo instrukcijoje; prireikus ją rasite gamintojo

interneto svetainėje. Įstaigų vidinis kompiuterių tinklas (intranetas) paprastai apsaugomas centralizuotai - išorės vartotojai negali į jį patekti. Todėl darbo vietų kompiuteriuose pakanka įjungti standartinę operacinės sistemos užkardą.

3.1.1.9. Belaidžio tinklo apsauga

Tokiame tinkle duomenys perduodami radijo signalais, kuriuos tinklo veikimo zonoje gali priimti bet kuris bevielio tinklo įrangą turintis kompiuteris. Neretai įsilaužėliai įsitaiso geras kryptines antenas, kuriomis siunčiamus duomenis priima šimto ir daugiau metrų atstumu. Dar kiti belaidžio ryšio įrangą montuoja automobilyje ir ieško pažeidžiamų tinklų.

Nors nėra visiškai patikimų belaidžio ryšio apsaugos būdų, tačiau verta pasinaudoti bent tomis priemonėmis, kurias turi operacinė sistema ir belaidžio tinklo įranga. *Microsoft Windows XP* operacinėje sistemoje belaidžio tinklo prieiga reguliuojama valdymo skydelio priemone *Bevielio tinklo nust. vedlys*. Čia būtina pasirinkti duomenų šifravimo raktą, - tuomet ryšys bus gana saugus. Atitinkamus nustatymus reikia nustatyti ir namų ar įstaigos belaidžio tinklo prieigos taške.

3.1.1.10. Virusai ir apsaugos nuo jų priemonės

Įvairios kenkėjiškos kompiuterinės programos, sutrikdančios kompiuterio veikimą ar trukdančios dirbti, vadinamos bendru kompiuterinių virusų vardu. Šiuo metu žinoma labai daug virusų, o kasdien sukuriami vis nauji. Nuo virusų saugo speciali programinė įranga. Vienos antivirusinės programos žvalgo kompiuterio laikmenas ir ieško užkrėstų dokumentų, o juos suradusios mėgina virusą pašalinti. Kitos antivirusinės programos budi visą naudojimosi kompiuteriu laiką ir stebi paleidžiamas programas, atveriamus ir įrašomus dokumentus [17].

Kokią antivirusinę programą benaudotumėte, ją reikia kaip galima dažniau atnaujinti, kad toji pažintų pačius naujausius atsiradusius virusus. Kokia bebūtų gera antivirusinė kompiuterio apsauga, tačiau visada išlieka nedidelė tikimybė, kad koks nors virusas šią apsaugą įveiks ir pažeis kompiuteryje laikomus duomenis. Todėl būtina reguliariai daryti svarbiausios informacijos kopijas į kitas laikmenas, kad prarastus duomenis vėliau iš jų būtų galima atkurti. Interneto vartotojai naršydami internete, parsisiųsdami įvairias programas bei dokumentus, gali susidurti su elektroniniais tinklais plintančiais virusais.

Kompiuteriniai virusai – tai nedidelės kompiuterinės programos. Tokios programos nuo įprastų skiriasi tuo, kad yra piktavališkos ir sugeba pačios plisti dažnai dideliu mastu. Kompiuteriniai virusai sukelia žalingus padarinius, pavyzdžiui, sugadina ar viešai paskelbia kompiuteryje esančią informaciją, siuntinėja elektroninius laiškus, perima kompiuterio valdymą ir atakuoja kitus kompiuterius. Virusai dažniausiai plinta elektroniniu paštu, kitais bendravimo kanalais ar būna pridėti prie įvairių programų, kurias paleidus, pradeda veikti ir virusas. Tačiau vis dažniau kompiuterį užkrėsti virusais galima tiesiog apsilankius užkrėstame tinklalapyje [17].

Kompiuteriniai virusai ir panašios kenksmingos programos būna įvairių rūšių.

Tikrieji virusai. Šios programos būna prijungtos prie tam tikro tipo kompiuterio dokumentų (programų ir netgi paveikslėlių). Atvėrus užkrėstą dokumentą, pradeda veikti jame esantis virusas, kuris ne tik užkrečia kitus dokumentus, bet ir gali pakeisti bei sugadinti juose esančią informaciją ar smarkiai sutrikdyti kompiuterio veikimą. Šie virusai plinta dažniausiai kopijuojant užkrėstus dokumentus.

Kirminai. Tai elektroniniu paštu ar bendravimo kanalais plintančios ir labai sparčiai besikopijuojančios programos, kurios bemat užima kompiuterio darbinę atmintinę ir paplinta po visą kompiuterių tinklą. Kirminai dokumentų kompiuteryje neužkrečia, bet rimtai sutrikdo kompiuterio ir tinklų veikimą. Kirminai dažniausiai būna pridėti prie elektroninių laiškų ir paleidžiami atvėrus laiško priedą.

Trojos arkliai. Taip vadinamos kompiuterinės programos, paslėptos kitose esą naudingose programose. Trojos arkliai patys neplinta, tačiau naudojasi interneto vartotojų smalsumu ir patiklumu. Parsisiuntus ir paleidus kokią nors tarsi naudingą programą, pradeda veikti ir joje glūdintis Trojos arklys, kuris dažniausiai kompiuterį padaro prieinamą visiems ar tik konkretiems interneto įsilaužėliams. Tuomet šie įsilaužėliai gali įsibrauti į kompiuterį, gauti jame saugomus duomenis, netgi valdyti kompiuterį ir juo pasinaudoti atakoms prieš kitus kompiuterius.

Makrovirusai. Šie virusai apkrečia įvairiomis raštinės programomis sukurtus dokumentus, pavyzdžiui, beveik visus Microsoft Office programų dokumentus. Jei atveriant apkrėstą dokumentą programoje būna neuždraustas makrokomandų vykdymas, tada virusas kopijuojamas į kitus atvertus dokumentus bei dokumentų šablonus. Nuo šablonų užkrečiami visi naujai kuriami dokumentai.

Interneto svetainėse gali būti kenkėjiškų *Java, JavaScript* bei *ActiveX* programėlių. Pakanka aplankyti tokią svetainę, ir žalinga programa parsiunčiama į kompiuterį bei pradeda jame veikti.

Antivirusinių programų paskirtis - aptikti ir nukenksminti žalingą programinę įrangą. Šiuolaikinės antivirusinės programos geba naikinti ne tik tikruosius kompiuterinius virusus, bet ir

Trojos arklius ar kirminus. Kai kurios iš jų netgi užkerta kelią duomenų išviliojimui. Platinama tikrai nemažai įvairių antivirusinių programų, kurios skiriasi savo galimybėmis, veiksmingumu ir, be abejo, kaina. Kokia bebūtų gera antivirusinė programa, ji bus veiksminga tik tada, jei reguliariai ją atnaujinsite. Kasdien paplinta vis nauji kompiuteriniai virusai, todėl antivirusinė programa turi juos pažinti. Dauguma tokių programų kasdien (galite nurodyti ir rečiau) automatiškai jungiasi internetu ir parsisiunčia naujausią informaciją apie galimus virusus.

Įsigydami antivirusinę programinę įrangą įvertinkite, kiek laiko ji bus nemokamai naujinama. Daugelis kompiuterių pardavėjų kaip papildomą vertę siūlo kompiuteryje įdiegtas komercines antivirusines programas su pusmečio ar metų naujinių prenumerata. Tačiau, pasibaigus šiam laikui, už prenumeratos pratęsimą turite sumokėti. To nepadarius, antivirusinė kompiuterio apsauga tampa nepakankamai veiksminga. Dar daugiau, kai kurių antivirusinių programų negalima paprastai pašalinti ir įdiegti kitą (vienu metu kompiuteryje gali veikti tik viena tokia programa). Todėl iškart turėtumėte apsispręsti - ar naudosite komercinę programą ir nuolat mokėsite už naujinimus, ar iškart diegsite nemokamą antivirusinę programą. Tokių nemokamų antivirusinių programų sukurta nemažai ir jas galima parsisiųsti internetu.

Labai panašios į Trojos arklius yra įvairios šnipinėjimo programos (angl. *Spyware, Adware*), kurios seka kompiuterio vartotojo elgesį ir šiuos duomenis išsiunčia internetu. Visa tai yra daroma vartotojui nežinant ir be vartotojo sutikimo. Tokie šnipai gali būti įdėti netgi į legalią programą, parduodamą su licencija. Nors įstatymai pripažįsta, kad kiekvienas žmogus turi teisę į privatumą ir asmeninės informacijos apsaugą, šnipinėjanti programinė įranga šiurkščiai pažeidinėja šias teises. Pagrindinis šnipinėjančių programų darbas yra surinkti ir išsiųsti informaciją apie naršymą internete: kokiuose tinklalapiuose lankosi vartotojai, kiek laiko yra prisijungę ir pan. Taip pat dažniausiai yra renkama informacija ir apie patį kompiuterį: kokia jo operacinė sistema, procesorius, atmintis ir t.t.

Surinkta informacija gali būti panaudota komerciniais tikslais ar statistikai, tačiau vartotojas nežino, kam konkrečiai yra renkama tokia informacija ir kas su ja yra daroma vėliau. Vienas sekimo sistemos pavyzdžių yra visiems gerai žinomos paieškos sistemos *Google* ir elektroninio pašto *GMail* pora. Nors atskirai veikianti *Google* yra visai nekenksminga, tačiau, tuo pat metu naudojant *GMail*, pastaroji surenka žinias apie ieškotą informaciją bei lankytas svetaines. Kadangi *GMail* turi vartotojo atpažinimo duomenis, jam gali būti siuntinėjamos reklaminės šiukšlės [16].

Kai kurie darbdaviai naudoja šnipinėjančias programos savo darbuotojams sekti. Paplitęs įsitikinimas, kad darbdavys turi teisę kontroliuoti darbuotojo susirašinėjimą ir naudojimąsi internetu,

tačiau Lietuvos Respublikos įstatymai draudžia darbuotojų sekimą, pokalbių pasiklausymą ir kitos asmeninės informacijos rinkimą [30].

Kaip interneto šnipai patenka į Jūsų kompiuterį? Daugelį šnipinėjančių programų parsisiunčiate ir įdiegiate kompiuteryje patys, susivilioję jų žadamomis galimybėmis. Pavyzdžiui, anksčiau garsi programa *Gator* įsimindavo įvairius svetainių slaptažodžius ir padėdavo užpildyti registracijos formas. Daugelis interneto naršyklių ir e. pašto programų priedų - šnipų palengvina informacijos paiešką ar papuošia e. laiškus įvairiais paveikslėliais.

Dauguma interneto svetainių kompiuteryje įrašo taip vadinamus slapukus (angl. *cookies*), kurie leidžia atpažinti tų svetainių lankytojus ir prisiminti jų veiksmus. Pavyzdžiui, internetinės bankininkystės svetainės po kiekvieno vartotojo veiksmo patikrina įrašytus slapukus ir pakartotinai nebereikalauja įvesti slaptažodžių. Baigus seansą, su juo susiję slapukai pašalinami. Tačiau kai kurių svetainių įbrukti slapukai galioja keliasdešimt metų ir juos gali pasiimti kitos lankomos svetainės.

Daugelis antivirusinių programų neapsaugo nuo šnipų. Tam skirta speciali programinė įranga, kuri peržiūri kompiuterio atmintinę ir laikmenas ieškodama žinomų informacijos rinkimo priemonių, o radusi - pasiūlo jas pašalinti. Kadangi šnipinėjimo priemonių, kaip ir virusų, atsiranda vis naujų, su jomis kovojančias programas taip pat reikia naujinti.

3.1.1.11. Programinės įrangos naujinimas

Net ir pati geriausia programinė įranga turi didesnių ar mažesnių saugumo spragų. Programinės įrangos kūrėjai šias spragas lopo ir pasiūlo arba naujesnes ir saugesnes programų atmainas, arba tik jų lopinius - naujinius. Programinio produkto pažeidžiamumą pirmieji aptinka dažniausiai su jo kūrimu nesusiję asmenys. Tada jie sprendžia, ką su savo atradimu daryti - naudoja patys įsilaužimui į svetimas sistemas, perduoda kitiems piktavaliams arba suteikia informaciją programos kūrėjams. Net ir pastaruoju atveju saugumo spraga ištaisoma ne taip greitai - per kelias dienas, savaites ar net metus. Pasirodžius atnaujintai programinei įrangai, rekomenduojama ilgai neatidėliojant ją parsisiųsti ir įdiegti. To nedarant, seniai ir daug kam žinomos saugumo spragos kelia rimtą grėsmę Jūsų kompiuterio ir duomenų saugumui. Tinkamai naujinamos tik legaliai įsigytos programos. Todėl neverta naudoti neteisėtų programų kopijų; neketinant už jas sumokėti, geriau pasirinkti analogiškas nemokamas programas.

Viena iš labiausiai potencialiai pažeidžiamų programų kompiuteryje yra interneto naršyklė. Todėl jos saugumu reikia pasirūpinti pirmiausia. Naudokite tik šiuolaikines saugias naršykles,

pavyzdžiui, *Internet Explorer 7(8)* (pateikiama kartu su *Microsoft Windows Vista* arba parsisiunčiama kaip *Microsoft Windows XP* naršyklės naujinimas), *Mozilla Firefox* ar *Opera.* Šiuolaikinės naršyklės nesunkiai papildomos priedais, leidžiančiais dar saugiau naršyti internete.

3.1.1.12. Privatumas ir duomenų apsauga

Duomenis galima ne tik atskleisti, bet ir prarasti, jei netinkamai juos saugosime. Kaip išvengti daugelio nepageidaujamų laiškų, kaip apsisaugoti nuo suklastotų svetainių ir apgaulingų e. pašto laiškų? Kiekvienas kompiuterio ar interneto svetainės paslaugų vartotojas atpažįstamas pagal jo prisijungimo vardą ir slaptažodį. Šiuos duomenis reikia saugoti ir jų neatskleisti nei bendradarbiams, nei artimiesiems.

Dažnai vienu kompiuteriu naudojasi keli vartotojai. Netgi namuose kiekvienas vartotojas turi turėti savo atskirą prisijungimo vardą ir slaptažodį. Tuomet kiekvieno vartotojo aplinka, nustatymai, dokumentų laikymo vietos bus atskiros ir galės būti apsaugotos nuo kitų to kompiuterio vartotojų. Sudarykite sunkiai atspėjamus slaptažodžius ir patikimai juos saugokite. Kokių apsaugos priemonių reikėtų imtis:

- Niekam neatskleisti savo slaptažodžio.
- Pasirinkti sudėtingą slaptažodį, sudarytą iš mažųjų ir didžiųjų raidžių, skaitmenų, specialiųjų ženklų. Kuo ilgesnis slaptažodis, tuo sunkiau jį atspėti.
- Nenaudoti slaptažodžių, sudarytų iš asmenvardžių, adresų, telefono numerių ir kitų nesunkiai atspėjamų žodžių.
- Slaptažodžius įsiminti, nerašyti jų popieriuje.
- Skirtingose interneto svetainėse naudoti skirtingus slaptažodžius, nes jei nepatikimoje svetainėje įvesite slaptažodį, jis bus žinomas piktavaliams.
- Dėl didesnio saugumo slaptažodžius periodiškai keisti.

Microsoft Windows vartotojų slaptažodžiai apsaugo privačią informaciją tik nuo kitų *Windows* vartotojų. Turint tam tikrą programinę įrangą *Windows* vartotojų slaptažodžius galima sužinoti, pakeisti (pavyzdžiui, pakeisti gali kitas to kompiuterio administratoriaus teises turintis vartotojas), o iš kompaktinio disko įkėlus kitą operacinę sistemą (pavyzdžiui, *Ubuntu Baltix*) visi kompiuteryje esami dokumentai bus matomi neįvedant jokių slaptažodžių. Liks apsaugoti tik profesionalių *Windows* atmainų sisteminėmis ar kitomis priemonėmis šifruoti dokumentai.

Kaip prisiminti įvairiose svetainėse naudojamus savo slaptažodžius ir prisijungimo vardus, juk jie gali ir turi būti skirtingi? Beveik visos naršyklės gali juos įsiminti. Tačiau įsilaužėliai tada nesunkiai galės jais pasinaudoti. Geriau naudokite specialią tam skirtą programinę įrangą. Slaptažodžių įsiminimo programos susieja prisijungimo vardus ir slaptažodžius su atitinkamomis svetainėmis ir dažnai netgi pasiūlo automatiškai užpildyti registracijos formų laukus. Slaptažodžiai gali būti saugomi kompiuterio diske ar net USB atmintinėje. Norint jais pasinaudoti, reikalingas pagrindinis slaptažodis.

Įvairių el. paslaugų, kurios reikalauja identifikacijos, daugėja, taip pat sparčiai populiarėja mobiliosios technologijos, elektroninis privatumas tampa vis rimtesne problema. Kiekvieną kartą, kai internetu atsiskaitinėjate kreditine kortele, registruojatės tinklalapyje ar tiesiog naršote viešame belaidžiame tinkle, rizikuojate, kad kažkas gali pasisavinti asmeninius Jūsų duomenis. Šie duomenys gali būti panaudoti piktam: piktavaliai gali apsimesti Jumis, išvilioti daugiau informacijos iš Jūsų ar Jūsų artimųjų, Jūsų vardu įsigyti prekes ar paslaugas. Ne šiaip sau tokie duomenys turi kainą, yra superkami ir parduodami. Jų vagystė dažnai ir vadinama tapatybės vagyste [17].

Ypatingą paklausą turi e. pašto adresai. Juos superka e. pašto šiukšlintojai.

Svarbiausia taisyklė naudojantis internetu - neatskleisti savo tapatybės: vardo, pavardės, adreso, e. pašto adreso, kitų individualių duomenų. Juk jų neatskleidžiame pirmam sutiktajam. Internete nenaudoti savo tikrojo vardo - sugalvoti slapyvardį. Būti atsargiems internete bendraujant su tais, kurie tuoj pat prašo atskleisti asmeninius duomenis ar susitikti.

Informacija apie darbą, artimuosius, asmeninės svetainės adresas taip pat yra privatūs duomenys. Neįvesti savo tikrų duomenų neaiškiose svetainėse, reikalaujančiose registracijos. Jei registracija reikalinga tam, kad galėtumėte iš tokios svetainės parsisiųsti dokumentą ar programą, nurodyti vienkartinį e. pašto adresą.

Pirkdami prekes ar paslaugas įsitikinti svetainės patikimumu. Joje turi būti nurodyti visi įmonės duomenys, garantijos ir kita informacija. Ryšys su šia svetaine turi būti šifruotas - svetainės adreso pradžia turi būti *https://*, o šalia adreso ar naršyklės būsenos juostoje turi būti rodomas užrakintos spynos ženkliukas ar rakto simbolis.

Naudojantis belaidžiais kompiuterių tinklais, reikia papildomai pasirūpinti savo privačių duomenų saugumu. Viešųjų interneto prieigos taškų siunčiami duomenys ne visuomet yra koduojami, kaip tai yra daroma daugelyje namų tinklų. Informaciją apie kodavimą galite rasti prieigos taško tinklalapio skirsnyje „privatumo tvarka“. Jei Jūsų interneto zonoje kodavimo nėra, o nešiojamame kompiuteryje saugote daug svarbios ar konfidencialios informacijos, tuomet geriau prieigos tašku nesinaudoti visai. Kitas sprendimas - patiems užkoduoti svarbius dokumentus.

Atliekant finansines operacijas internetu įsitikinti ryšio saugumu: šalia svetainės adreso ar naršyklės būsenos juostoje turi būti rodoma rakto ar užrakintos spynelės piktograma , o saugios svetainės adresas prasidėti „https“.

Šios priemonės apsaugos nuo atsitiktinių interneto piktavalių, tačiau ryžtingi nusikaltėliai vis tiek galiausiai apgaus bet kokią saugumo sistemą. Tad norint visiškai užtikrinti savo duomenų saugumą, reikia iš viso vengti viešame belaidžiame tinkle siųsti svarbią informaciją, pavyzdžiui, kreditinių kortelių numerius, finansinius duomenis, svarbius slaptažodžius ir pan.

Pasinaudojus interneto kavinėje, kompiuterių klasėje ar kitoje viešoje vietoje esančiu kompiuteriu paliekame nemažai interneto naršymo pėdsakų, kuriais gali pasinaudoti konfidencialios informacijos vagys.

Tam, kad taip nenutiktų, reikia laikytis kelių paprastų taisyklių:

- Baigę darbą saugiose ir slaptažodžių reikalaujančiose svetainėse, - atsijungti. Pasinaudojus e.pašto, internetinio banko ar kita saugia svetaine, pirmiausia atsijungti, o po to užverti naršyklės langą. Antraip kitas vartotojas galės be jokių slaptažodžių patekti į Jūsų aplinką toje svetainėje ir veikti Jūsų vardu.
- Neleisti naršyklei įsirašyti Jūsų įvedamų prisijungimo vardų ir slaptažodžių. Jei taip atsitiktų, Jūsų duomenimis galėtų pasinaudoti kitas vartotojas. Kai kurios naršyklės gali būti taip sureguliuotos, kad įvedamus duomenis įrašo be atsiklausimo. Todėl, baigus darbą, dėl tikrumo išvalyti visus naršyklės sukauptus privačius duomenis.
- Pašalinti naršyklės saugomus naršymo žurnalo įrašus ir laikinuosius interneto dokumentus.
- Nepalikti kompiuteryje parsisiųstų ir tvarkytų dokumentų, pasiimkite visas savo keičiamąsias laikmenas.

Kaip nepamiršti išvalyti visus naršymo pėdsakus? Geriausia USB atmintinėje nešiotis nuosavą naršyklę, e. pašto ir kitas reikalingas programas. Interneto kavinėse ir kituose viešuose kompiuteriuose piktavaliai dažnai palieka šnipinėjimo programinę įrangą, kuri registruoja visus klavišų paspaudimus ir taip įsirašo Jūsų įvedamus prisijungimo vardus ir slaptažodžius. Turbūt vienintelė išeitis, nereikalaujanti ilgai trunkančio šnipinėjančių programų aptikimo ir valymo, - naudotis USB atmintinėje laikoma slaptažodžių tvarkymo programa, kuri šiuos slaptažodžius automatiškai įrašytų registracijos formose.

3.1.1.13. Atsiskaitymai internetu

Paplitus elektroninei prekybai ir bankininkystei, nemažai mokėjimų atliekame tiesiogiai internetu. Tačiau dažnai nežinome, kas iš tikrųjų gaus mūsų perduodamą informaciją. Galbūt svetainė, kurioje perkate, yra suklastota, o kreditinės kortelės duomenys pateks į rankas sukčiams.

Keletas taisyklių, kaip saugiai naudotis internetine bankininkyste:

- Saugoti prisijungimo prie interneto banko slaptažodžius. Niekas ir jokiomis aplinkybėmis (net ir pats bankas) neturi teisės reikalauti Jūsų pateikti šių slaptažodžių – nei telefonu, nei e.paštu ar kitais būdais. Niekada neatsakinėti į neva Jūsų banko laiškus, reikalaujančius šių duomenų. Bankas e. paštu taip pat nereikalauja pakeisti prisijungimo vardų ar slaptažodžių.
- Saugoti prisijungimo prie interneto banko duomenis. Neatskleisti pašaliniams asmenims savo naudotojo ID ir kitų slaptažodžių. Niekuomet ir niekam nesiųsti šių duomenų e. paštu. Nerašyti savo naudotojo ID ant kodų kortelės ir nepalikti kodų kortelės vietose, kur ją galėtų pamatyti kiti asmenys.
- Nuolatinį slaptažodį tiesiog įsiminti ir niekur jo nerašyti. Tinkamiausias nuolatinis slaptažodis yra nieko nereiškiantis raidžių ir skaitmenų rinkinys. Tuoj pat pakeisti nuolatinį slaptažodį, jei yra įtarimų, kad kažkas jį galėjo sužinoti.
- Visuomet įsitikinti, kad baigus darbą atsijungta nuo interneto banko. Baigus darbą, įsitikinti, kad uždaryta naršyklė.
- Jei sąskaitoje yra daugiau pinigų, negu reikia kasdienėms išlaidoms, nustatyti operacijų apribojimus. Sudarant interneto banko sutartį, iš anksto nustatoma didžiausia pinigų suma, kurią galima išleisti naudojantis interneto banku. Juos vėliau galima pakeisti.
- Jungiantis prie interneto banko, reikia visuomet įsitikinti, kad tikrai esate reikiamame tinklalapyje. Svetainės adresą visada rinti patiems, nenaudoti nuorodų e. laiškuose, antraip rizikuojama patekti į suklastotą svetainę.
- Prisijungiant prie interneto banko visuomet atverti atskirą interneto naršyklės langą. Ryšys turi būti koduotas: svetainės adresas prasideda raidėmis *https://,* o šalia adreso ar naršyklės lango apačioje rodomas užrakintos spynelės ženklelis ar rakto simbolis.
- Prisijungiant prie interneto banko naudotis tiktai saugiais kompiuteriais. Namų ar darbo kompiuteryje turi būti įdiegta interneto užkarda, antivirusinė programa, programinė įranga turi būti atnaujinta.

- Netikėtu atveju – nedelsiant pranešti bankui.

Įsigyjant prekes ar paslaugas internetu, vengti svetainėse įvedinėti mokėjimo kortelės duomenis. Geriau naudotis žinomomis trečiųjų šalių paslaugomis.

Atsiskaitymams internetu naudoti atskiras kreditines korteles, o jose laikyti tik tiek pinigų, kiek reikia pirkiniui. Lietuvos bankai platina vien atsiskaitymui internetu skirtas nebrangias virtualias kreditines korteles.

Perkant prekes ir paslaugas internetu, reikia žinoti dar ir tokius dalykus:

- prieš įsigyjant prekę reiktų pasidomėti, kokiomis sąlygomis pardavėjas įsipareigoja priimti ar pakeisti netinkamą prekę. Paprastai vadovaujamasi Lietuvos Respublikos vartotojų teisių gynimo įstatymu. Jei kitaip nenustatyta, prekės garantinis laikas yra 6 mėnesiai;
- pirkėjas, registruodamasis elektroninėje parduotuvėje ar apmokėdamas pirkinį, pateikia savo asmeninius duomenis. Reikia atkreipti dėmesį, ar pardavėjas deklaruoja jų saugumą ir ar įsipareigoja laikytis ES ar Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nustatytų reikalavimų;
- pirkėjas vizualiai negali patikrinti siūlomų prekių išvaizdos ir kokybės, todėl reikia internete paieškoti daugiau informacijos ir nepriklausomų atsiliepimų apie pardavėją ir jo parduodamas prekes;
- nors internete siūlomos prekės dažniausiai kainuoja daug pigiau, tačiau išsiaiškinkite, kokios bus pašto išlaidos, importo PVM ir muitai. Neretai iš anksto neįmanoma nustatyti, iš kurios šalies bus siunčiamos prekės, todėl skaičiuojant nesunku ir apsirikti.

3.1.1.14. Duomenų apsauga kompiuteryje

Duomenys dažniausiai turi didesnę vertę, nei pats kompiuteris. Todėl verta daugiau dėmesio skirti jų saugumui. Duomenys gali būti prarasti įsiskverbus kompiuteriniam virusui, sugedus diskui, praradus kompaktinį diską, USB atmintinę, pagaliau ir patį kompiuterį. Įvairūs tyrimai rodo, kad pasaulyje kasmet pavagiama, pametama ar kitais būdais netenkama dešimčių tūkstančių nešiojamųjų kompiuterių. Todėl viena pagrindinių taisyklių tokių kompiuterių šeimininkams – reguliariai darykite atsargines kompiuteryje esančių svarbių duomenų kopijas. Ypač patartina tai atlikti prieš keliones, nes jų metu prarandama itin daug kompiuterių (pavyzdžiui, oro uostuose kartu su bagažu).

Atsargines kopijas, be abejo, reikia daryti į kitą laikmeną - įrašyti į kitą kompiuterį, USB atmintinę, CD ar DVD diskus: praradus kompiuterį ar sugedus kompiuterio diskui, atsarginė kopija

išlieka kitoje vietoje. Operacinėse sistemose būna specialios atsarginio kopijavimo priemonės, bet daugeliui vartotojų pernelyg sudėtinga jomis naudotis; tuomet tiks ir paprasčiausias dokumentų kopijavimas.

Jei nešiojamame kompiuteryje ar keičiamose laikmenose informacija yra konfidenciali, tuomet taip pat reikėtų pasirūpinti papildoma jos apsauga. Patikimiausia informaciją užkoduoti. Operacinės sistemos *Microsoft Windows* profesionaliose atmainose dokumentus galima užšifruoti, tačiau daug vartotojų naudojasi namams skirtomis atmainomis, kuriose to padaryti negalima. Be to, negalima koduoti keičiamose laikmenose ar serveriuose esančių dokumentų. Daugumoje įstaigų darbuotojams nerekomenduojama dokumentų laikyti savo darbo kompiuteriuose - jie saugomi gerai prižiūrimuose ir saugiuose bendruose kompiuteriuose - serveriuose.

3.1.2. Klausimyno sudarymo tyrimo rezultatai

Pagal EDCL fondo standartus sudarytas e-Guardian sertifikavimo programos klausimynas, iš pradžių lietuvių, paskui ir anglų kalba. Klausimyno dalys yra šios:

- Bendros saugumo užtikrinimo priemonės
- Kenkėjiškos programos (*malware*)
- Elektroninis bendravimas
- Saugus naršymas ir atsiskaitymai internete
- Vaikų saugumas

Toliau pateikiamas pilnas, pirmosios klausimyno versijos lietuviškas variantas:

1. Bendros saugumo užtikrinimo priemonės:

1.1. Mokėti sekti, gauti ir naudoti naujausius operacinės sistemos, papildomos programinės bei aparatūrinės įrangos ir saugos mazgų atnaujinimus. Suprasti šių atnaujinimų naudą.

1.2. Žinoti apie kelių asmenų naudojimosi vienu kompiuteriu galimybes. Suprasti, kas yra vartotojo asmeninis prisijungimo ir naudojimosi kompiuteriu vardas, bei kaip atskiriama skirtingų vartotojų informacija.

1.3. Žinoti, kompiuterinių sistemų duomenų saugumo problemų sprendimo būdus – tinkamos slaptažodžių sistemos naudojimą ir kt. Žinoti vartotoją identifikuojančio vardo reikšmę ir skirtumą tarp vartotojo vardo ir slaptažodžio. Suprasti prieigos teisių (angl. *access rights*) sąvoką ir žinoti jos svarbą.

1.4. Žinoti prisijungimo prie sistemos slaptažodžio reikalingumą, kad naudojant prisijungimo slaptažodžius, nepageidaujamiems asmenims apsunkinamas patekimas į sistemą. Mokėti sudaryti sudėtingus slaptažodžius. Žinoti kokia turi būti sudėtingo slaptažodžio sandara. Žinoti saugių slaptažodžių keitimo ir saugojimo taisykles.

1.5. Mokėti naudotis standartinėmis, pačioje OS integruotomis, apsaugos priemonėmis (*Firewall, Defender* ir t.t.)

1.6. Mokėti apsaugoti duomenis kompiuterio diske. Žinoti apie duomenų šifravimą, apsaugojimą slaptažodžiu. Žinoti kokios yra patikimos duomenų šifravimo programinės įrangos, bei kam jos naudojamos. Mokėti užkoduoti svarbius duomenis juos šifruojant.

1.7. Mokėti nustatyti ar duomenų laikmena turi slaptažodžio apsaugos galimybę apsisaugojimui nuo nepageidaujamos prieigos prie duomenų. Mokėti naudoti šiuos slaptažodžius apsaugai. Mokėti fiziškai apsaugoti *CD, DVD, USB* atmintines ir kitas išorines duomenų laikmenas nuo vagysčių ar sugadinimo.

1.8. Suprasti žalingų duomenų plitimo grėsmę nešiojamomis laikmenomis.

1.9. Žinoti duomenų bei programų atsarginių kopijų darymo keičiamose laikmenose tikslingumą ir reikšmę. Žinoti apie *Windows System Restore* priemonę. Mokėti naudotis minėtomis priemonėmis.

2. Kenkėjiškos programos (*malware*):

2.1. Suprasti skirtingų kenkėjiškų programų sąvokas (*viruses, trojan horses, spyware, dishonest adware, malicious software* ir kt.), naudojamus kompiuterijoje, ir suvokti jų skirtumus.

2.2. Žinoti, kada ir kaip kenkėjiškos programos gali patekti į kompiuterinę sistemą.

2.3. Žinoti, kas yra apsisaugojimo nuo kenkėjiškų programų programinė įranga.

2.4. Mokėti konfigūruoti programinę įrangą reguliariai ir automatiškai atsinaujinti kenkėjiškų programų definicijas. Mokėti diegti apsaugos pataisas (angl. *patches*). Žinoti, kam jos skirtos ir kaip parsisiųsti pataisas skirtingai programinei įrangai.

2.5. Žinoti, kaip elgtis ir kokia seka atlikti veiksmus jei įtariate, kad sistema apkrėsta. Suprasti apsaugos programos ribotumą. Žinoti ką reiškia „dezinfekuoti“ bylas (rinkmenas).

2.6. Suvokti, kad parsisiunčiant bylas ar atveriant elektroninių laiškų priedus reikia naudotis budinčia apsaugos programa, derėtų neatverti neaiškių nelauktų elektroninio pašto laiškų, neatverti tokių laiškų prieduose esančių bylų.

2.7. Suprasti kas yra nepatikimos duomenų laikmenos. Suprasti, kad negalima kompiuteryje naudoti nepatikimų *CD, DVD, USB* laikmenų, kuriuose gali būti kenkėjiški duomenys. Suprasti, kad

užkrėstų duomenų laikmenų naudojimas kompiuteryje gali įtakoti sistemos užkrėtimą, arba negrįžtamą sugadinimą.

3. Elektroninis bendravimas:

3.1. Žinoti apie *spam* tipo elektroninius laiškus ir elektroninius laiškus apkrėstus kenkėjiškomis programomis. Suvokti, kad *spam* laiškai tai ne vien vartotojo, bet ir elektroninio pašto paslaugos teikėjo klaidos.

3.2. Mokėti elgtis su elektroniniais laiškais iš nežinomų šaltinių. Žinoti apie programinę bei techninę įrangą skirtą filtruoti ir apsisaugoti nuo *spam* ir pavojingų elektroninių laiškų su kenkėjiškomis programomis.

3.3. Mokėti saugai elgtis naudojant momentinių žinučių sistemas.

4. Saugus naršymas ir atsiskaitymai internete:

4.1. Žinoti, apie priemones skirtas užtikrinti saugumui naršant internete (*cookies* blokavimas, *ActiveX* kontrolė ir kt.)

4.2. Žinoti internetinių *cookies* naudojimo privalumus, trūkumus ir pavojus.

4.3. Žinoti apie pavojus, kylančius pateikiant savo asmeninius duomenis internetiniuose puslapiuose. Žinoti apie spragas ir pavojus, tokius kaip galimybes piktavaliams pasinaudoti ar pavogti klientų informaciją.

4.4. Žinoti, kas yra tinklo šifravimo raktai, kokie jie būna ir mokėti jais naudotis.

4.5. Mokėti atskirti saugias pirkimo internete svetaines nuo nesaugių.

4.6. Mokėti saugiai naudotis pirkimo internetu galimybe. Atpažinti suklastotas prisijungimo prie internetinės bankininkystės svetaines. Mokėti saugiai naudotis elektroninės bankininkystės slaptažodžių generatoriumi ir slaptažodžių kortele.

4.7. Mokėti saugiai atlikti mokėjimus internetu naudojantis kredito ar mokėjimo kortelėmis. Mokėti naudotis atsiskaitymų mokėjimo ar kredito kortelėmis tarpininkų svetainėmis, atskirti patikimas paslaugas nuo *phishing*.

5. Vaikų apsaugojimas:

5.1. Žinoti, kaip pakalbėti su vaikais apie pavojus internete ir sužinoti informaciją, kuri vaikus trikdo.

5.2. Žinoti apie tinkle esančius pavojus: „plėšikus“, internetinį chuliganizmą, finansines suktybes, virusus, kibernetinius nusikaltimus, ir internete plintančią pornografiją, seksualinius priekabiavimus interneto pokalbių svetainėse ir elektroniniu paštu.

5.3. Žinoti sistemų stebėjimo būdus, kuriais galima stebėti vaiko naudojimąsi kompiuteriu. Mokėti naudotis programine įranga skirta kontroliuoti vaikų naudojimąsi internetu, operacine sistema bei programomis.

5.4. Žinoti, kokių tipų yra programinė įranga skirta vaikams apsaugoti.

5.5. Mokėti naudotis interneto turinio filtravimo priemonėmis integruotomis naršyklėse.

5.6. Suprasti, kokią reikia naudoti programinę įrangą apsaugojimui. Kas yra kokybiška antivirusinė, anti-spyware, spam blokavimo, ugniasienės programinė įranga ir kaip ja naudotis, bei atsinaujinti.

5.7. Mokėti kombinuoti kelias apsaugojimo priemones.

5.8. Žinoti, kokios yra paieškos svetainės skirtos vaikams ir kokios paaugliams.

5.9. Žinoti, kokie yra saugūs vaikams mobilieji telefonai.

6. Advanced dalis:

6.1. Ugniasienės naudojimas:

6.2. Mokėti naudotis ugniasiene. Jei ugniasienės nėra, mokėti ją parsisiųsti.

6.3. Mokėti naudotis informavimais, kuriuos siunčia apsisaugojimo programinė įranga.

6.4. Mokėti saugiai keistis bylomis, naudotis bylų saugumo patikrinimo priemonėmis.

6.5. Nešiojami kompiuteriai:

6.6. Prižiūrėti savo kompiuterio naudojimosi tvarką. Neleisti naudotis Jūsų sistema asmenims, kuriais pilnai nepasitikite. Nesuteikti nepažįstamiems prieigos prie Jūsų sistemos, kad neatliktų pavojingų veiksmų.

6.7. Žinoti kaip fiziškai apsaugoti nešiojamąjį kompiuterį nuo vagysčių. Būti susipažinusiam su nešiojamųjų kompiuterių užraktais, kurie apsunkina vagystes.

6.8. Žinoti kas yra kompiuterio BIOS slaptažodis ir kam jis naudojamas. Žinoti kaip BIOS slaptažodis įjungiamas kompiuteriui startavus ir kokios slaptažodžio praradimo pasekmės.

6.9. Žinoti apie kylančius pavojus, naudojantis nekoduotais bevieliais tinklais.

6.10. Mokėti naudotis bevielio interneto tinklais. Žinoti kas yra saugūs bevieliai tinklai, kokie yra bevielio interneto saugumo standartai (IEEE802.11a, IEEE802.11b, IEEE802.11g ir kt.) ir šifravimo algoritmai. Žinoti kas yra WEP ir WPA bevielio tinklo apsaugos būdai. Mokėti apsaugoti savo bevielį tinklą WEP ar WPA raktais.

6.11. Suprasti kodėl verta savo bevielį tinklą atjungti, jei jis nereikalingas naudojimui ilgesnį laiką, žinoti grėsmes.

6.12. Namų tinklo įranga: plačiajuosčiai maršrutizatoriai, bevielės tinklo stotelės:

6.13. Žinoti kas yra interneto protokolas, TCP/IP ir UDP. Žinoti kas yra TCP/IP ir UDP portai, kam jie naudojami ir kokie jie būna.

6.14. Žinoti kas yra aparatūrinės ugniasienės ir kam jos naudojamos. Mokėti naudoti aparatūrines ugniasienes.

6.15. Žinoti kas yra WEP ir WPA bevielio tinklo apsaugos būdai. Mokėti apsaugoti savo bevielį tinklą WEP ar WPA raktais.

6.16. Žinoti kas yra administracinis tinklo slaptažodis. Mokėti pasikeisti administracinį slaptažodį, kuris suteikiamas pagal nutylėjimą gamintojo. Žinoti koks turi būti geras administracinis slaptažodis.

6.17. Suprasti kodėl verta naminį tinklą atjungti, jei jis nereikalingas naudojimui ilgesnį laiką, žinoti grėsmes.

6.18. Mokėti naudotis sekimo priemonėmis, kurios integruotos tinkliniuose įrenginiuose ir skirtos Jūsų įrenginiu besinaudojančių sistemų sekimui. Mokėti pastebėti įtartinus veiksmus su Jūsų tinkle.

Kaip matome, pradinėje klausimyno versijoje dar buvo ir šešta – sudėtingesnių įgūdžių ir žinių dalis, kuri vadinosi *Advanced*, tačiau vėliau, pasikonsultavus su sertifikuojamos srities ekspertais, ši dalis buvo panaikinta, nusprendus, kad ji pakankamai sudėtinga šio lygio sertifikavimui.

Galutinė e-Guardian sertifikavimo programos klausimyno versija yra anglų kalba, kadangi produktą norima standartizuoti ECDL fonde ir pritaikyti ne tik Lietuvos rinkai. Pirmosios šios tyrimo dalies galutinis rezultatas – klausimynas anglų kalba, pateiktas 1 lentelėje.

1 lentelė

e-Guardian klausimynas anglų kalba

1.	**Common means for safety assurance:**
1.1.	Know how to follow, download and use updates for your operating system, additional software and security components. Understand the benefits of these updates.
1.2.	Know multiple user account. Understand what a personal user account is and how information of different users is separated.
1.3.	Understand the purpose of a user name, and the difference between user name and user password. Understand the meaning and importance of access rights
1.4.	Know the necessity of login to system password, and the usage of login passwords
1.5.	Be able to make complex password. Know the structure of a complex password and the rules for changing and keeping passwords.
1.6.	Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Defender, etc.).
1.7.	Be able to protect data on computer disk. Know about data encryption and password protection.

1.8.	1 Lentelės tęsinys Know how to find out whether a data media has a password protection possibility, used for protecting against unwanted data access. Be able to use these passwords for protection. Be able to protect CD, DVD, USB memory and other external data media.
1.9.	Understand the threat of malicious data spread in external data medias.
1.10.	Understand the benefits and purpose of data and software backups.
1.11.	Know who you should contact if you discovered or suspect that data can be classified as illegal or dangerous.
2.	**Malicious software :**
2.1.	Understand different malicious software (viruses, Trojan horses, spyware, dishonest adware, etc.) definitions and differences.
2.2.	Know when and how malicious software can get into computer system.
2.3.	Know what security software is used to protect against malware.
2.4.	Be able to configure software to automatic and regular update.
2.5.	Know what has to be done and in what order, if you suspect that computer system is infected. Understand the limitation of security software.
2.6.	Understand that an active version of security software should be running when downloading files or opening email attachments.
2.7.	Know that unknown and unwanted emails and their attachments should not be opened.
2.8.	Understand what is unsafe data media. Understand that unsafe CD, DVD, USB memory media should not be used.
3.	**Electronic messages :**
3.1.	Know about email that is classified as spam, and email messages infected with malware.
3.2.	Be aware of privacy protection legal act.
3.3.	Know how to redirect children email to your account.
3.4.	Know how to reject email from specific email addresses.
3.5.	Know how to block private messages between a child and another user.
3.6.	Know how to treat email messages from unknown senders.
3.7.	Know how to treat securable with instant messaging.
3.8.	Be aware of mobile phone capabilities.
4.	**Securable web browsing and paying on internet :**
4.1.	Know about tools that ensure safety when browsing the internet (blocking of cookies, ActiveX control, etc.).
4.2.	Know about advantages, disadvantages and dangers of internet cookies.
4.3.	Know about threats associated with the personal data disclosure.
4.4.	Know about gaps and threats, such as possibilities for evil-minders to use or steal client information.
4.5.	Know about encryption keys used on internet, know about types of encryption keys and how to use them.
4.6.	Be able to distinguish safe/genuine online transaction/commerce sites from unsafe.
4.7.	Be able to perform online transaction using credit or debit cards.
4.8.	Know how to contact service administrator while required.
4.9.	Know who to contact if you discovered or suspect dangerous or illegal content.

1 Lentelės tęsinys

5.	**Children safety:**
5.1.	Understand that open communications between parent and children is important to keeping children safe.
5.2.	Know about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet.
5.3.	Know about system monitoring types and be able to monitor use of computer.
5.4.	Be able to access temporary internet files and browser history.
5.5.	Be able to use software to control children use of internet, operating system and software.
5.6.	Know about children protection software.
5.7.	Be able to use internet content filtering tools integrated on web browsers.
5.8.	Know what defensive software is.
5.9.	Know what a quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use it.
5.10.	Be able to access the chat, instant messenger history.
5.11.	Be able to contact service administrator.
5.12.	Know about recommended kid directories, search sites geared for children and targeted at teenagers.

Šaltinis: Sudaryta Autoriaus

3.1.3. ECDL-F standartų atitikimo patvirtinimo paraiškos formos ruošimo tyrimo rezultatai

Sudarius klausimyną, pagal ECDL fondo partnerinės programos standartizavimo procedūrą, parengta sertifikavimo programos e-Guardian standartizavimo ECDL fonde patvirtinimo paraiškos forma. Užpildyta forma pateikta ECDL fondo tvirtinimui. Pilna patvirtinimo paraiškos forma pateikta 3 priede.

3.1.4. Testo klausimų bazės sudarymo tyrimo rezultatai

Gavus ECDL fondo klausimyno patvirtinimą, sudaryti e-Guardian testo klausimai skirti automatizuotam testavimui. Pirmojo tipo klausimų (klausimas su keturiais atsakymo variantais, iš kurių vienas arba daugiau teisingų) AQTB yra 85 %, antrojo (klausimai su atsakymo imitavimu) - 15 %. Sudaryti klausimai, prieš talpinant į testavimo serverį, surašyti į standartizuotą formą, kurios pavyzdys pateikiamas 4 paveiksle. Kiekvienai e-Guardian sertifikavimo programos klausimyno sričiai sudaryta bent po 4 klausimus. Testo klausimų turinys sudarytas, kaip įmanoma mažiau priklausomas nuo

kompiuterinės platformos, operacinės sistemos ar konkrečios programinės įrangos, bei aplikacijos. Klausimų turinys atitinka, šiam laikotarpiui būdingas, aktualias IT tendencijas, naujoves, bei žinias. Visi e-Guardian sertifikavimo programos testo klausimai pateikiami 6 priede.

3.2. e-Guardian testo klausimų bazės modifikavimo tyrimas

Tyrimo tikslas – nustatyti bei įvertinti e-Guardian sertifikavimo programos klausimyno ir testo klausimų bazės klaidas, modifikuoti klausimyną ir automatinio testavimo testo klausimų bazę.

Tyrimas atliekamas dviem etapais. Pirmajame etape apklausiami sertifikuojamos srities ekspertai, o antrojoje – bandomąjį sertifikavimo sistemos testą laikę sertifikavimo srities specialistai. Gauti apklausos rezultatai leistų įvertinti, kaip testų sudarymo, kokybės, bei kompiuterinių sistemų saugos ekspertai bei specialistai vertina e-Guardian sertifikavimo programos reikalingumą, klausimyno tinkamumą, bei sudarytų automatizuoto testavimo klausimų bazės klausimų tikslumą ar klaidas. Pagal gautus rezultatus būtų modifikuojama testo klausimų bazė. Antrajame etape pakoreguota bandomoji sertifikavimo sistemos testo klausimų bazė talpinama į testavimo serverį. Bandomąjį testą duodama laikyti sertifikavimo srities specialistams ir iš laikančiųjų surenkami atsiliepimai, pagal kuriuos testo klausimai vėl koreguojami, tikslu paruošti galutinę klausimų bazės versiją.

Tyrimo tikslui pasiekti iškeliami tokie uždaviniai:

1. Sudaryti apklausos anketą šio tyrimo tikslui išsiaiškinti.

Šios tyrimo anketos tikslas yra išsiaiškinti ekspertų nuomonę apie e-Guardian programos reikalingumą, klausimyno ir testo klausimų bazės tikslumą. Bus sudaryta klausimų anketa.

2. Parinkti ekspertus.

Šis darbas atliktas konsultuojantis su ECDL padalinio Lietuvoje vadovu ir naudojantis oficialiu ECDL kontaktų sąrašu. Ekspertų sąrašas perduotas ECDL fondui ir gautas patvirtinimas.

3. Išplatinti anketas ir klausimų bazę ekspertams.
4. Apdoroti gautus iš ekspertų duomenis.
5. Išsiaiškinti, ar ekspertai patvirtina sertifikavimo programos reikalingumą.

Pagal gautus rezultatus nustatyti ekspertų nuomonę apie programos reikalingumą.

6. Išsiaiškinti ekspertų nuomonę apie klausimyno tinkamumą.

Pagal gautus rezultatus nustatyti ekspertų nuomonę apie klausimyno tinkamumą.

7. Išsiaiškinti, kokie testo klausimai turėtų/galėtų būti pataisyti ar pakeisti.

Pagal gautus rezultatus nustatyti ekspertų nuomonę apie testo klausimų bazės tikslumą ir klaidas.

8. Pateikti tyrimo metu padarytas išvadas ir jomis remiantis koreguoti sertifikavimo programos testo klausimų bazę.

9. Pakoreguotą sertifikavimo sistemos testo klausimų bazę patalpinti testavimo serveryje, kaip bandomąją sertifikavimo testo versiją.

10. Bandomąjį testą duoti laikyti sertifikavimo srities specialistams ir surinkti iš laikančiųjų atsiliepimus apie testo klausimus.

11. Pagal gautus atsiliepimus koreguoti testo klausimų bazę, kad paruošti galutinę versiją ECDL fondo tvirtinimui.

Tyrimo imtis – 13 ekspertų iš kelių skirtingų sričių susijusių su testų sudarymu, testų kokybe, bei kompiuterinių sistemų saugumu ir 60 sertifikavimo srities specialistų. ECDL fondo patvirtinti ekspertai:

- Frank Mockler – programų plėtros vadybininkas, ECDL fondas.
- Bryan Donovan – testų tvirtinimo vadovas, ECDL fondas.
- Piotr Mrozinski – regiono plėtros vadovas. ECDL fondas.
- Dr. Radoslav Yoshinov – Bulgarijos Mokslų Akademijos Telematikos laboratorijos direktorius, ECDL Bulgarija.
- Dr. Mara Jakobsone – Latvijos informacijos ir komunikacijos technologijų asociacijos viceprezidentė, ECDL Latvija.
- Dr. Jan Raszewski – ECDL fondo atstovas Lenkijoje, ECDL Lenkija.
- Renata Danielienė – programų plėtros vadybininkė, ECDL Lietuva.
- Tomas Lygutas – testavimo sistemos administratorius, ECDL Lietuva.
- Doc. Stasys Maciulevičius – sistemų analitikas (atsakingas už testų kokybę), ECDL Lietuva.
- Doc. Steponas Jonušauskas – testavimo kokybės inspektorius, ECDL Lietuva.
- Doc. Alfredas Otas – sistemų analitikas, ECDL Lietuva.
- Darius Janušauskas – techninės ir programinės įrangos skyriaus vadovas, UAB „Sekasoft“.
- Ramūnas Berulis – sistemų administratorius, UAB „Sekasoft“.

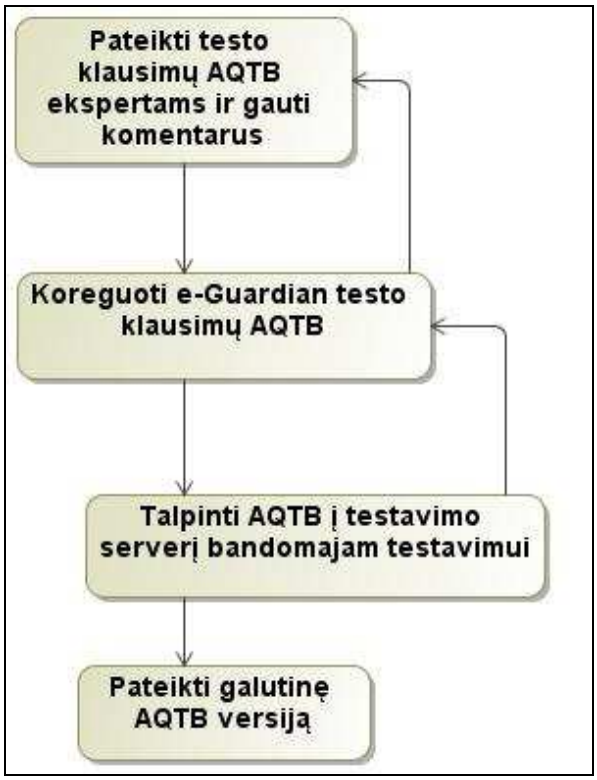
Tyrimo metodai. Šiam tyrimui buvo taikomas kiekybinis ir kokybinis tyrimo metodai – anketinis metodas, priskiriamas prie sociologinių tyrimo metodų, apklausa, palyginimo metodas.

Analizuojat ir vertinant tyrimo rezultatus taip pat taikytas dokumentų analizės metodas, kartu su tyrimo rezultatais interpretuojant statistinę medžiagą. Klausimų bazės koregavimui buvo taikomas metodas aprašytas 2.3. darbo dalyje.

Sudarant anketą buvo atsižvelgta, kad respondentai turi daug žinių ir yra gerai nusimanantys ekspertai sertifikuojamoje srityje, todėl anketa yra trumpa, paprasta ir aiški. Anketoje yra trys klausimai. Pirmajame klausiama apie e-Guardian programos reikalingumą (atsakymas turi būti pateikiamas stiprumo balais 5 balų skalėje ir prašoma pateikti paaiškinimą). Antrasis klausimas apie e-Guardian klausimyno tikslumą (atsakymas turi būti pateikiamas stiprumo balais 5 balų skalėje ir prašoma pateikti paaiškinimą). Trečiasis klausimas apie e-Guardian testo klausimų bazės tikslumą (atsakymas turi būti pateikiamas stiprumo balais 5 balų skalėje ir prašoma pateikti paaiškinimą, taip pat prašoma testo klausimų lentelėje pridėti komentarus ir pastebėjimus, jei tokie reikalingi). Tyrimo apklausos anketos kartu su e-Guardian testo klausimų bazėmis, buvo pateiktos ekspertams elektronine forma. Anketos forma pateikta priede nr. 5.

Tyrimo rezultatai leis įvertinti paruoštų sertifikavimo sistemos klausimyno ir automatinio testavimo testo klausimų bazės tinkamumą ir tikslumą, bei apskritai e-Guardian sertifikavimo reikalingumą.

Pagal ekspertų pastabas pakoreguoti AQTB testo klausimų bazės klausimai talpinami į testavimo serverį. Bandomąjį testą laikys sertifikavimo specialistai ir pateiks atsiliepimus elektroniniu paštu. Pagal atsiliepimus AQTB testo klausimų bazės klausimai koreguojami ir ruošiama galutinė klausimų bazės versija. Tyrimo veiklos diagrama pateikiama 7 paveiksle.



Šaltinis: Sudaryta autoriaus

Pav. 7 Tyrimo veiklos diagrama

Tyrimo organizavimas. Tyrimo metu buvo apklausta 13 ekspertų. Kadangi ekspertai ne visi lietuvių tautybės, tai apklausos anketa, paruošta anglų kalba, išplatinta respondentams elektroniniu paštu. Apklausos pradžia 2008 12 08, o paskutinė užpildyta anketa gauta 2009 01 12. Klausimų bazė pagal ekspertų komentarus pakoreguota iki 2009 03 06 ir patalpinta į testavimo serverį bandomajam testavimui 2009 03 13. Iki 2009 04 30 bandomąjį testą buvo laikę 60 sertifikavimo srities specialistų. Nuo bandomojo testo paleidimo iki 2009 05 07, pagal laikiusiųjų atsiliepimus, testo klausimų bazė buvo koreguojama, klausimus koreguojant pačiame testavimo sistemos serveryje. Vėliau galutinė klausimų bazės versija paruošta ECDL fondo tvirtinimui.

Tyrimo rezultatai.

Gavus iš ekspertų užpildytas anketas, didžiausias dėmesys buvo skirtas testo klausimų bazėje parašytiems komentarams ir pastaboms. Pagal juos, tyrimo metu, atliktas pagrindinis uždavinys – atsižvelgus į ekspertų pastabas, testo klausimų bazę pataisyti ir paruošti bandomąją jos versiją talpinimui į bandomąją testavimo sistemą.

Paveiksle nr. 8 pavaizduota kokiu būdu buvo pateikti ekspertų komentarai. Gavus testo klausimų bazes su komentarais iš visų ekspertų, buvo sukurta apjungta testo klausimų bazė. Jeigu venas elementas komentuotas kelių ekspertų – paliekami visi komentarai. Pagal ekspertų pastabas testo klausimų bazės klausimai buvo koreguojami, pertvarkomi arba pergalvojami. Pakeistoji testo klausimų bazė dar kartą pateikiama ekspertams, tam kad patvirtintų pataisytą versiją. Bandomoji testo klausimų bazės versija per specializuotą klausimų redaktorių patalpinta į ECDL automatizuoto testavimo serverį Lietuvoje.

Suskaičiavus ekspertų užpildytų anketų rezultatus apibendrinti rezultatai. Iš 204 esančių testo klausimų komentarai, pastabos, taisymai pateikti 45 klausimuose. Tai sudaro 22% visų testo klausimų. Pirmajame klausime apie e-Guardian reikalingumą, 12 iš 13 ekspertų programą įvertino kaip labai aukšto prioriteto, likusis suteikė aukštą prioritetą. Klausimyno tikslumas surinko 10 aukščiausių įvertinimų ir 3 aukštus. Testo klausimų bazė gavo 10 aukščiausių, 2 aukštus ir vieną vidutinį įvertinimą. Ekspertų užpildytų anketų rezultatų grafinė statistika pateikiama 9 paveiksle.

ECDL Lietuva testavimo sistemoje http://www.ecdl.lt/EN/ECDL.nsf [37] patalpintą bandomąją sertifikavimo sistemos versiją duota laikyti sertifikavimo srities specialistams. Specialistus parinko darbo autorius ir Lietuvos ECDL atstovybė – Informacinių technologijų institutas. Specialistai, laikiusieji testą, elektroniniu paštu pateikė atsiliepimus su iškilusiais neaiškumais ir pastebėtomis testo klausimų klaidomis. Gautų atsiliepimų pavyzdys pateiktas 7 priede. Pagal atsiliepimus testo klausimų bazė buvo dar kartą koreguojama, tik šį kartą, jau tiesiogiai testavimo sistemos serveryje. Paruošta galutinė klausimų bazės versija.

3.3. Know how to redirect children email first to your account.							
	92.	3.3.	~~Is it possible to review~~ What statistical information about child's email can be reviewed ~~, such as: whether email was sent or received, who sent it, who received it and so on~~?		~~Yes~~ ~~No~~Date of receiving Sender email Size of message All answers are correct		
	93.		Which information about child's email can you see by using parental software?		The date and time the email was sent or received, The subject, The contents and any attachments All options above		
	94.		If you want to redirect e-mail messages from one mailbox to another in Windows Mail program, ...		You should create email rule It is possible only during creation of email account in your program You should change your email account configuration by choosing Tools>Options It is not possible		
	95.		How can you redirect e-mail messages from one mailbox to another?		Use third party software that is designed to redirect e-mail messages. Log in to the mailbox, open the particular message and forward it to another e-mail address.) (Ask system administrator for help configuring your email) All answers above are correct		
3.4. Know how to reject email from specific email addresses.							

Comment [FM34]: It would be better to keep to one format of multiple choice question (e.g. four options – three incorrect, one correct).

Formatted: Font color: Red, Highlight

Formatted: Font color: Red

Formatted: Font color: Auto

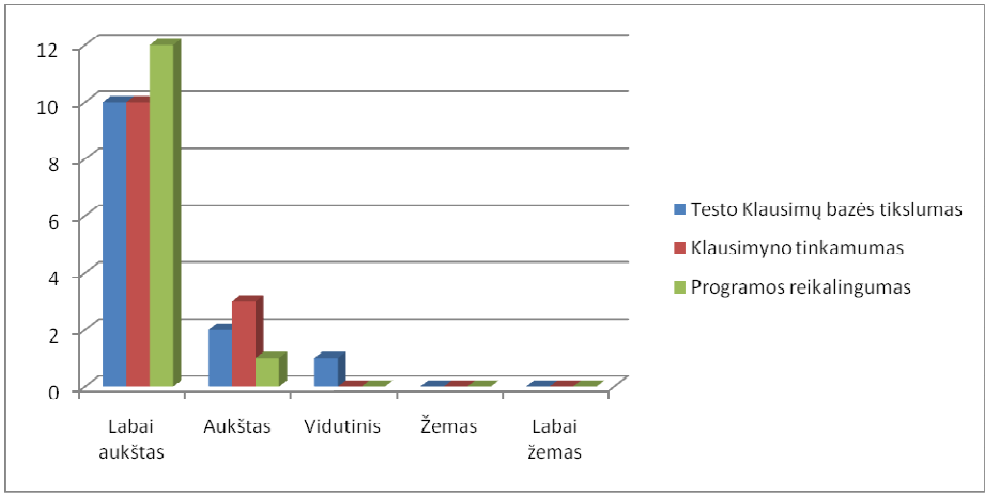
Comment [FM35]: It's better to have only one correct response.

Comment [FM36]: This is not necessarily wrong.

Formatted: Font color: Red

Šaltinis: sudaryta autoriaus.

Pav. 8 Ekspertų komentarai testo klausimų bazėje



Šaltinis: sudaryta autoriaus.

Pav. 9 Ekspertų užpildytų anketų rezultatų statistika

3.3. Pasiūlymai tolimesniam e-Guardian programos vystymui

Šiuo metu bandomoji e-Guardian sertifikavimo programos versija patalpinta ECDL Lietuva testavimo sistemoje ir surinkti rezultatai iš 60 testą laikiusiųjų sertifikavimo srities specialistų. **Tolimesnio tyrimo tikslai** – atlikti laikytų testų rezultatų statistinę analizę, sukurti naują e-Guardian testo rezultatų vertinimo metodą, pateikti pasiūlymus ECDL fondui dėl pekeitimų partnerinių programų kokybės valdymo sistemoje.

1. Dabartinis testo vertinimas atitinka ECDL standarto leidžiamus automatizuoto testų vertinimo kriterijus. Testas išlaikomas teisingai atsakius į 80% testo klausimų. Kiekvieno klausimo teisingo atsakymo svorinis koeficientas yra 1. Naujo vertinimo metodo idėja yra suteikti didesnius svorinius koeficientus 4 ir 5 klausimų sritims ir sumažinti 1-3. Tokiu būdu didesnis dėmesys būtų skiriamas vaikų saugumo ir saugumo internete sritims, o mažesnis – klausimams apie bendrąsias saugumo užtikrinimo priemones.

2. Atlikus papildomus bandomuosius testavimus eilėje Europos šalių ir įvertinus jų rezultatus, siūloma keisti testavimo laiko (mažinant) ir išlaikymo balo parametrus.

3. ECDL partnerinio produkto patvirtinimo standartai sudaryti rankinio testavimo atvejui ir juose nagrinėjamas MQTB sudarymas. e-Guardian programa yra pirmoji ECDL fondo patvirtintos partnerinės programos statuso siekianti programa, naudojanti testavimo sistemą ir AQTB. Magistrinio darbo metu nebuvo galima aklai sekti ECDL fondo kokybės valdymo sistemos standartais, bet reikėjo taikyti juos kūrybiškai, derinant su ECDL fondo ekspertais. Siūlymas ECDL fondui tiesiogiai modifikuoti produktų patvirtinimo standartus automatizuoto testavimo atvejui ir apiforminti tai kokybės valdymo sistemoje.

IŠVADOS

1. Internetas vis giliau ir plačiau skverbiasi į mūsų kasdieninį gyvenimą. Pagrindiniai vartotojai tampa vaikai ir nepilnamečiai. Yra žinoma daug mokymo programų skirtų apsaugoti vaikus nuo interneto grėsmių. Jų reikšmę pervertinti yra sunku. Tai liudija ypač didelis Europos komisijos dėmesys vaikų saugumo internete problematikai.

2. E-Parent klasės mokymo programos moko kaip apsaugoti duomenis, kompiuterinę programinę ir aparatūrinę įrangą, bei vaikus naudojančius internetą, tačiau sertifikavimo programų nėra sukurta.

3. Būtina sukurti sertifikavimo programą, kurios pagrindinis tikslas - tiesiogiai padėti organizacijų, susijusių su vaikų ugdymu, darbuotojams bei tėvams įgyti žinias, reikalingas apsaugoti vaikus nuo grėsmių virtualiame pasaulyje ir patvirtinti tai atitinkamu bendraeuropiniu sertifikatu.

4. Kuriama vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programa e-Guardian autorizuojama ECDL fonde kaip patvirtinta partnerinė programa (Endorsed Partner Programme), todėl ji turi būti kuriama anglų kalba, siekiant kuo platesnio jos panaudojimo ir galimo adaptavimo.

5. Magistrinio darbo metu paruoštas vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programos klausimynas. Paruošta patvirtinimo paraiškos forma ir pateikta ECDL fondui. Gautas patvirtinimas, jog e-Guardian programa yra užregistruota kaip siekianti patvirtintos partnerinės programos statuso, rodo jog e-Guardian svarba yra ypač didelė ir jos reikalingumas neginčytinas.

6. Pagal sudarytą vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programos e-Guardian klausimyną sudaryta testo klausimų bazė automatizuotam testavimui. Testo klausimų bazė buvo pateikta ECDL fondo patvirtintiems probleminės srities ekspertams. Gavus ir įvertinus ekspertų pastabas, buvo atliktas testo klausimų bazės koregavimas. Tai patvirtina klausimyno ir testo klausimų bazės atitikimą ECDL fondo kokybės valdymo standartams.

7. e-Guardian sertifikavimo programos bandomoji versija patalpinta ECDL Lietuva testavimo sistemoje. Gauti atsiliepimai iš daugiau kaip 60 sertifikavimo srities specialistų. Tai patvirtina testo klausimų bazės kokybiškumą.

8. ECDL Lietuva vadovybei pateiktas siūlymas realizuoti naują e-Guardian vertinimo metodą įvedant didesnius klausimų vertinimo svorio koeficientus vaikų saugumo ir interneto saugumo klausimyno dalims.

9. ECDL fondui pateiktas siūlymas modifikuoti partnerinių produktų patvirtinimo dokumentaciją automatizuoto testavimo atvejui.

10. Rezultatų aprobavimą liudija 2 straipsniai, internetinė publikacija ir 3 pranešimai konferencijose:

- Straipsnis “e-Guardian Programme – The new ECDL Endorsed Product Proposal from ECDL Lithuania”, kuris kartu su bendraautoriumi Eugenijumi Telešiumi pristatytas tarptautinėje mokslinėje konferencijoje “Strategies, Media, and Technologies in European Education Systems”.
- Padarytas pranešimas “e-Guardian Certification Programme Pilot in Lithuania” tarptautiniame forume „Baltic IT&T 2009: eBaltics“, sekcijoje “Secure Future Internet Solutions“ kartu su bendraautoriumi Eugenijumi Telešiumi.
- Magistrantų ir doktorantų mokslinėje konferencijoje „IT 2009“, sekcijai „Informacinės technologijos mokyme“ pristatytas straipsnis „E-Guardian – the New Certification Programme on Skills of Ensuring Children Safety Using Internet“.

Preliminarus magistrinio darbo planas

VILNIAUS UNIVERSITETAS
KAUNO HUMANITARINIS FAKULTETAS
INFORMATIKOS KATEDRA

VERSLO INFORMATIKOS MAGISTRANTŪROS PROGRAMOS
MOKSLO TIRIAMOJO DARBO PLANAS

Magistrantas Mantas Lukoševičius. Tel.: 8-600-79744

Magistrantūros trukmė nuo 2007 m. iki 2009 m.

TEMA: Vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programos tyrimas

Vadovas: Eugenijus Telešius, daktaras, Vilniaus Universitetas Kauno Humanitarinis fakultetas.

Darbo anotacija:

Tikslas: anglų kalba sukurti vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programą e-Guardian, turint tikslą ją autorizuoti ECDL fonde.

Uždaviniai

- Išnagrinėti esamas ECDL sertifikavimo programas orientuojantis į specializuotų programų turinį.
- Išnagrinėti naujų ECDL programų kūrimo standartus.
- Sukurti, kiek galima labiau nuo aparatūrinės platformos ir PĮ nepriklausomą e-Guardian sertifikavimo programos klausimyną (syllabus).
- Sukurti e-Guardian sertifikavimo programos testų klausimų bazę automatizuotam testavimui (AQTB).
- Įkelti e-Guardian sertifikavimo testo klausimų bazę naudojimui ECDL Lietuva testavimo sistemoje.

- Ištirti e-Guardian klausimyno ir testo klausimų bazės atitikimą ECDL fondo kokybės valdymo sistemos reikalavimams.

Laukiami rezultatai: sukurta vaikų saugumo internete užtikrinimo įgūdžių sertifikavimo programa e-Guardian ir patalpinta ECDL Lietuva testavimo sistemoje.

Mokslo – tiriamojo darbo planas

Semestras	**(data)**	**Užduotys**
S1	2007 09 01 – 2008 01 01	Literatūros apie tiriamą sritį rinkimas ir analizė.
S2	2008 02 01 – 2008 06 01	ECDL-F programų kūrimo kokybės valdymo standartų analizė. Programos klausimyno sudarymas.
S3	2008 09 01 – 2009 01 01	Testo klausimų bazės sudarymas. Klausimyno ir testo klausimų bazės atitikimo ECDL-F kokybės valdymo sistemos reikalavimams tyrimai.
S4	2009 02 01 – 2009 06 01	Testo klausimų bazės talpinimas ECDL testavimo sistemoje. Apibendrinimas, išvados, darbo užbaigimas.

Magistrantas: ..... Vadovas .....

(parašas) (parašas)

LUKOŠEVIČIUS, Mantas. (2009) *Research of the Certification Programme on Skills of Ensuring Children Safety Using Internet.* MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty of Humanities, Department of Informatics. 82 p.

SUMMARY

The main purpose of the paper is to develop a certification programme on Skills ensuring children safety using Internet. In order to acheve this goal, five tasks were formed:

- *Explore current ECDL certification programmes aiming to specialized programmes.*
- *Explore the standards of new ECDL programmes developement.*
- *Develop the e-Guardian programme syllabus which would be as much hardware platform and software independent as possible.*
- *Develop the e-Guardian certification programme questions test base for automotive testing.*
- *Place the e-Guardian certification programme questions test base on the ECDL-Lithuania testing system.*
- *Examine ECDL Foundation quality management requirements of the e-Guardian syllabus and AQTB.*

To achieve these tasks such research methods as nonfiction analysis and summation, expert and user surveys, observation, experiments, statistical analysis were used. The theoretical part explores ECDL certification programmes, ECDL programme development standards, e-Guardian programme part among the ECDL Foundation products. The methods for developing ECDL programmes are described in second part. These methods include ECDL Foundation product authorization standards, certification programme syllabus and questions test base development. Third part includes descriptions of the two researches. e-Guardian syllabus and questions test base are developed in the first of them and corrections for the test base questions are made in the second research by making a survey with experts. Experiment results are used for developing questions test base. The main results are:

- *Current specialized ECDL certification programmes reviewed.*
- *New specialized ECDL Foundation programme development standard and quality management system analysis is made, e-Guardian programme part among the ECDL Foundation programmes is set.*
- *The certification Programme syllabus is developed.*
- *Questions test base is developed according to the syllabus.*
- *e-Guardian product endorsement standards form is filled and given for the ECDL Foundation, which agreed with e-Guardian being very important.*
- *The trial version of the certification programme is placed on ECDL-Lithuania testing system in order to estimate testing characteristics and valuation parameters. Researches are made proving quality of the certification programme syllabus and questions test base.*

Learning programmes teach how to protect computer data, software and hardware, also children using Internet, but there are no certification programmes developed. The e-Guardian is aiming to become ECDL Foundation endorsed certification programme on skills of ensuring children safety using internet. The programme‘s syllabus and questions test base is now developed, endorsement form is filled and given to the ECDL Foundation, which recognized e-Guardian as a very important certification programme seeking ECDL endorsement.

The volume of the paper is 82 pages. In the main parts there are 1 table and 9 pictures.

LITERATŪROS SĄRAŠAS

1. ePractice.eu: Prague Declaration on 'Safer Internet for Children' [interaktyvus] [Žiūrėta 2009 gegužės 3 d.]. Prieiga per internetą: <http://www.epractice.eu/en/library/289517>;
2. PARSHALL, C. G.; SPRAY, J. A.; DAVEY T. (2002) Practical Considerations in Computer-Based Testing. New York: Springer, p. 50-105.
3. MACIULEVIČIUS, Stasys; LYGUTAS, Tomas. (2007) ECDL testavimo sistemos naudojimo patirtis ir tobulinimo galimybės. *Informacijos mokslai*, Vilnius 2007 42–43, p. 103-107. ISSN 1392-0561.
4. BARTRAM, D.; HAMBLETON, R. (2006) Computer-Based Testing and the Internet: Issues and Advances. John Wiley & Sons Ltd p. 9-29. ISBN: 978-0-470-01721-0.
5. THOMPSON, A.T. (2008) A Proposed Framework of Test Administration Methods. *Journal of Applied Testing Technology*. Vol. 9, p. 15-21.
6. LUECHT, R. M. (2006) Operational Issues in Computer-Based Testing. John Wiley & Sons Ltd, p. 91-115.
7. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2008) Analysis of Computer-based Testing Systems. *Conference on Human System Interaction*. May 25-27, Krakow, Poland. IEEE Catalog Number 08EX1995C. Library of Congress: 2007905110, p.15-20. ISBN 1-4244-1543-8.
8. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2008) Time of Revolution in Computer–based Testing: The Innovative Solutions of the Lithuanian ECDL TestEngine. The 12th International Conference *"Information Technologies and Telecommunications in the Baltic Sea and CEE Region"*
9. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2006) Research of a typical e-services based ECDL testing infrastructure. *Technologie i bezpieczenstvo.* Polskie Towarzystwo Informatyczne, p. 111-122. ISBN 978-83-922646-5-1.
10. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2005) ECDL testavimo sistemos formalizavimo problemos. *Mokslo darbai*. Informacijos mokslai, 34 tomas p. 13-17. ISSN 1392-0561.
11. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2005) ECDL testavimo sistemos analizė ir sistemos darbo apkrovimo valdymas. *Informacinės technologijos verslui – 2005.* Tarptautinės konferencijos pranešimų medžiaga. Vilniaus universiteto Kauno humanitarinis fakultetas. 2005, p. 118-121.

12. DANIELIENĖ, Renata; TELEŠIUS, Eugenijus. (2004) ECDL testavimo sistemos administravimo veiklos procesų reinžinierijos aspektai. *Informacinės technologijos verslui – 2004.* Konferencijos pranešimų medžiaga. Vilniaus universiteto Kauno humanitarinis fakultetas. 2004, p. 54-58.

13. European Computer Driving Licence Foundation. [Interaktyvus]. [Žiūrėta 2007 lapkričio 18 d.]. Prieiga per internetą: < http://www.ecdl.com/publisher/index.jsp>;

14. Sekunde.lt - ES įstatymų leidėjai ragina apsaugoti vaikus nuo netinkamo turinio internete. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.sekunde.lt/content.php?p=read&tid=20988 >;

15. Crimes against children reseach center. [Interaktyvus]. [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: < http://www.unh.edu/ccrc/Child_Vic_Papers_pubs.html>;

16. eSecurity. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.esecurity.lt/ >;

17. eSaugumas. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.esaugumas.lt/ >;

18. Draugiškas internetas. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.draugiskasinternetas.lt/lt ;

19. Childnet International. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.childnet-int.org/ >;

20. Safe Kids. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://safekids.com/ >;

21. Easy Test Maker. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.easytestmaker.com/default.aspx >;

22. Yahoo safely. [interaktyvus] [Žiūrėta 2008 gruodžio 19 d.]. Prieiga per internetą: <http://family.yahoo.com/?q=node/78&nodetype=blog>;

23. Bebo safety tips. [interaktyvus] [Žiūrėta 2008 gruodžio 19 d.]. Prieiga per internetą: <http://www.bebo.com/SafetyTips.jsp>;

24. eBaltics: Baltis IT&T 2009. [interaktyvus] [Žiūrėta 2009 gruodžio 3 d.]. Prieiga per internetą: <http://www.ebaltics.com/?sadala=106&PHPSESSID=aa7946fa5d0a410bcb65f2c9d5b37c60>;

25. Langas į ateitį: Saugus darbas internete. [interaktyvus] [Žiūrėta 2008 gruodžio 19 d.]. Prieiga per internetą: <http://www.vipt.lt/moodle/course/view.php?id=4>;

26. AICA: Cetrificazione GIS. [interaktyvus] [Žiūrėta 2009 sausio 6 d.]. Prieiga per internetą: <http://www.ecdlgis.com/>;

27. ECDL: Croatia – E-KIDS. [interaktyvus] [Žiūrėta 2009 sausio 6 d.]. Prieiga per internetą: <http://www.ecdl.hr/content/view/93/110/>;

28. Cyber Crime: Security Center. [interaktyvus] [Žiūrėta 2009 sausio 15 d.]. Prieiga per internetą: <http://www.bytecrime.org/>;

29. Nemokami kompiuterinio raštingumo e. mokymosi kursai: Apsaugokime save ir vaikus internete. [interaktyvus] [Žiūrėta 2009 kovo 16 d.]. Prieiga per internetą: <http://ekursai.langasiateiti.lt/cms/app?service=external/index&sp=6123&sp=5422>;

30. Vikipedija: Trojos arklys. [interaktyvus] [Žiūrėta 2009 balandžio 10 d.]. Prieiga per internetą: <http://lt.wikipedia.org/wiki/Trojos_arklys_(programa)>;

31. Vaikai ir internetas. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.vaikaiirinternetas.net/consejos_PSI.swf >;

32. eMarketer. [Interaktyvus]. [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.emarketer.com/Article.aspx?id=1005616>;

33. Windows Security. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.windowsecurity.com/whitepapers/Protecting-Children-Internet.html >;

34. TELEŠIUS, Eugenijus; LUKOŠEVIČIUS, Mantas. (2008) e-Guardian Programme – The New ECDL Endorsed Product proposal from ECDL Lithuania. *Ryga: Strategies, Media, and Technologies in European Education Systems*, p. 41-43.

35. LUKOŠEVIČIUS, Mantas. (2009) E-Guardian – the New Certification Programme on Skills of Ensuring Children Safety Using Internet. Kaunas: *IT 2009*, p. 215-218.

36. TELEŠIUS, Eugenijus; LUKOŠEVIČIUS, Mantas. (2009) e-Guardian Certification Programme Pilot in Lithuania. *Ryga: Baltic IT&T 2009: eBaltics*, [interaktyvus] [Žiūrėta 2009 gegužės 17 d.] Prieiga per internetą: <http://www.ebaltics.com/forum2009/Presentations/Telesius.pdf>;

37. ECDL test engine. [interaktyvus] [Žiūrėta 2009 gegužės 15 d.]. Prieiga per internetą: <http://www.ecdl.lt/EN/ECDL.nsf>;

38. Wikipedia – Youth Internet Safety Survey. [Interaktyvus]. [Žiūrėta 2007 lapkričio 13 d.]. Prieiga per internetą: <http://en.wikipedia.org/wiki/Youth_Internet_Safety_Survey>;

39. Europos kompiuterinio vartotojo pažymėjimas. [Interaktyvus]. [Žiūrėta 2007 lapkričio 18 d.]. Prieiga per internetą: <http://www.ecdl.lt/modules/tinycontent/index.php?id=3>;

40. National Center for Missing & Expoited Children. [Interaktyvus]. [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=200>;

41. Protecting Children From Pornography and Mature Content. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: < http://ezinearticles.com/?Protecting-Children-From-Pornography-and-Mature-Content&id=647359 >;

42. Dans Guardian – true web content filtering for all. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: < http://dansguardian.org/?page=introduction >;

43. SquidGuard. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: <http://www.squidguard.org/about.html >;

44. Content watch – Internet management. [interaktyvus] [Žiūrėta 2007 lapkričio 19 d.]. Prieiga per internetą: < http://www.contentwatch.com/education/suite >;

PRIEDAI

1 PRIEDAS **STRAIPSNIS APIE E-GUARDIAN PROGRAMĄ**

E-Guardian programme – the new ECDL Endorsed Product proposal from ECDL Lithuania

Dr. Eugenijus Telešius, Information Technologies Institute, et@ecdl.lt
Mantas Lukoševičius, Vilnius University Kaunas Faculty of Humanities, m.lukosevicius@sekasoft.com

Key words: digital literacy, skills certification, European Computer Driving Licence Foundation, Internet threats, e-Guardian programme.

Abstract:

Rapid development of the Information and Communication Technologies has huge impact on every day life. Unfortunately there is a high number of threats on the Internet. Cyber crime is only one part of the Internet rights violations. The main purpose of e-Guardian programme is to directly help getting the needed knowledge to protect children from dangers on virtual world. The e-Guardian programme is one of the Endorsed Partner programmes from the European Computer Driving Licence Foundation Ltd., the worldwide governing body and licensing authority for the global standard in end-user computer skills certification.

3 ECDL Foundation

European Computer Driving Licence Foundation Ltd (ECDL Foundation), registered in Ireland, is the worldwide governing body and licensing authority for ECDL (European Computer Driving Licence) and ICDL (International Computer Driving Licence) programme, the global standard in end-user computer skills certification.
The considerable reputation of the Foundation is based on their pioneering role in identifying and developing programme content, strong commitment to rigorous test design methodologies and adherence to the highest quality standards.
The Foundation has strong social ethos, has not-for-profit status and enjoy the unique support from over 50 National Computer Societies across the globe [1].

1.2. Mission

The ECDL Foundation mission is to enable proficient use of ICT that empowers individuals, organisations and society, through the development, promotion and delivery of quality certification programmes throughout the world [1].

1.3. Values

The ECDL Foundation values are:

- Social Responsibility: as a not-for-profit organisations, the members of the Foundation are committed to improving digital skills proficiency within their own societies. The certification programmes from the Foundation are designed to be accessible to all citizens, irrespective of age, gender, status, ability or race.
- Vendor Independence: the certification programmes give to candidates the flexibility and freedom to acquire digital skills and confidently apply them in any software environment that they may be required to use.
- Quality: the Foundation strive for continuous improvements in all that they do and ensure their programmes are implemented to consistent standards internationally [1].

4 Programmes

A key factor behind the success of the ECDL / ICDL certification programmes has been an emphasis on consistently high quality standards. These standards are not merely aspirational. ECDL Foundation operates a comprehensive Quality Assurance system made up of its Licensee Audit Programme and its Quality Management System.
ECDL / ICDL raises the level of ICT and computer skills and allows candidates to be more productive at home and at work. ECDL / ICDL also improves job prospects by providing an internationally recognised qualification.
ECDL / ICDL offers many different certification programmes. E-Citizen is a new certification specifically developed for people with a limited knowledge of computers and the Internet. EqualSkills programme is specifically designed for complete beginners and is open to everyone regardless of status, education, age, ability or understanding.
ECDL / ICDL CAD is for students and professionals seeking an internationally recognised qualification to certify their current core CAD skills. This certification can provide the basis towards further studies or professional development in a CAD related field. ECDL / ICDL Advanced is a higher-level programme designed for those who have successfully reached ECDL / ICDL skills levels and wish to further enhance their computer proficiency. ECDL / ICDL Advanced covers

Advanced Word Processing, Advanced Spreadsheets, Advanced Database and Advanced Presentation. CTP is a programme suitable for both ECDL trainers and organisations. The programme has been designed to reflect the reality of professional IT training [1].
Within ECDL Foundation, a Quality Management System has been put in place to ensure that all internal activities are carried out in a structure that ensures effectiveness, efficiency, and continuous improvement. The cornerstone of this Quality Management System is the Quality Policy. In 2005, ECDL Foundation's Quality Management System was certified by the external auditors, Certification Europe, as being compliant with the internationally recognised ISO 9001:2000 standard [1].

5 Endorsed Partner Programme

In addition to the wide range of the ECDL Foundation certification programmes Endorsed Products are locally developed certification programmes which adhere to a high standard of content and operational administration. Adherence to these standards allows the developer use of the ‚Endorsed by ECDL Foundation' logo in its promotion of the product. Although endorsed products are not owned by ECDL Foundation, the content, structure and maintenance method is approved and validated against the ECDL Foundation Endorsed Product Quality Assurance Standards [1].
Product Endorsement Standards as to e-Guardian apply to existing products and product concepts seeking endorsement.
The standards are grouped into three categories:

- Syllabus standards relate to the specification of the Certification's skills/knowledge domain.
- Assessment standards relate to the rationale behind and development of the mechanisms for deciding to certify a Candidate.
- Operational standards relate to rules around the administration of the programme and ensure the on-going high quality of the Certification's operation

The Licensee seeking endorsement for a product must complete the Product Endorsement form as comprehensively as possible in order to facilitate endorsement. For a product to become endorsed, it must be judged by the ECDL Foundation to have met all the standards set out in this form. The standards are expressed generically because there is an acknowledgement that there may be variation in the type of product seeking endorsement. Nevertheless, they clearly state the key product attributes that must exist for a certification to be judged to be of high quality.

6 E-Guardian Programme

Rapid development of the Information and Communication Technologies has huge impact on every day life. We can see that number of Internet users is increasing every day. Unfortunately with the higher number of users is coming higher number of threats. Cyber crime is only one part of the Internet rights violations, where more often we can see impact of negative Internet experience in real life. We have to acknowledge that number of users among the elderly is decreasing, but increasing among minors and teens.
The main purpose of E-Guardian programme is to directly help getting the needed knowledge to protect children from dangers on virtual world.
Currently on market space there are a lot of training programmes which could be identified under the name of e-Parent with main goal to directly help parents to gain the knowledge necessary to protect their children. Programmes are intended to give knowledge for adults, to become able to understand the situations, possibilities of actions and usage of tools for those actions to perform. The main purpose of E-Guardian programme is also to directly help getting the needed knowledge to protect children from dangers on virtual world. The main difference is that there will be formal certification for employees of institutions dealing with children on daily basis under the e-Guardian programme. The e-Guardian will have formal final ECDL Foundation level examination proving the certain level of competency.
E-Guardian offers gaining knowledge and certification covering areas:

- Common means for safety assurance – understanding benefits of computer system updates, need of user accounts and passwords, standart OS integrated security means, data protection and backups, etc.
- Malicious software - understanding different malicious software, threats of malware infected emails, securable usage of instant messaging, knowing security software to protect systems against malware, etc. [4].
- Sacurable web browsing and paying on Internet – understanding Internet browsing threats, tools that ensure safety, encryption keys, distinguishing safe/genuine online transaction/commerce sites from unsafe , being able to perform online transaction using credit or debit cards, etc. [2].
- Children safety – understanding that open communications between parent and children is important to keeping children safe, knowing about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet, system monitoring types and being able to monitor use of computer, being able to use software to control children use of Internet, operating system and software, knowing about children protection software, defensive software, quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use them, etc. [3].

ECDL Lithuania registered e-Guardian Programme proposal for the ECDL Foundation Endorsed Partner Programme.

References

1.ECDL FOUNDATION (2008) *About ECDL Foundation*, www.ecdl.com

2.NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (2008) *Resources for Parents & Guardians*, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=200

3.GRUNWALD ASSOCIATES (2004) *Children, Families, and the Internet*, http://grunwald.com/surveys/cfi/index.php

4.ESECURITY (2008) IT Security, http://www.esecurity.lt/info.php?ident=it&type_id=

E-GUARDIAN – THE NEW CERTIFICATION PROGRAMME ON SKILLS OF ENSURING CHILDREN SAFETY USING INTERNET

Mantas Lukoševičius

Vilnius University Kaunas Faculty of Humanities, Muitinės 8, Kaunas, Lithuania,
m.lukosevicius@sekasoft.com

Abstract. The article introduces the ECDL Foundation and its mission, main ECDL / ICDL programme differencies. The main means of the Endorsed Partner Programme are defined together with the e-Guardian programme endorsement application standards. E-Guardian section introduces the programme realization steps and gives certification covering areas: commom means for safety assurance, malicious software, electronic messages, securable web browsing and paying on internet and children safety.

Key words: digital literacy, skills certification, European Computer Driving Licence Foundation, Internet threats, e-Guardian programme.

Introduction

Rapid development of the Information and Communication Technologies has huge impact on everyday life. Unfortunately there are a high number of threats on the Internet. Cyber crime is only one part of the Internet rights violations. The goal of e-Guardian is to develop a programme to directly help getting the needed knowledge to protect children from dangers on virtual world. The e-Guardian programme is one of the Endorsed Partner programmes from the European Computer Driving Licence Foundation Ltd., the worldwide governing body and licensing authority for the global standard in end-user computer skills certification. Programme tasks include: making a syllabus, questions for the Automotive Question Test Base, provide an experiment in order to establish essential characteristics for automotive test, determine a duration of the test, complexity level, passing scores and number of correct answers.

4. ECDL Foundation

European Computer Driving Licence Foundation Ltd (ECDL Foundation), registered in Ireland, is the worldwide governing body and licensing authority for ECDL (European Computer Driving Licence) and ICDL (International Computer Driving Licence) programme, the global standard in end-user computer skills certification [1].

The considerable reputation of the Foundation is based on their pioneering role in identifying and developing programme content, strong commitment to rigorous test design methodologies and adherence to the highest quality standards.

7 Mission

The ECDL Foundation mission is to enable proficient use of ICT that empowers individuals, organisations and society, through the development, promotion and delivery of quality certification programmes throughout the world [1].

1.2. Programmes

ECDL / ICDL offers many different certification programmes. E-Citizen is a new certification specifically developed for people with a limited knowledge of computers and the Internet. EqualSkills programme is specifically designed for complete beginners and is open to everyone regardless of status, education, age, ability or understanding.

ECDL / ICDL CAD is for students and professionals seeking an internationally recognised qualification to certify their current core CAD skills. This certification can provide the basis towards further studies or professional development in a CAD related field. ECDL / ICDL Advanced is a higher-level programme designed for those who have successfully reached ECDL / ICDL skills levels and wish to further enhance their computer proficiency. ECDL / ICDL Advanced covers Advanced Word Processing, Advanced Spreadsheets, Advanced Database and Advanced Presentation. CTP is a programme suitable for both ECDL trainers and organisations. The programme has been designed to reflect the reality of professional IT training [2].

8 Endorsed Partner Programme

In addition to the wide range of the ECDL Foundation certification programmes Endorsed Products are locally developed certification programmes which adhere to a high standard of content and operational administration. Adherence to these standards allows the developer use of the Endorsed by ECDL Foundation logo in its promotion of the product.

Although endorsed products are not owned by ECDL Foundation, the content, structure and maintenance method is approved and validated against the ECDL Foundation Endorsed Product Quality Assurance Standards [1].

Product Endorsement Standards as to e-Guardian apply to existing products and product concepts seeking endorsement. The standards are grouped into three categories:

- Syllabus standards relate to the specification of the Certification's skills/knowledge domain.
- Assessment standards relate to the rationale behind and development of the mechanisms for deciding to certify a Candidate.
- Operational standards relate to rules around the administration of the programme and ensure the on-going high quality of the Certification's operation

The Licensee seeking endorsement for a product must complete the Product Endorsement form as comprehensively as possible in order to facilitate endorsement. For a product to become endorsed, it must be judged by the ECDL Foundation to have met all the standards set out in this form. The standards are expressed generically because there is an acknowledgement that there may be variation in the type of product seeking endorsement. Nevertheless, they clearly state the key product attributes that must exist for a certification to be judged to be of high quality.

9 E-Guardian Programme

Rapid development of the Information and Communication Technologies has huge impact on everyday life. We can see that number of Internet users is increasing every day. Unfortunately with the higher number of users is coming higher number of threats. Cyber crime is only one part of the Internet rights violations, where more often we can see impact of negative Internet experience in real life. We have to acknowledge that number of users among the elderly is decreasing, but increasing among minors and teens.

Currently on market space there are a lot of training programmes which could be identified under the name of e-Parent with main goal to directly help parents to gain the knowledge necessary to protect their children. Programmes are intended to give knowledge for adults, to become able to understand the situations, possibilities of actions and usage of tools for those actions to perform. The main purpose of E-Guardian programme is also to directly help getting the needed knowledge to protect children from dangers on virtual world. The main difference is that there is a formal certification for employees of institutions dealing with children on daily basis under the e-Guardian programme. The e-Guardian has a formal final ECDL Foundation level examination proving the certain level of competency.

The main steps of the realization of the e-Guardian programme are syllabus making, developing automotive question test base questions, providing experiments in order to establish essential characteristics for automotive test, determine a duration of the test, complexity level, passing scores and number of correct answers. While working on the programme realization, the author was involved in all steps. We are working on the pilot implementation of the programme at the moment.

E-Guardian automotive question test base questions are made according to the syllabus that is certified by the ECDL Endorsed partner program. E-Guardian offers five gaining knowledge and certification covering areas.

3.1. Common means for safety assurance

This area covers knowledge such as knowing how to follow, download and use updates for your operating system, additional software and security components. Understand the benefits of updates. Knowing multiple user accounts and understanding what personal user accounts are and how information of different users is separated. Understanding the purpose of a user name, and the difference between user name and user password. Understand the meaning and importance of access rights. Knowing the necessity of login to system password, and the usage of login passwords. Knowing the structure of a complex password and the rules for changing and keeping passwords. Adjusting protection level in standard security means that are integrated in the operating system (Firewall, Defender, etc.). Being able to protect data on computer disk. Knowing about data encryption and password protection. Knowing how to find out whether a data media has a password protection possibility, used for protecting against unwanted data access. Be able to use these passwords for protection. Be able to protect CD, DVD, USB memory and other external data media. Understanding the threat of malicious data spread in external data medias. Understanding the benefits and purpose of data and software backups. Knowing who to contact when discovering or suspecting that data can be classified as illegal or dangerous.

3.2. Malicious software

Malicious software are is about understanding different malicious software (viruses, Trojan horses, spyware, dishonest adware, etc.) definitions and differences. Knowing when and how malicious software can get into computer system. Knowing what security software is used to protect against malware. Being able to configure software to automatic and regular update. Knowing what has to be done and in what order, if suspecting that computer system is infected.

Understanding the limitation of security software. Understanding that an active version of security software should be running when downloading files or opening email attachments. Knowing that unknown and unwanted emails and their attachments should not be opened. Understanding what is unsafe data media. Understand that unsafe CD, DVD, USB memory media should not be used.

10 Electronic messages

Area covers knowledge based on knowing about email that is classified as spam, and email messages infected with malware. Being aware of privacy protection legal act. Knowing how to redirect children emails. Knowing how to reject email from specific email addresses. Knowing how to block private messages between a child and another user. Knowing how to treat email messages from unknown senders. Knowing how to treat safe with instant messaging. Being aware of mobile phone capabilities. Knowing who to contact if discovered or suspect dangerous or illegal content.

11 Securable web browsing and paying on internet

This area is about knowing about tools that ensure safety when browsing the internet (blocking of cookies, ActiveX control, etc.). Knowing about advantages, disadvantages and dangers of internet cookies. Knowing about treats associated with the personal data disclosure. Knowing about gaps and treats, such as possibilities for evel-minders to use or steal client information. Knowing about encryption keys used on internet, knowing about types of encryption keys and how to use them. Being able to distinguish safe/genuine online transaction/commerce sites from unsafe. Being able to perform online transaction using credit or debit cards. Knowing how to contact service administrator while required. Knowing who to contact when discovering or suspecting dangerous or illegal content.

12 Children safety

This section covers means of understanding that open communications between parent and children is important to keeping children safe. Knowing about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet. Knowing about system monitoring types and be able to monitor use of computer. Being able to access temporary internet files and browser history. Being able to use software to control children use of internet, operating system and software. Knowing about children protection software. Being able to use internet content filtering tools integrated on web browsers. Knowing what defensive software is. Knowing what a quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use it. Being able to access the chat, instant messenger history. Being able to contact service administrator. Knowing about recommended kid directories, search sites geared for children and targeted at teenagers. Knowing who to contact when discovered or suspect dangerous or illegal content.

References

[1] ECDL FOUNDATION (2009) *About ECDL Foundation,* www.ecdl.com

[2] CERTIFIED TRAINING PROFESSIONAL (2009) *Programme information,* http://www.ecdl.ie/Downloads/ECDl_CTP_Programmes_Information.pdf

[3] GRUNWALD ASSOCIATES (2004) *Children, Families, and the Internet,* http://grunwald.com/surveys/cfi/index.php

[4] ESECURITY (2009) IT Security, http://www.esecurity.lt/info.php?ident=it&type_id

[5] ESAUGUMAS (2009) Vaikai ir Internetas, http://www.esaugumas.lt/index.php?181464073

[6] CHILDNET INTERNATIONAL (2009) Projects, http://www.childnet-int.org/projects/

[7] SAFEKIDS (2009) Child Safety, http://www.safekids.com/child-safety-on-the-information-highway/

Product Endorsement Standards – e-Guardian

The following standards, expressed in a form, apply to existing products and product concepts seeking endorsement.

The standards are grouped into three categories:

- Syllabus standards relate to the specification of the Certification's skills/knowledge domain.
- Assessment standards relate to the rationale behind and development of the mechanisms for deciding to certify a Candidate.
- Operational standards relate to rules around the administration of the programme and ensure the on-going high quality of the Certification's operation

The Licensee seeking endorsement for a product must complete this form as comprehensively as possible in order to facilitate endorsement. For a product to become endorsed, it must be judged by the ECDL Foundation to have met all the standards set out in this form. The standards are expressed generically because there is an acknowledgement that there may be variation in the type of product seeking endorsement. Nevertheless, they clearly state the key product attributes that must exist for a Certification to be judged to be of high quality. For some standards, examples are provided to illustrate how conformance may be demonstrated.

1. Syllabus

1.1 The fundamental purpose of the Certification, identifying the broad skills and knowledge areas covered, must be stated in an overview paragraph.

This should position the skills and knowledge in terms of their application by the Candidate. A statement of Certification goals, stating the general requirements and then providing some detailed requirements by main skills or knowledge area, meets this requirement.

Example: See introductory module goals in ECDL Syllabus Version 4.0

Requirement:

The candidate should understand **Common means for safety assurance:**
The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas **Malicious software:**
The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas of **Securable web browsing and paying on internet:**
The candidate should be able to recognize the threats and be able to protect/ prevent them in the areas **Children safety:**

1.2 The specific learning outcomes for the Certification must be clearly defined so that the Candidate can unambiguously identify the skills and knowledge areas in which they are being certified.

Common means for safety assurance:

- Know how to follow, download and use updates for your operating system, additional software and security components. Understand the benefits of these updates.
- Know multiple user account. Understand what a personal user account is and how information of different users is separated.
- Understand the purpose of a user name, and the difference between user name and user password. Understand the meaning and importance of access rights.
- Know the necessity of login to system password, and that the usage of login passwords
- Be able to make complex password. Know the structure of a complex password and the rules for changing and keeping passwords.
- Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Defender, etc.).
- Be able to protect data on computer disk. Know about data encryption and password protection.
- Know how to find out whether a data media has a password protection possibility, used for protecting against unwanted data access. Be able to use these passwords for protection. Be able to protect CD, DVD, USB memory and other external data media.
- Understand the threat of malicious data spread in external data medias.
- Understand the benefits and purpose of data and software backups.
- Know who you should contact if you discovered or suspect that data can be classified as illegal or dangerous

Malicious software:

- Understand different malicious software (viruses, Trojan horses, spyware, dishonest adware, etc.) definitions and differences.
- Know when and how malicious software can get into computer system.
- Know what security software used to protect against malware.
- Be able to configure software to automatic and regular update
- Know what has to be done and it what order, if you suspect that computer system is infected. Understand the limitation of security software.
- Understand that an active version of security software should be running when downloading files or opening email attachments.
- Know that unknown and unwanted emails and their attachments should not be opened.
- Understand what is unsafe data media. Understand that unsafe CD, DVD, USB memory media should not be used
- Electronic messages:
- Know about email that is classified as spam, and email messages infected with malware.
- Be aware of privacy protection legal act
- Know how to redirect children email first to your account
- Know how to reject email from specific email addresses
- Know how to block private messages between a child and another user
- Know how to threat email messages from unknown senders.
- Know how to threat securable with instant messaging.
- Be aware of mobile phone capabilities
- Know who to contact if you discovered or suspect dangerous or illegal content

Securable web browsing and paying on internet:

- Know about tools that ensure safety when browsing the internet (blocking of cookies, ActiveX control, etc.).
- Know about advantages, disadvantages and dangers of internet cookies.
- Know about threats associated with the personal data disclosure
- Know about gaps and threats, such as possibilities for evel-minders to use or steal client information.

- Know about encryption keys used on internet, know about types of encryption keys and how to use them.
- Be able to distinguish safe/genuine online transaction/commerce sites from unsafe.
- Be able to perform online transaction using credit or debit cards.
- Know how to contact service administrator while required
- Know who to contact if you discovered or suspect dangerous or illegal content

Children safety:

- Understand that open communications between parent and children is important to keeping children safe.
- Know about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet.
- Know about system monitoring types and be able to monitor use of computer.
- Be able to access temporary internet files and browser history
- Be able to use software to control children use of internet, operating system and software.
- Know about children protection software.
- Be able to use internet content filtering tools integrated on web browsers.
- Know what defensive software is.
- Know what a quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use it.
- Be able to access the chat, instant messenger history
- Be able to contact service administrator
- Know about recommended kid directories, search sites geared for children and targeted at teenagers.
- Know who to contact if you discovered or suspect dangerous or illegal content

1.3 The specific learning outcomes must be created using a formal process validated by appropriate subject matter expertise.

The steps involved in creating the syllabus and the details of the subject matter experts, together with their credentials, should be provided. It should be noted that the syllabus will be reviewed by an ECDL Foundation subject matter expert. This review is concerned with technical accuracy and with the appropriateness of the syllabus regarding the stated programme goals.

Example: See the ECDL Validation Overview document.

Requirement:

Please provide details of the relevant subject matter expertise:

. Alfredas Otas, Chairman of the Lithuanian Computer Society; Chair of IT Expert oup at Ministry of Science and Education, Lithuania
Piotr Mrozinski, Regional Development Executive, ECDL Foundation
Dr. Marek Milosz, CEO of ECDL–Poland, Head of Division at Lublin University Technology, Poland
Vaino Brazdeikis, Director of the Centre of Information Technologies of ucation, Lithuania
Tomas Lygutas, Doctoral student, Institute of Informatics, Lithuania (Internet urity)
Mantas Lukosevicius, Security administrator, Company Sekasoft, Lithuania

- Advice is sought at key points from teachers, significant individuals and organisations. In particular, professional teacher associations play an important role.
- A project manager employed by the Office of the Board of Studies manages the syllabus development project, developing the initial proposal, establishing consultative networks, managing consultation, and drafting and revising syllabus documentation.
- Project teams will, at various stages of the syllabus development process, include curriculum, assessment and publications officers.
- Contracted writers are, at times, also included in the project teams. The Expert Group maintains a register of writers. To be considered for appointment as writers, teachers from all syllabus areas with demonstrated writing expertise can submit an expression of interest to the Expert Group.

1.4 A specific method for maintaining and revising the syllabus should be established and documented.

Syllabus revision ensures that the syllabus is current and relevant as it addresses technological advances, innovation and Candidate requirements following a specified time from product release. The recommendation for change should be derived from test centre questionnaires and Candidate feedback in addition to subject matter expert guidance and an industry review.

Example: Syllabus Version Upgrade Process Map - **See Appendix 1.1 Pg 9**

Requirement:

Please provide details of a process for syllabus review and upgrade:

Phase 1 Syllabus review
Purpose
A review of the existing syllabus provision and a plan for the revision or development of the syllabus.

Following consideration of relevant data the Licensee determines whether a review of existing syllabus provision will be conducted.

The review phase will typically involve
• establishment of a Expert Group to monitor the syllabus development process and provide advice throughout the project
• establishment of the project plan which includes consultation and a timeline
• informing Licensees and Test Centres of the project plan including the timeline for consultation
• evaluation of the existing syllabus against the syllabus criteria approved by the Licensee
• consultation with teachers and key groups regarding the existing syllabus and the general directions for the syllabus development
• research, including a review of literature and practice in Europe and overseas
• recommendation to the Expert Group of the broad directions for syllabus revision or development in response to the review findings to the Expert Group
• Expert Group endorsement of broad directions for syllabus revision or development

Outcomes
• endorsement by the Expert Group of the broad directions for syllabus revision or development
• information provided to the third parties

Phase 2: Writing brief development
Purpose
The development of a writing brief for the draft syllabus that takes account of the Expert Group directions established during the syllabus review phase.

This phase will typically involve
• preparation of a draft writing brief by a project team, taking into account information from consultation and research undertaken during the previous phase
• widespread consultation on the draft writing brief, involving:
- teachers
- key groups, including professional associations and school systems
- other relevant third partie committees
• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response
to those issues
• modification of the draft writing brief in response to consultation feedback
• consideration of the amended draft writing brief for the Expert Group with recommendation

• submission of the draft writing brief, consultation report and Licensee recommendation to the
ECDL Foundation for endorsement
• Internet publication of the consultation report and endorsed writing brief.

Outcome
A writing brief which provides the detailed blueprint for the development of the syllabus, against which the final syllabus
is judged.

Phase 3: Syllabus development
Purpose
The development of the syllabus package as defined by the project plan.

This phase will typically involve
• preparation of a draft syllabus package, by a project team, according to the endorsed writing brief
• distribution of a draft syllabus package for consultation (via the Internet) to:
- teachers
- key groups, including professional associations and school systems
- the Expert Group
- other relevant third parties committees
• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response
to those issues
• preparation of a report that describes the extent to which board criteria for approval of syllabuses have been met
• modification of the draft syllabus package in response to consultation feedback
• consideration of the amended draft syllabus package by the expert group for recommendation to
the ECDL-F
• submission of the draft syllabus package, consultation report and expert group recommendation to
the ECDL-F for endorsement
• submission of the syllabus to the ECDL-F for approval
• Internet publication of the consultation report
• editing, design, layout and printing of the approved syllabus package
• briefing of school authorities to effect handover of syllabus package for implementation in schools
• distribution of the syllabus package to schools.
Outcomes
• A syllabus approved by the ECDL-F
• Publication and distribution of the syllabus package.

Phase 4: Implementation
Purpose
Implementation of the syllabus is conducted by the Test Centres and other Licensee. The LIKS role is the on-going collection of
data on the use of the syllabus to ascertain whether the intentions of the syllabus are

being achieved.

This phase will typically involve
• collection, collation and analysis of data on the use of the syllabus
• routine reports to the Board and ECDL-F
• identification and recording of issues that need to be taken into account in subsequent syllabus
revision.

Outcome
Data on the use of the syllabus that can be used to inform a future syllabus review.

13 Assessment

2.1 Assessments should be developed on a sound scientific basis.

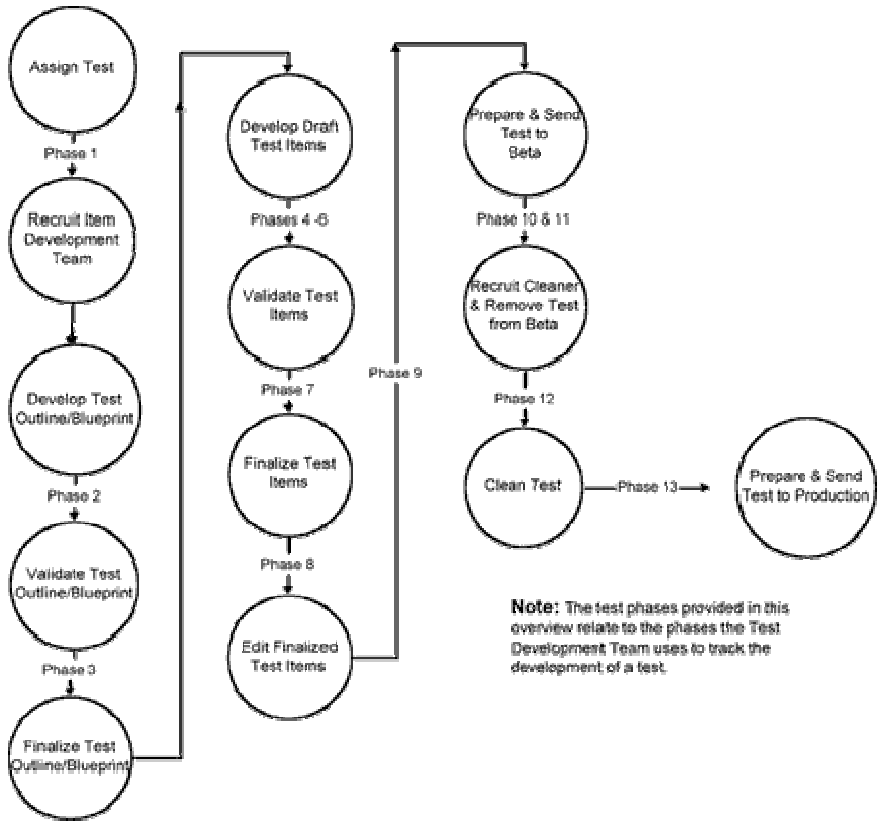
There should be a clear rationale behind the use of a particular assessment approach. In addition, the assessment must be created in a formal process with appropriate subject matter expertise.

Example: **ECDL Foundation CTT Process Map –** See Appendix 1.2 Pg:11

MQTB Development Process Map – See Appendix 1.3 Pg: 14

Requirements:

Please provide a clear rationale behind the use of a particular assessment approach and the assessment development process.



2.2 Detailed assessment specifications should be documented, along with their rationale and the process by which they were developed.

Document the assessment specifications. Assessment specifications should include the following items, where appropriate.

Number of items / elements

Assessment format (test-based versus portfolio-based, automated versus manual etc.)

Item format (multiple choice versus simulation versus evidence requirement etc.)

- Time Specification (For tests that have time limits, test development research should examine the degree to which scores include a speed component and evaluate the appropriateness of the component given the domain the test is designed to measure.)

Cut Score (The procedures used to interpret test scores, and, when appropriate, the normative or standardization sample or the criterion used should be documented – for example the ECDL Foundation use the modified Angoff method to obtain the cut score).

Test administration procedures – the directions for test administration should be presented with sufficient clarity and emphasis so that it is possible for others to replicate adequately the administration conditions under which the data on reliability and validity are obtained.

It should be noted that an ECDL Foundation subject matter expert may review the assessment. This review is concerned with technical accuracy and with the appropriateness of the assessment regarding the syllabus.

Requirements: Please attach a detailed assessment specification.

2.3 There should be processes for monitoring the ongoing quality of the assessment and for revising the assessment as appropriate to ensure that it continues to be valid and relevant.

Processes should be put in place to ensure that the quality of the certification is preserved over time. These processes should include an element of management and action on feedback from stakeholders involved in the Certification as well as formal review of the technical aspects of the Certification.

Example: MQTB Version Upgrade Process 20 – **See Appendix 1.4 Pg.14**

Requirements:

Please provide a detailed process for reviewing and revising the assessment:

Phase 1 Existing MQTB review
Purpose
A review of the existing MQTB provision and a plan for the revision or development of the MQTB.

Following consideration of relevant data the Licensee determines whether a review of existing MQTB provision will be conducted. The review phase will typically involve
• establishment of Item review/development team
• establishment of the project plan which includes consultation and a timeline
• informing Licensees and Test Centres of the project plan including the timeline for consultation
• research, including a review of literature and practice in Europe and overseas
• Expert Group endorsement of broad directions for MQTB revision or development
Outcomes
• endorsement by the Expert Group of the broad directions for MQTB revision or development
• information provided to the third parties

Phase 2: MQTB blueprint development
Purpose
The development of a MQTB blueprint that takes account of the Expert Group directions established during the MQTB review phase.

This phase will typically involve
• preparation of a draft writing brief by a project team, taking into account information from consultation and research undertaken during the previous phase
• widespread consultation on the draft writing brief, involving:
- teachers
- key groups, including professional associations and school systems
- other relevant third partie committees
• preparation of a report that identifies issues emerging from the consultation and the action to be taken in response to those issues
• modification of the draft writing brief in response to consultation feedback
• **Outcome**
A writing brief which provides the detailed blueprint for the development of the MQTB, against which the final MQTB is judged.

Phase 3: MQTB development and Validation
Purpose
The development of the MQTB as defined by the project plan.

This phase will typically involve
• preparation of a draft MQTB, by a project team, according to the blueprint
• distribution of a draft MQTB for consultation (via the Internet) to:
- teachers
- key groups, including professional associations and school systems
- the Expert Group
- other relevant third parties committees
• preparation of a report that identifies issues emerging from the consultation and the

action to be taken in response
to those issues
• modification of the syllabus package in response to consultation feedback
• consideration of the MQTB amended draft group for recommendation to
the ECDL-F
• submission of the MQTB, consultation report and expert group recommendation to
the Expert Group for endorsement
• submission of the MQTB
• Internet publication of the consultation report
• editing, design, layout and printing of the approved MQTB
• briefing of school authorities to effect handover of MQTB package for
implementation in TC
• distribution of the MQTB to Licensees and TC

Outcomes

• A MQTB approved by the Expert Group
• Publication and distribution of the MQTB

Phase 4: Implementation

Purpose

Implementation of the MQTB is conducted by the Test Centres and other Licensees.

This phase will typically involve
• collection, collation and analysis of data on the use of the syllabus and MQTB
• identification and recording of issues that need to be taken into account in subsequent
MQTB revision.

Outcome

Data on the use of the MQTB that can be used to inform a future MQTB review.

14 Administration

3.1 There should be a clearly documented system for ensuring the efficient and valid operation of the Certification Programme.

A quality-focused system for operating the programme should be documented and communicated to all relevant parties. The key functions of this system are to ensure consistency and fairness of candidate treatment, preservation of the integrity of the assessment, and efficient operation.

3.1.1 An administration system should be established to record all key information relating to certification.

This system should contain key information such as candidate registration, assessment results, and certification. This system should store the data securely and meet all relevant data protection requirements.

Example: See ECDL Foundation QA Standards Section 2.1 “Administration”.

Requirement:

Please describe the administration system that will support this endorsed product. The same administration system will be used as for support of other ECDL Foundation products in Lithuania. The administration system is in full compliance with the QA Standards.

3.1.2 Where partners are involved in the operation of the endorsed product, the requirements for partner approval must be clearly stated and a formal process must support this approval.

If other organisations are involved in elements of delivering the endorsed product, then clear requirements must be established that must be met by these partners. If a partner is to be involved in implementing the assessment element of the product, there should be clear requirements concerning the appropriateness of the organisation and its facilities and staff. There should also be a formal process through which a partner must pass before becoming approved. Typical partners would be Test Centres, Courseware Vendors, or ATES Vendors.

Example: See ECDL Foundation QA Standards Section 2.2 “Partner Approval”.

Requirement:

Please describe the criteria and processes for approving any partners. The same process will be used as currently which is in full compliance with the QA Standards.

3.1.3 There should be a formal process for evaluation the ongoing validity of operational activity.

Particularly where partners are involved in conducting assessments, there should be a formal process for review activity to ensure compliance to operational standards. There should also be a process for managing any instances of non- compliance.

Example: See ECDL Foundation QA Standards Section 2.2 “Partner Approval”.

Requirements:

Please describe the process for evaluating operational activity. The same process will be used as currently which is in full compliance with the QA Standards.

ECDL ICDL

E-GUARDIAN CERTIFICATION PROGRAM PILOT IN LITHUANIA

Speaker: Eugenijus Telešius

Baltic IT@T Forum, Riga, 2009

ECDL ICDL

Authors

Dr. Eugenijus Telešius
Information Technologies Institute
(ECDL Lithuania)
et@ecdl.lt

Mantas Lukoševičius
Vilnius University Kaunas Faculty of Humanities
m.lukosevicius@sekasoft.com

ECDL ICDL

What are we about today?

- ECDL Foundation and Programmes
- Endorsed Partner Programmes
- e-Guardian Programme
- e-Guardian Programme Start and Perspective

ECDL ICDL

ECDL-F and situation in region

- European Computer Driving Licence Foundation Ltd - the worldwide governing body and licensing authority for ECDL (*European Computer Driving Licence*) and ICDL (*International Computer Driving Licence*) programme, the global standard in end-user computer skills certification
- End Y2008, SCs issued: 42 140 in Lithuania, 7 387 in Estonia, 3 689 in Latvia
- Available in Russian language countries (Russia, Belarus, Ukraine, Azerbaijan, Kazakhstan,…)

ECDL ICDL

Programmes:

- e-Citizen
- ECDL Start, ECDL Core
- ECDL Advanced:
  - Advanced Word Processing
  - Advanced Spreadsheets
  - Advanced Database
  - Advanced Presentation
- ECDL CAD, ECDL WebStarter, ECDL ImageMaker, ECDL Health

ECDL ICDL

Endorsed Partner Programme

- Product Endorsement Standard
- The Licensees seeking endorsement
- Categories of Product Endorsement Standards:
  - Syllabus standards
  - Assessment standards
  - Operational standards

ECDL ICDL

E-Guardian Programme

•Why do we need it?

•The main purpose of E-Guardian programme is to directly help getting the needed knowledge to protect children from dangers on virtual world.

•Formal final ECDL Foundation level examination for the e-Guardian.

ECDL ICDL

Covering areas of the e-Guardian

Common means for safety assurance:

•Malicious software

•Sacurable web browsing and paying on Internet

•Children safety

ECDL ICDL

Test Engine for e-Guardian

Date: 22/02/2007

ATES Provider:	ECDL Lithuania
ATES Product Title:	ECDL Lithuanian Test Engine (ECDLTE)
ATES Version Number:	Ver.5.1 (Lithuanian)
ATES Type:	Hotspot / MCQ
Operating System:	Win2000/XP, Linux SUSE
Software Application Version:	Office2000/XP, OpenOffice, IE/OE5, IE/OE6, Mozilla
ECDL Syllabus Version:	Version 4

The ECDL Foundation under the guidance of the ATES (Automated Test Evaluation Systems) Working Group advises that the above product is technically compliant - **Lithuania** as the designated territory.

ECDL ICDL

e-Guardian Pilot in Lithuania

• Current implementation

• Duration and test composition

• More large AQTB

• Master level IT students involved

ECDL ICDL

e-Guardian Perspectives

• LdV Project Proposal

• Lithuanian and Latvian AQTB versions

• Courseware in English, Lithuanian and Latvian

• Open for collaboration

ECDL ICDL

Summary

• The number of Internet users is increasing among minors and teens
• The main purpose of e-Guardian programme is to help getting the knowledge to protect children from dangers of virtual world.
• ECDL Lithuania registered e-Guardian Programme proposal for the ECDL Foundation Endorsed Partner Programme and started with a pilot.

5 PRIEDAS **APKLAUSOS ANKETA EKSPERTAMS**

This is a questionnaire about e-Guardian test question base. E-Guardian is a certification programme on skills of ensuring children safety using Internet. The test questions were made according to the syllabus, that is certified by the ECDL Endorsed partner program.

E-Guardian syllabus:

Common means for safety assurance:

- Know how to follow, download and use updates for your operating system, additional software and security components. Understand the benefits of these updates.
- Know multiple user account. Understand what a personal user account is and how information of different users is separated.
- Understand the purpose of a user name, and the difference between user name and user password. Understand the meaning and importance of access rights.
- Know the necessity of login to system password, and that the usage of login passwords
- Be able to make complex password. Know the structure of a complex password and the rules for changing and keeping passwords.
- Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Defender, etc.).
- Be able to protect data on computer disk. Know about data encryption and password protection.
- Know how to find out whether a data media has a password protection possibility, used for protecting against unwanted data access. Be able to use these passwords for protection. Be able to protect CD, DVD, USB memory and other external data media.
- Understand the threat of malicious data spread in external data medias.
- Understand the benefits and purpose of data and software backups.
- Know who you should contact if you discovered or suspect that data can be classified as illegal or dangerous

Malicious software:

- Understand different malicious software (viruses, Trojan horses, spyware, dishonest adware, etc.) definitions and differences.
- Know when and how malicious software can get into computer system.
- Know what security software used to protect against malware.
- Be able to configure software to automatic and regular update
- Know what has to be done and it what order, if you suspect that computer system is infected. Understand the limitation of security software.
- Understand that an active version of security software should be running when downloading files or opening email attachments.
- Know that unknown and unwanted emails and their attachments should not be opened.
- Understand what is unsafe data media. Understand that unsafe CD, DVD, USB memory media should not be used
- Electronic messages:
- Know about email that is classified as spam, and email messages infected with malware.

- Be aware of privacy protection legal act
- Know how to redirect children email first to your account
- Know how to reject email from specific email addresses
- Know how to block private messages between a child and another user
- Know how to threat email messages from unknown senders.
- Know how to threat securable with instant messaging.
- Be aware of mobile phone capabilities
- Know who to contact if you discovered or suspect dangerous or illegal content

Securable web browsing and paying on internet:

- Know about tools that ensure safety when browsing the internet (blocking of cookies, ActiveX control, etc.).
- Know about advantages, disadvantages and dangers of internet cookies.
- Know about threats associated with the personal data disclosure
- Know about gaps and threats, such as possibilities for evel-minders to use or steal client information.
- Know about encryption keys used on internet, know about types of encryption keys and how to use them.
- Be able to distinguish safe/genuine online transaction/commerce sites from unsafe.
- Be able to perform online transaction using credit or debit cards.
- Know how to contact service administrator while required
- Know who to contact if you discovered or suspect dangerous or illegal content

Children safety:

- Understand that open communications between parent and children is important to keeping children safe.
- Know about online predators, financial scams, malware, cyber-bullying and the pervasiveness of pornography on the Internet.
- Know about system monitoring types and be able to monitor use of computer.
- Be able to access temporary internet files and browser history
- Be able to use software to control children use of internet, operating system and software.
- Know about children protection software.
- Be able to use internet content filtering tools integrated on web browsers.
- Know what defensive software is.
- Know what a quality anti-virus, anti-spyware, spam blocker, and personal firewall is and how to use it.
- Be able to access the chat, instant messenger history
- Be able to contact service administrator
- Know about recommended kid directories, search sites geared for children and targeted at teenagers.
- Know who to contact if you discovered or suspect dangerous or illegal content

Questionnaire:

11. Do You find e-Guardian test and certification needed?

Strength:	Not	Low	Medium	High	Very High
Why:					

12. Do You find the e-Guardian syllabus accurate?

Strength:	Not	Low	Medium	High	Very High
Why:					

13. There is the e-Guardian test questions attached. Please read them and fill any comments or notes needed according to Your judgement.

After finishing with the test questions base, please answer: Do you find the e-Guardian test questions accurate?

Strength:	Not	Low	Medium	High	Very High
Why:					

Thank You for Your time and attention!

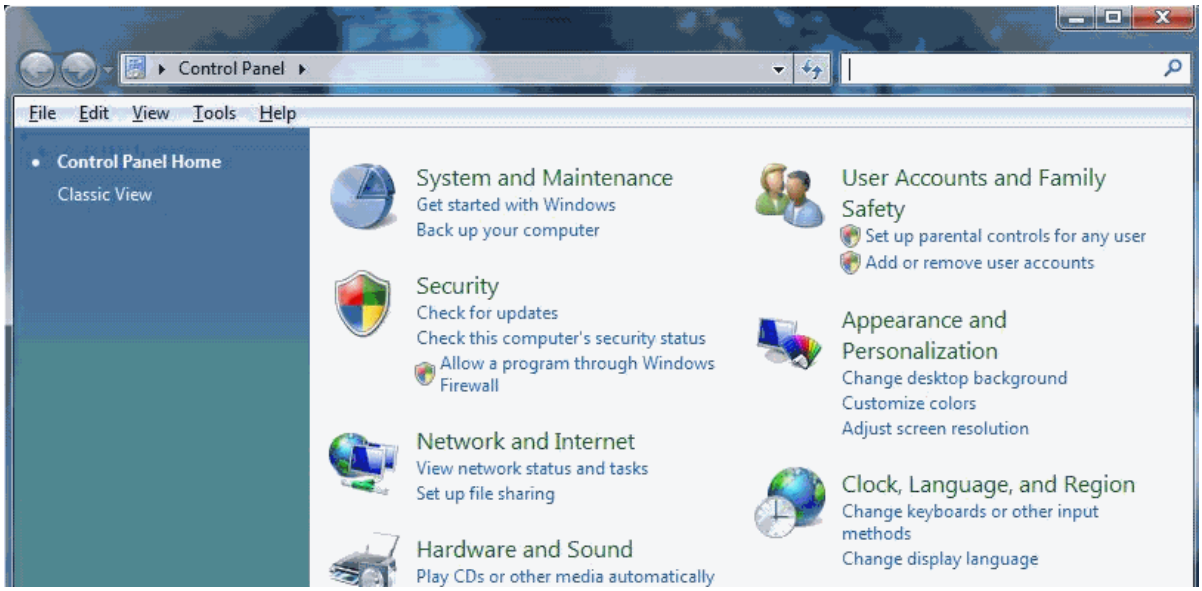
rinkinys

Kategorija: 1.10

Why do you need to backup your data?

Kategorija: 1.10

What should you choose on Control Panel, if you want to create backup?



Kategorija: 1.10

Which of the following propositions is correct?
1. Backups can be created using the Windows standard Backup application only manually
2. Backups can be created using the Windows standard Backup application, and it allows making backups regularly
3. Backup capability is available only in Windows Vista Business Edition
4. Windows Vista does not have the standard Backup Program

Teisingas: 2

Kategorija: 1.10

What information can you backup by using a standard Windows backup tool?

Kategorija: 1.11

You work in a large company. What should you do if you suspect that an e-mail you got to your work mailbox has a virus attached?
1. Inform the boss of your department
2. Save the attachment to disk and scan it with your antivirus system
3. Delete the letter immediatelly
4. Inform your system administrator

Teisingas: 4

Kategorija: 1.11

You have found content on Internet that is promoting racism. What will you do?
1. Tell my friends and relatives to avoid this page
2. Inform local Internet Hotline
3. Send this information for your Internet provider and ask for help
4. All answers are correct

Teisingas: 4

Kategorija: 1.11

If your child has got an e-mail message which includes information about atrocity or child's pornography, you should:
1. Speak with your child about danger of this information
2. Inform your system administrator
3. Make sure anti-spam software is installed on your computer
4. All answers are correct

Teisingas: 4

Kategorija: 1.11

You have found an illegal website with pornography content. What will you do?
1. Tell my friends and relatives to avoid this page
2. Inform search engines
3. Send this information for your Internet provider and ask for help
4. All answers are correct

Teisingas: 4

Kategorija: 1.1

What do you need to click if you want to update your operating system? Click on a particular place in the picture.

Kategorija: 1.1

What do you need Microsoft Windows updates for?
1. Windows Updates provide new design features for the OS
2. Windows Updates provide updates for the OS and its installed components
3. Windows Updates downloads definitions of new computer viruses in order to protect your computer against them
4. Windows Updates provide updates for all third party applications installed on your computer

Teisingas: 2

Kategorija: 1.1

Which item of Start menu should you choose, if you want to update your operating system?

Kategorija: 1.1

Is it possible to disable automatic Microsoft Update software?
1. Yes, it is possible
2. No, it isn't possible because Internet connection will be disabled
3. It is possible only, when SP3 is installed
4. No, it isn't possible because computer becomes open for viruses

Teisingas: 1

Kategorija: 1.2

John has a Microsoft Windows user account on a computer at work. He shares the computer with his collegue. The collegue does not have administrator privileges on the computer. Where does John have to store his personal files in order to keep them private from his collegue? No security settings have to be modified.
1. C:\Program Files\John_private
2. D:\Users\John's_folder
3. C:\Users\John
4. C:\Users\Administrator

Teisingas: 3

Kategorija: 1.2

Which proposition about user's rights is correct?
1. Users with limited accounts cannot install programs
2. Users with administrator accounts can always install programs
3. Only users with administrator accounts can install all programs
4. Users with limited and guest accounts can always install programs

Teisingas: 2

Kategorija: 1.2

Which proposition about user's rights is correct?
1. All users can read and copy files from directory "My documents"
2. Only users with administrator and limited accounts can read and copy files from directory "My documents"
3. Only users with administrator account can read and copy files from directory "My documents"
4. Users with limited and guest accounts can read files from directory "My documents"

Teisingas: 3

Kategorija: 1.2

Is it possible to view password-protected folders, if you are logged as guest user?
1. If you are logged as quest user, you don't have access to password-protected folders
2. Guest user has rights of administrator and can access password-protected folders
3. Guest user can only read password-protected folders
4. Guest user can access password-protected folders

Teisingas: 1

Kategorija: 1.2

You will share your computer with another user. You need to prevent the user from making unauthorized changes to the computer. What should you do?
1. Add the user to the Remote Desktop Users group
2. Create an administrator account for the user
3. Create a standard user account for the user
4. Add another user to Guests group

Teisingas: 3

Kategorija: 1.3

Why do you need a personal user account in Windows Operating System?
1. In order to have folders on disk
2. In order to be identified by your friends while visiting webchat sites
3. In order to log onto your computer, for security purposes and resource management
4. In order to install applications on your computer

Teisingas: 3

Kategorija: 1.3

Click on the icon that allows you to look for number of registered users on the computer?

Kategorija: 1.3

Is it possible for a user with administrator account to open and read encrypted documents?
1. Only users with administrator accounts can read and open encrypted documents
2. If a file is encrypted, other users cannot open it without a relevant password
3. All computer users can read and open encrypted documents
4. Only users with administrator or limited accounts can read and open encrypted documents

Teisingas: 2

Kategorija: 1.3

Is it allowed for a guest user to create another user?
1. Guest account owner can create another user if he is a computer administrator
2. Guest account owner can create another user if computer administrator has given him permission to manage all privileges
3. Guest account can create another user because he has the same privileges as the administrator, but does not have a login password
4. Guest account cannot create another user; he can only change its picture and set up its account to use .NET Passport

Teisingas: 4

Kategorija: 1.3

What is the safest way to leave computer when you are off for a moment?
1. Switch off the monitor
2. Disconnect internet cable
3. Log off or switch user
4. Disconnect keyboard

Teisingas: 3

Kategorija: 1.4

Is it necessary to protect user account with password?
1. Yes, if you want to protect your data from strangers
2. Yes, if your computer is connected to internet

3. Yes, if other people can access your computer
4. All answers are true
Teisingas: 4

Kategorija: 1.4

How can you change your Windows user account password?
1. Press Ctrl+Alt+Delete and select „Change a password...“
2. Open User Accounts from Control Panel and select „Change your password"
3. Open Computer Management, navigate to Local Users and Groups, click on Users, right click on Your username and select „Set Password...“
4. All answers are correct
Teisingas: 4

Kategorija: 1.4

Which proposition about safety of password is correct?
1. If password is built according strong password rules, it can be left unchanged indefinitely
2. You should keep your password on the paper in your desk drawer in case you forget it
3. If your most important documents are protected by password, you don’t have to use password to login to your computer
4. Password should be built according strong password rules and should be changed about every three months
Teisingas: 4

Kategorija: 1.5

Which of the mentioned below is the stongest password?
1. ABCD1234
2. acdb132efgh
3. Abcd@123
4. CuCuMbeR
Teisingas: 3

Kategorija: 1.5

Which recommendations should you use for creating strong password?
1. For creating a strong password, you can use a section of consecutive letters from alphabet or consecutive numbers, for example “abcd678”
2. You can use some word to remember it easier
3. The password should consist of no less than 7 symbols; there should be at least one number and one non-alphabet character
4. For the password you should use either capital or non-capital letters
Teisingas: 3

Kategorija: 1.5

To remember your passwords better and keep them safe you should:
1. Use “remember my password” option on internet websites
2. If you are asked to change your password, you should change only several last letters
3. It is advisable to create associations, alter capital and not capital letters, and change some letters to numbers
4. Use the same password everywhere
Teisingas: 3

Kategorija: 1.5

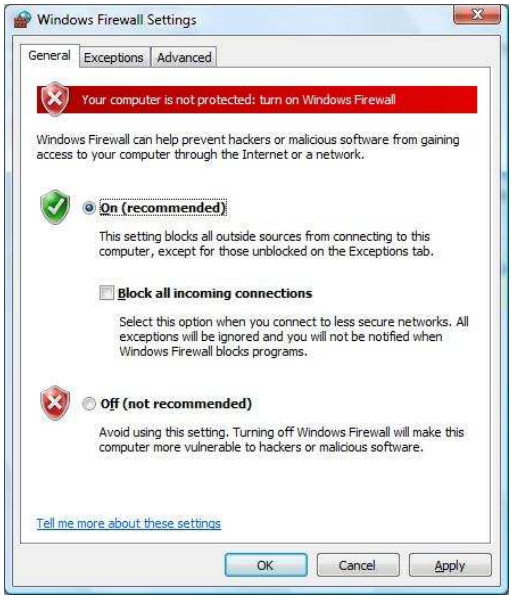
Which recommendations should you use for creating a strong password?
1. A password can be some word which only you may know, for example, maiden name
2. A password can be some numbers which only you may know, for example, your birth date

3. A password can be a word from vocabulary of other languages
4. A password should consist of capital or non-capital letters, some numbers and at least one non-alphabet characters

Teisingas: 4

Kategorija: 1.6

Where do you click if you want to allow a program through Windows Firewall?



Kategorija: 1.6

To protect better and clean your computer from spyware you should:

1. Use firewall
2. Install Windows defender
3. Read e-mail messages by using mail programs only
4. Activate Windows messages

Teisingas: 2

Kategorija: 1.6

What does Windows Defender status “out of date” mean?

Kategorija: 1.6

Click on the option that will scan your computer with Windows Defender?

Kategorija: 1.6

You install a third-party application on your computer. The application uses port 80 to negotiate a listening port. After establishing the listening port, the application uses dynamic ports above 6000. You need to configure Microsoft Windows Firewall to allow traffic for the application. What should you do?

1. Add a program exception for the new application
2. Add a port exception for port 80
3. Disable the Core Networking exception
4. Restore the Windows Firewall defaults

Teisingas: 1

Kategorija: 1.6

You notice a valid program listed in Quarantined items list after you run Windows Defender scan on your computer. You need to use this program on your computer. What should you do?

1. Repair the program from the Programs option in Control Panel
2. Remove the program from the Quarantined items list
3. Restore the program from the Quarantined items list
4. Reinstall the application to another computer

Teisingas: 3

Kategorija: 1.6

Windows Defender scan indentifies one of your applications as having potentially unwanted behaviour. You need to configure to use the application. You also need to stop Windows Defender from alerting you about this application. Which Windows Defender option should you use?

1. Always Allow
2. Quarantine
3. Ignore
4. Remove

Teisingas: 1

Kategorija: 1.7

How can you encrypt a file on an MS Windows computer?
1. Right-click the file that you want to encrypt and then click Properties. On the General tab, click Advanced. Select the Encrypt content to secure data check box
2. Right-click the file that you want to encrypt and then click Encrypt content to secure data
3. Put the file to a *.zip archive and protect the archive with password, then delete the original file on disk, leaving the password protected archive
4. All answers are correct

Teisingas: 1

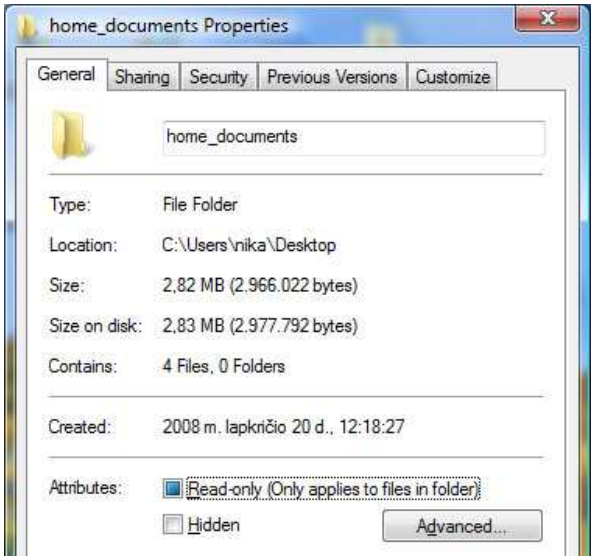
Kategorija: 1.7

Is it possible to protect files from other users of the computer?
1. Yes, you can encrypt files and folders, and other users lose ability to open or copy
2. Only when files are in folder “My Documents”, other user loses ability to read or copy
3. When your login is limited, you cannot protect your files
4. You cannot protect files and folders from other users

Teisingas: 1

Kategorija: 1.7

Where should you click if you want to encrypt a folder?



Kategorija: 1.7

Which tab should you choose if you want to encrypt a folder?

Kategorija: 1.8

Which of the following data media can be protected by password?
1. CD, DVD, USB memory and other external data media if third party tools are used
2. Only USB memory can be protected by password
3. Only access to operating system can be protected by password
4. CD, DVD, USB memory and other external data media can‘t be protected by password

Teisingas: 1

Kategorija: 1.8

You are burning data to a CD. How can this CD be protected against unwanted data access?
1. By choosing CD properties and adding a password
2. By using third party media protection software
3. By changing names of files to be burned on CD
4. By using special CD media for protection

Teisingas: 2

Kategorija: 1.8

You cannot copy files from CD you inserted. What is the reason?
1. CD is password protected
2. CD is encrypted
3. CD or CD drive is corrupted
4. CD is not compatible with your system

Teisingas: 3

Kategorija: 1.8

You are copying data to a USB key. How can this USB key be protected against unwanted data access?
1. By choosing USB key properties and adding a password
2. By using third party media protection software
3. By changing names of files to be burned on USB
4. It is not possible to protect data against unwanted data access

Teisingas: 2

Kategorija: 1.9

Can a USB flash drive contain viruses?
1. Yes, they can contain viruses
2. No, they cannot contain viruses
3. No, if USB Flash memory device is smaller than 1 GB
4. Yes, if USB Flash memory device is produced earlier than 2002

Teisingas: 1

Kategorija: 1.9

If you want to read an unknown CD and want to keep your computer safe:
1. Check the CD with an antivirus software first
2. Copy necessary files from the CD to your computer
3. Ask the CD owner, if there are no viruses on his CD
4. It is safe to use an unknown CD

Teisingas: 1

Kategorija: 1.9

Is it possible to infect computer by using a USB key?
1. Yes, if AutoRun of external data sources is enabled
2. No
3. No, when a USB key is write protected
4. Yes, only when computer is connected to internet

Teisingas: 1

Kategorija: 1.9

What should you do if you know there is a virus in your USB key?
1. Copy the content of the USB key and format it
2. Scan it with Windows Defragmenter
3. Try to disinfect it with antivirus software
4. You can do nothing about it because viruses on USB keys can not be removed

Teisingas: 3

Kategorija: 2.1

What is the difference between a virus and a trojan horse?
1. A virus and a trojan horse are same thing
2. A virus is a type of trojan horse
3. A trojan horse is a type of virus
4. A trojan horse is not a virus

Teisingas: 3

Kategorija: 2.1

What is a virus?
1. A virus is a program or code fragment that can damage your computer hardware and information
2. A virus is a specialized search engine which is intended for industrial espionage
3. A virus is a programming code in the MS Word which is used to spy word documents in your computer
4. A virus is a program which can remove Trojan horses from your computer

Teisingas: 1

Kategorija: 2.1

Which proposition about viruses is correct?
1. May speed up your computer

2. May spread from one computer to another along with some program or file
3. The virus can be used to connect to the Internet for free
4. All above are correct
Teisingas: 2

Kategorija: 2.1

What is a spyware?
1. Spyware gathers user information through the Internet connection without the user's knowledge
2. Spyware replicates itself and in this way infects other computers
3. Spyware sends its copies to all e-mail recipients whose contacts are on the user's computer
4. Spyware disconnects Internet connection
Teisingas: 1

Kategorija: 2.2

Your home computer is connected to the Internet. How is it possible to get infected with a computer virus?
1. A virus may be attached to a received e-mail message
2. A virus may be downloaded without intention while browsing the internet
3. A virus may infect the computer from a CD\DVD or USB flash drive
4. All answers are correct
Teisingas: 4

Kategorija: 2.2

You can get a worm:
1. When you have the spam filter
2. When firewall is disabled
3. When you open MS Word or MS Excel document
4. When you open MP3 file
Teisingas: 2

Kategorija: 2.2

What should you do if you need to identify if malware is causing performance issues on your computer?
1. Run chkdsk on each drive
2. Start a Windows Defender scan
3. View the Microsoft Windows Experience Index of the system
4. View the System Stability Chart on the Reliability Monitor taskpad
Teisingas: 2

Kategorija: 2.2

You can get macro command virus:
1. When macro commands aren't disabled on your computer and when you open an infected document
2. When you run an unknown program which looks like a useful program
3. When you open an MP3 document
4. There are no macro command viruses
Teisingas: 1

Kategorija: 2.3

Which of the mentioned below is an antivirus software?
1. Nod32
2. SQL Server
3. Firefox
4. Ashampoo
Teisingas: 1

Kategorija: 2.3

Which of the mentioned below is an antivirus software?
1. Kaspersky
2. SQL Server
3. Firefox
4. All answers are correct

Teisingas: 1

Kategorija: 2.3

Which answer is not correct talking about computer's protection against spyware?
1. Malware is a useful program for performing utility tasks
2. Malware is some type of operating system
3. Malware is used to detect viruses
4. Malware can harm your data stored on computer

Teisingas: 4

Kategorija: 2.3

Which of the following can be monitored by an antivirus software to detect and block malicious threats?
1. POP3 e-mail traffic
2. Web-based e-mail traffic (web mail)
3. Instant messaging traffic
4. All answers are correct

Teisingas: 4

Kategorija: 2.3

Which scanning method is used for scanning the content of a specific folder?
1. On-access scanning
2. On-demand scanning
3. Unified scanning
4. Cleanup scanning

Teisingas: 2

Kategorija: 2.4

You want to receive MS Windows Vista updates for your computer. How can you do that?
1. You visit an IT store and purchase the updates
2. Type "update" in Command Prompt
3. You open Start menu and select "Install updates and shutdown the computer"
4. You open Control Panel and select "Check for updates" in the Security section

Teisingas: 4

Kategorija: 2.4

You should configure your antivirus software to update automatically:
1. once a week
2. once a month
3. at least once a day
4. every 5 minutes

Teisingas: 3

Kategorija: 2.4

What should you do to receive MS Windows Vista updates for your computer?

1. You visit an IT store and purchase the updates
2. You open Control Panel and select "Check for updates" in the Security section
3. You open start menu and select "Install updates and shutdown the computer"
4. You open Control Panel and select Sync Center

Teisingas: 2

Kategorija: 2.4

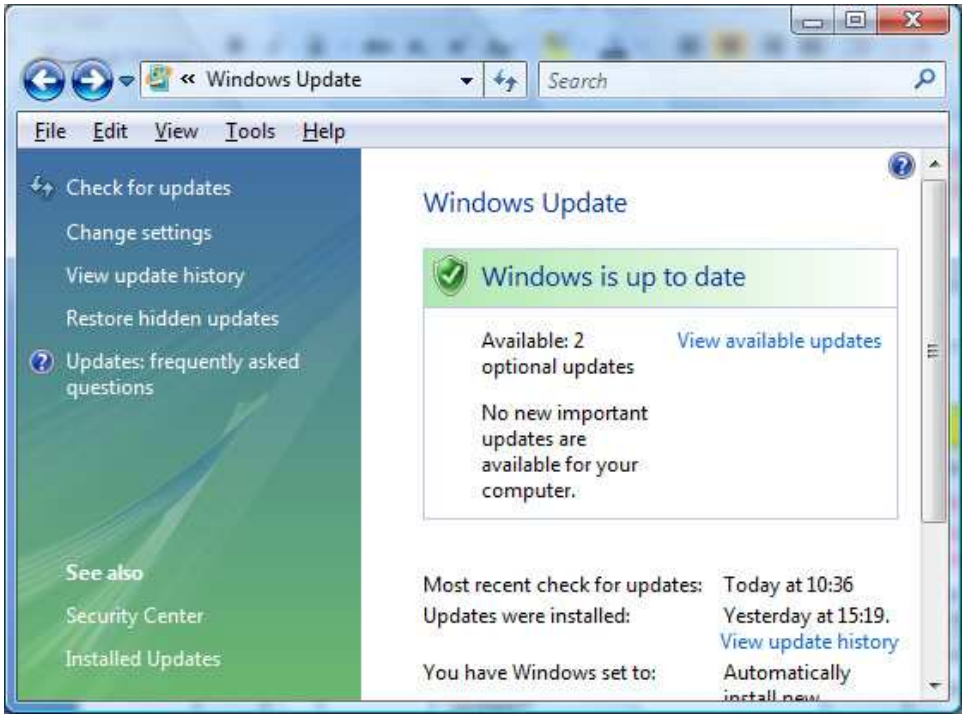
Which programs should you update regularly?

1. Only operating system
2. Only antivirus program
3. Operating system and antivirus program
4. All programs which have an option to be updated

Teisingas: 4

Kategorija: 2.4

Where should you click if you want to enable regular and automatic MS Windows updates?



Kategorija: 2.4

After running Windows Defender on your computer you receive the following warning message: “Windows Defender Definitions haven’t been updated.” You need to ensure that Defender definition files are updated. What should you do?

1. Download and install the latest Windows Defender application from the Microsoft Web site
2. Download and install the appropriate files from Microsoft Windows Update
3. Repair the Microsoft location Finder program
4. Restart the Windows Defender service

Teisingas: 2

Kategorija: 2.4

You share your computer with two users who belong to the Users group. You need to ensure that all users are informed of new updates. What should you do?
1. Disable the Do not display “Install Updates and Shut Down” option in Shut Down Windows Dialog box option
2. Enable the Enable client-side targeting option and specify the target group
3. Enable the Allow non-administrators to receive update notifications option
4. Enable the Turn on recommended updates via Automatic Updates option

Teisingas: 3

Kategorija: 2.5

What should you do first if you suspect that a data file is infected with a computer virus? You already have an antivirus system installed
1. Restart the computer operating system
2. Download and install a different antivirus system
3. Check for updates of the installed antivirus system
4. Delete the file from disk

Teisingas: 3

Kategorija: 2.5

You have a well known antivirus system installed on your computer and active protection turned on. You notice suspiciuous attachments in a letter you have received from an unknown sender. What should you do?
1. Save the files to disk and scan them for viruses
2. Save and open the files because you have an antivirus software installed and active protection turned on
3. Delete the letter immediately, even if you are not sure if it is type of spam
4. Consult your system administrator

Teisingas: 4

Kategorija: 2.5

What should you do if you suspect that a data file is infected with a computer virus?
1. Update your antivirus program and scan your computer with it
2. You should search the Internet for symptoms of infection
3. Consult your system administrator
4. All answers are correct

Teisingas: 4

Kategorija: 2.5

You suspect that your computer is infected with viruses but you do not have antivirus software installed. What should you do?
1. Run an online antivirus scanning program
2. Download and install a new antivirus system and scan for viruses
3. Install an antivirus system from an installation that you have on disk and scan for viruses
4. Format your hard disk and reinstall the operating system

Teisingas: 1

Kategorija: 2.6

You are downloading some files from an ftp site. You are not confident about the site's security
1. You should scan the files on the ftp site
2. You will turn on your antivirus software active protection
3. You will not download the needed files
4. Ftp sites can not have viruses

Teisingas: 2

Kategorija: 2.6

If you have got an e-mail message with an attachment from a colleague but you are not sure about the attachment's safety:
1. You should use an anti-spam program
2. You should use an antivirus real time scanning program
3. You should use an Ad-aware scanning program
4. You should use an Antispyware scanning program

Teisingas: 2

Kategorija: 2.6

You want to download an *.exe file from a website but you are not sure about its safety. What should you do?
1. You should use antivirus real time protection software
2. You should save the file to disk and scan it for viruses
3. You should use an Ad-aware scanning software
4. You should use an Antispyware scanning software

Teisingas: 1

Kategorija: 2.6

What is the most likely reason that your antivirus active protection did not find the virus in an e-mail with a virus attached?
1. Picture files cannot contain viruses.
2. Your friend’s antivirus system is wrong because his computer is already infected with viruses
3. Your antivirus system is not up-to-date
4. You did not have an antispyware system installed

Teisingas: 3

Kategorija: 2.7

What is a proper way to deal with an e-mail message from an unknown sender with an attachment?
1. Add sender‘s contact to address book
2. Delete the message
3. Open the attached file
4. Forward back to sender

Teisingas: 2

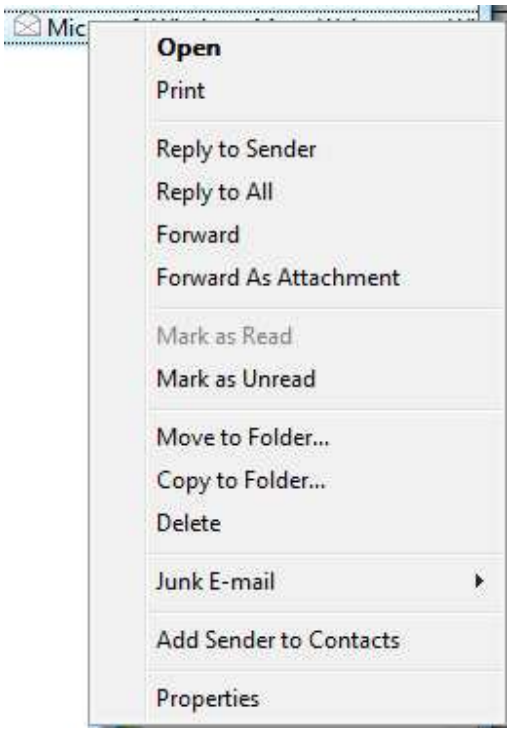
Kategorija: 2.7

If you have got an e-mail message from your bank where you are asked to provide your data, the safest way would be:
1. Reply to the message and give the asked information
2. Call the bank and ask if they have actually sent that e-mail
3. Scan the message with an antivirus program
4. If there is a hyper link, click it and check if that site is actually a bank site

Teisingas: 2

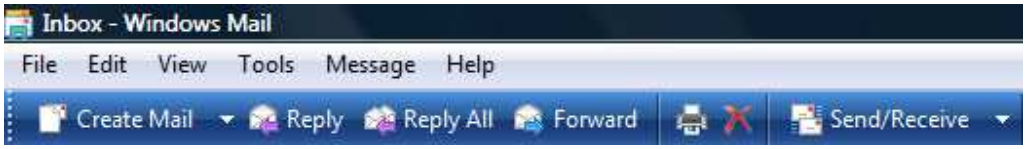
Kategorija: 2.7

Which option would you select to deal with an email message with an attachment from an unknown sender?



Kategorija: 2.7

Which icon would you click to deal with an email message with an attachment from unknown sender?



Kategorija: 2.8

How should you use USB memory media got from your colleague?
1. You shouldn't use other people's USB memory drives
2. Ask colleague if his USB memory drive is safe and then use it
3. Open the memory drive only after scanning it with an antivirus program
4. Open the memory drive without scanning with an antivirus program

Teisingas: 3

Kategorija: 2.8

Which proposition about data media safety is correct?
1. Your computer can be infected when you put an external data media in your computer
2. Your computer can be infected when you open an MP3 from a CD
3. You cannot get a virus from an external data media
4. All above are correct

Teisingas: 1

Kategorija: 2.8

Which proposition about USB key safety is correct?

1. USB keys can be read remotely
2. Information from USB keys can be read or copied by others
3. USB keys cannot be infected with viruses
4. A USB key is the safest data media for keeping information

Teisingas: 2

Kategorija: 2.8

What outcomes may unsafe USB media removal cause?

1. Corrupted files on media
2. Corrupted media
3. Corrupted files on system
4. All answers are correct

Teisingas: 4

Kategorija: 3.1

Which of the following statements concerning spam e-mail and virus-infected e-mail is correct?

1. Spam and virus infected e-mail messages are the same thing
2. Spam messages can contain viruses
3. A virus infected e-mail message is always spam
4. Spam messages can not contain viruses

Teisingas: 2

Kategorija: 3.1

What is spam?

1. Spam is an unwanted e-mail message, frequently with advertising content
2. Spam is a type of virus
3. Spam messages infect your computer
4. Spam messages steal your personal information

Teisingas: 1

Kategorija: 3.1

You have received an e-mail with a link to an online picture of you. What will you do?

1. Follow the link and open the picture
2. Download the content and check it with an antivirus software for possible malware
3. Forward the e-mail to your friends
4. Download the content and then open it locally

Teisingas: 2

Kategorija: 3.1

What types of files attached to e-mail messages are safe to open on your computer?

1. *.com
2. *.exe
3. *.scr
4. None of these are safe

Teisingas: 4

Kategorija: 3.2

If you want to forward an e-mail message with an attached document, you should:

1. Know that you will not violate copyright or ask the e-mail owner for permission to send his attachment
2. Forward this e-mail message without owner permission, because copyright does not apply to e-mail messages
3. Not send this e-mail message, because only message owner can send the original document
4. Send only e-mail message without attachment, because all attachments are owned by e-mail message authors

Teisingas: 1

Kategorija: 3.2

Which of the following statements relating to copyright and forwarding mail is correct?
1. You violate copyrights by forwarding any e-mail message
2. You don’t violate copyrights by forwarding e-mail messages
3. You always violate copyrights, if e-mail message being forwarded has an attachment
4. You can violate copyrights by forwarding e-mail message if there is some confidential information, for example someone’s private data

Teisingas: 4

Kategorija: 3.2

If you create a report and include some part of a document you got by e-mail created by your friend working in another company, ...
1. You violate copyrights, if you use it without friend’s permission
2. You don’t violate copyrights, because copyrights apply only to e-mail message
3. You violate copyrights only if you use information from attachments
4. All answers are correct

Teisingas: 1

Kategorija: 3.2

Can your children freely download digital music and movies from internet?
1. Yes, if content is free from viruses
2. Yes, if it is copyrights free
3. Yes, if content is available on P2P network
4. Only when the content is safe for children

Teisingas: 2

Kategorija: 3.3

What statistical information about child’s e-mail can be reviewed?
1. Date of receiving
2. Sender's e-mail
3. Size of the message
4. All answers are correct

Teisingas: 4

Kategorija: 3.3

Which information about children’s e-mail can you see by using parental software?
1. The date and time an e-mail was sent or received
2. The subject
3. The contents and any attachments
4. All options above

Teisingas: 4

Kategorija: 3.3

If you want to redirect e-mail messages from one mailbox to another in Windows Mail program, …
1. You should create e-mail rule
2. It is possible only during creation of e-mail account in your program
3. You should change your e-mail account configuration by choosing Tools>Options
4. It is not possible

Teisingas: 1

Kategorija: 3.3

How can you redirect e-mail messages from one mailbox to another?
1. Use third party software that is designed to redirect e-mail messages
2. Log in to the mailbox, open the particular message and forward it to another e-mail address
3. Ask system administrator for help configuring your e-mail
4. All answers are correct

Teisingas: 4

Kategorija: 3.4

You want to block e-mail messages from specific senders. What do you do?
1. Use spam filtering software
2. Use an antivirus software
3. Use antispyware system
4. Use a firewall

Teisingas: 1

Kategorija: 3.4

You use Microsoft Windows Mail to download e-mail messages to your inbox. You need to minimize the receipt of e-mail messages that attempt to acquire private financial information. What should you do?
1. Configure Windows Defender to perform a custom scan of potentially malicious e-mail
2. Configure the phishing filter to move the e-mail messages to the Junk Mail folder
3. Configure the Parental Controls Web restriction setting to High
4. Create an Inbox rule that moves potentially malicious e-mail to the Junk Mail folder

Teisingas: 2

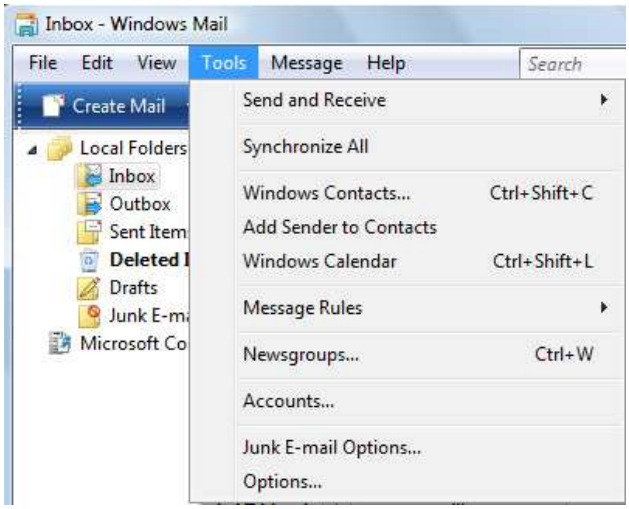
Kategorija: 3.4

If you want to reject e-mail form specific e-mail addresses in Windows Mail program, you:
1. Should create filter rule
2. Should delete these messages manually
3. Cannot reject specific messages
4. Can reject e-mail form specific e-mail addresses using a firewall filter

Teisingas: 1

Kategorija: 3.4

Which menu option should you use, if you want to block e-mail messages from specific senders?



Kategorija: 3.5

What is the difference between private messages and public messages in a forum?
1. Only another registered forum user can read private messages
2. Only other registered forum users can reply to private messages, but all registered users can read content of private messages
3. All registered forum users can read private messages
4. Not registered forum users can see private messages, but cannot read content of these messages

Teisingas: 1

Kategorija: 3.5

It is possible to block private messages between a child and another user?
1. It isn't possible to block private message
2. It is possible to block only e-mail messages
3. It is possible to block only video and audio conference
4. It is possible to block a private message

Teisingas: 4

Kategorija: 3.5

How can you block e-mail messages from a particular user?
1. Add the particular user to the blocked user list in your e-mail messages filter
2. Delete all messages (from inbox and the recycle bin) that come from the particular user
3. Delete the particular user's address form your e-mail system address book
4. Send the particular user an e-mail informing that you do not want to get any more messages from him/her

Teisingas: 1

Kategorija: 3.5

What are the ways to block e-mail messages from unwanted user? Choose all that apply.
1. Block e-mail messages using your antivirus system
2. Add the sender's e-mail address or domain to the White Senders list
3. Configure the e-mail junk filtering setting to High
4. Use a third party software or hardware to block e-mail messages

Teisingas: 4

Kategorija: 3.6

You got an e-mail from unknown sender, and he is claiming that you won a lottery and your personal data is needed to transfer your prize. How should you behave?

1. You should verify this e-mail message with antivirus, and if there are no threats, provide your personal data
2. If you didn't participate in the game you should delete this message
3. You should provide your personal data, if the message doesn't have an attachment
4. You should provide your personal data in any way

Teisingas: 2

Kategorija: 3.6

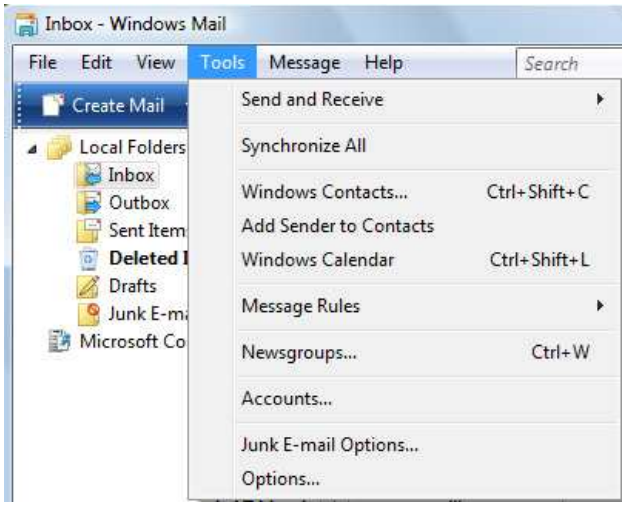
You add a particular e-mail address to the Blocked Senders list in the Microsoft Windows Mail application. You still receive messages from this e-mail address. You need to prevent the receipt of all e-mail messages from this e-mail address. You should:

1. Configure the Microsoft Windows Mail application to delete suspected junk e-mail permanently
2. Configure the junk e-mail filtering setting to High
3. Add the senders e-mail domain name to the Blocked Senders list
4. Remove the senders e-mail address from the Safe Senders list

Teisingas: 4

Kategorija: 3.6

Which menu item would you select to block unwanted e-mail messages?



Kategorija: 3.6

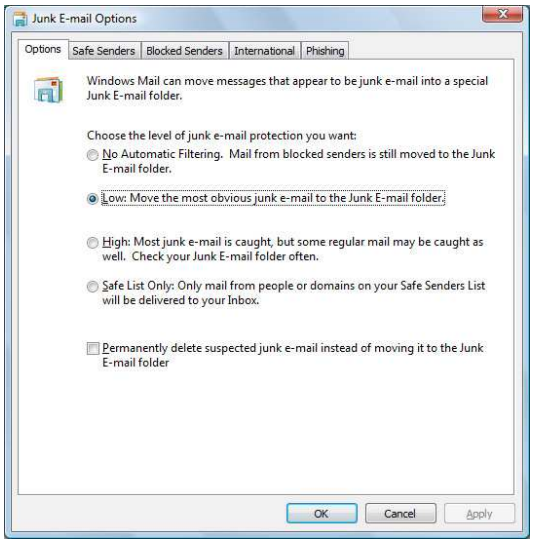
You receive an e-mail message from unknown sender. The e-mail contains no attachment but the is an URL to an Internet shop that looks interesting to you. What should you do?

1. Scan the e-mail message with antivirus software
2. Click the URL directly, because you have a reliable and up-to-date Antivirus ant Antispyware software installed on your computer
3. Copy the URL to your browser address bar and then open it
4. Delete the e-mail message and consider blocking the sender

Teisingas: 4

Kategorija: 3.6

Where would you click if you want e-mail messages from specific senders not to be treated as junk?



Kategorija: 3.7

You want to receive a file over instant messenger safely. How do you protect against computer viruses?
1. Instant messengers have integrated antivirus systems installed
2. Viruses can not be received over instant messengers
3. Files can not be sent over instant messenger
4. You have to use a separate antivirus system and active protection turned on

Teisingas: 4

Kategorija: 3.7

Which of the following protects against Instant Messaging security threats?
1. Always ask sender if it is safe to open the attachment
2. If a person on your Buddy list is sending strange messages, files, or web site links, terminate your IM session
3. Do not install several different Instant Messaging software on one computer
4. All answers are wrong

Teisingas: 4

Kategorija: 3.7

Which of the following is not an Instant Messaging security threat?
1. Confidential information leak
2. Virus attack
3. Phishing
4. Pop-up

Teisingas: 4

Kategorija: 3.7

How can you protect against unwanted Instant Messages senders? Choose all that apply.
1. Check option “Only allow people in my contact List to contact me”
2. Add unwanted senders to White users list
3. Associate your Antivirus software with your Instant Messaging software
4. Block port 80 in your firewall options

Teisingas: 1

Kategorija: 3.8

What security means can a mobile phone have?
1. Spy-blocker system
2. An Antispyware software
3. Antivirus software
4. A Firewall

Teisingas: 3

Kategorija: 3.8

Your mobile phone has a Bluetooth technology. What are the ways to protect against mobile attacks via Bluetooth?
1. Install antivirus software on your mobile phone
2. Turn on Bluetooth connection on your mobile phone
3. Turn on "Visible to other devices" option in your mobile phone Bluetooth options menu
4. Protect Bluetooth connections to your mobile phone using a complex passkey

Teisingas: 4

Kategorija: 3.8

What security threats apply for data stored on mobile phones?
1. Phone calls from unknown callers
2. Mobile phone viruses
3. Replacement of mobile phone battery
4. All mentioned above

Teisingas: 2

Kategorija: 3.8

What type of connection applies to mobile phones?
1. Bluetooth, Infrared and IDE
2. Ultrared and Redtooth and GPRS
3. Cable-connect, Bluetooth and GPRS
4. IDE, SATA and 3G

Teisingas: 3

Kategorija: 3.9

What you should to do if you discovered or suspect dangerous or illegal content?
1. Contact responsible institution
2. Inform all your friends by email
3. Nothing to do
4. Click Ctrl+Alt+Delete

Teisingas: 1

Kategorija: 3.9

What institution is responsible for collecting and reacting to illegal content reports?
1. Ministry of Education
2. Police
3. Private detective agency
4. Internet Safety Hotline

Teisingas: 4

Kategorija: 4.1

Which is the optimal way configuring your Internet browser to treat with web ActiveX controls?
1. Block unsigned AxtiveX controls

2. Block signed AxtiveX controls
3. Allow unsigned AxtiveX controls
4. Prompt for unsigned AxtiveX controls
Teisingas: 4

Kategorija: 4.1

What does HTTPS have in common with HTTP?
1. It is not a separate protocol but refers to the combination of a normal HTTP interaction over an encrypted SSL or TLS connection
2. It is the same protocol as HTTP
3. It has nothing in common because it is a Header To Top Page Security protocol
4. HTTPS is an analog protocol like HTTP, but used on MAC platforms
Teisingas: 1

Kategorija: 4.1

The pop-up blocker is enabled on your computer. How can you always view pop-ups from a Web site and still maintaining the highest level of security?
1. Visit the Web site and select the Always allow pop-ups from this site option
2. Enable the Automatic Website Checking option on the Phishing filter
3. Add the URL of the Web site to the list of trusted sites
4. Disable the pop-up blocker
Teisingas: 1

Kategorija: 4.1

You need to reduce the level of access that malicious Web site might have to your computer. What should you do?
1. Confirm that Microsoft Windows Internet Explorer Protected Mode is enabled on the Internet security zone
2. Start a Windows Defender scan
3. Enable Microsoft Windows Internet Explorer Phishing Filter
4. Enable Microsoft Windows Internet Explorer Pop-up Blocker
Teisingas: 1

Kategorija: 4.2

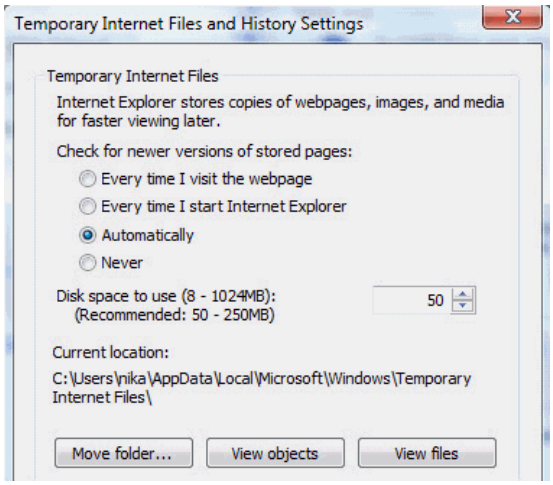
What are HTTP cookies not used for?
1. Authenticating
2. Session tracking
3. Maintaining information about users
4. Playing flash animation during browsing
Teisingas: 4

Kategorija: 4.2

You need to prevent additional windows from opening automatically when you visit a web site. You use Microsoft Internet Explorer as your browser. What should you do?
1. Configure Windows Security Center to not display antivirus and firewall warnings
2. Configure Windows Firewall to block inbound traffic from TCP port 80
3. Configure Internet Explorer to block pop-up windows
4. Configure Internet Explorer to reject cookies from Web sites
Teisingas: 3

Kategorija: 4.2

Where can you see cookies you have accepted? Click on a particular place in the picture



Kategorija: 4.2

Choose the best definition for an Internet cookie
1. A very small text file placed on your hard drive by a Web Page server
2. A very small text file placed on your hard drive by a system administrator
3. A *.zip file placed on your hard drive by a Web Page server
4. An image file placed in Temp directory to make picture from web loading faster

Teisingas: 1

Kategorija: 4.3

What can happen if you disclose your personal data about your name, nickname, surname, date of birth, credit card number on the Internet?
1. You can get charged for Internet purchases that you did not do
2. You can get your Windows password guessed
3. All answers are correct
4. Nothing serious can happen

Teisingas: 1

Kategorija: 4.3

What kind of personal data is dangerous to reveal on Internet? Choose all that apply
1. Nickname
2. Credit card number
3. Shoe size
4. All answers are correct

Teisingas: 2

Kategorija: 4.3

Which of the mentioned below belong to a definition “personal data”?
1. Nickname
2. Credit card number
3. Hobbies
4. Insurance number

Teisingas: 4

Kategorija: 4.3

You visit an online shop to choose and buy a book. The automatic guide asks you to enter your interests and taste about books. How do you act to keep your personal data safe?
1. You may skip it or complete the questionnaire because this is not personal data disclosure
2. Use only Internet Explorer for buying online
3. Use only Firefox for buying online
4. Choose a different online book shop
Teisingas: 1

Kategorija: 4.4

How should you protect yourself from evel-minders who may steal and use client information?
1. Not turn on the Internet on your computer
2. Change your LAN IP address
3. Install Antivirus system
4. Not leave your personal Client information on the Internet
Teisingas: 4

Kategorija: 4.4

You receive an e-mail from your bank operator informing about a need to change your Internet banking account password and secret keys. You are asked to send the old keys and password first. What do you do?
1. Visit your Internet banking site and change the security information
2. Send the data that you are asked for
3. Call the telephone number included in the e-mail
4. Block the senders e-mail address on your e-mail system
Teisingas: 4

Kategorija: 4.4

You received an e-mail from Internet shop where you have an account. E-mail asks you to confirm your credit card information and enter it again. What will you do?
1. Follow steps indicated in e-mail and confirm credit card information
2. Ignore e-mail and block sender
3. Check e-mail with antivirus program and if no viruses found confirm credit card information
4. Reply e-mail and ask more details regarding this issue, update your credit card info only when you receive confirmation e-mail from the sender
Teisingas: 2

Kategorija: 4.4

You receive an e-mail from a person, asking you to open empty bank account on your name and give the access on this account for the person. For your help you will receive 100 USD to your other personal account. What will you do?
1. Open account on my name and give access to the person. Operation is safe as my new account will be empty
2. Wait for the 100 USD payment first and then give the person access for my new empty account
3. Use your current bank account for this operation but remove your own money first
4. Ignore the request and delete the e-mail
Teisingas: 4

Kategorija: 4.5

What key do you need to know if you want to connect to a secured wireless network?
1. WEP key
2. PCI key
3. RGB key
4. MAC key
Teisingas: 1

Kategorija: 4.5

Choose a correct sentence about data encryption on Internet
1. Encryption is the translation of data into a secret code
2. To read an encrypted data, you must have access to a powerful server, what enables to decrypt it
3. Encryption is never used to achieve data security
4. Encrypted data is called archive

Teisingas: 1

Kategorija: 4.5

Which from the list is not a wireless key?
1. WEB-TKIP
2. WEP-PSK
3. WEP
4. WPA

Teisingas: 1

Kategorija: 4.5

What is RSA?
1. File sharing network working directly between users
2. Algorithm for public-key cryptography
3. Secure network protocol
4. File protection software

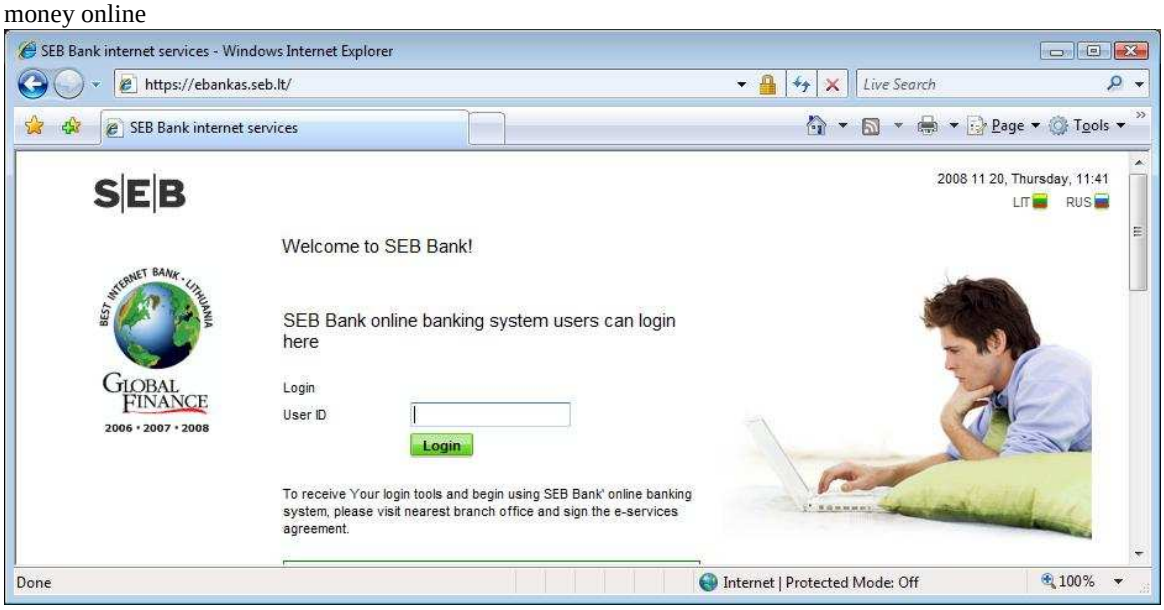
Teisingas: 2

Kategorija: 4.6

Where would you click to check if website certificate is valid?

Kategorija: 4.6

The web login to electronic bank is displayed in the picture below. How do you know if it is a safe way or not to treat your money online



Kategorija: 4.6

Which of the mentioned below is an example of a safe Internet banking site?

1. https:\\www.bank.com
2. http:\\www.bank.com
3. ftp:\\www.bank.com
4. http:\\https.bank.com

Teisingas: 1

Kategorija: 4.6

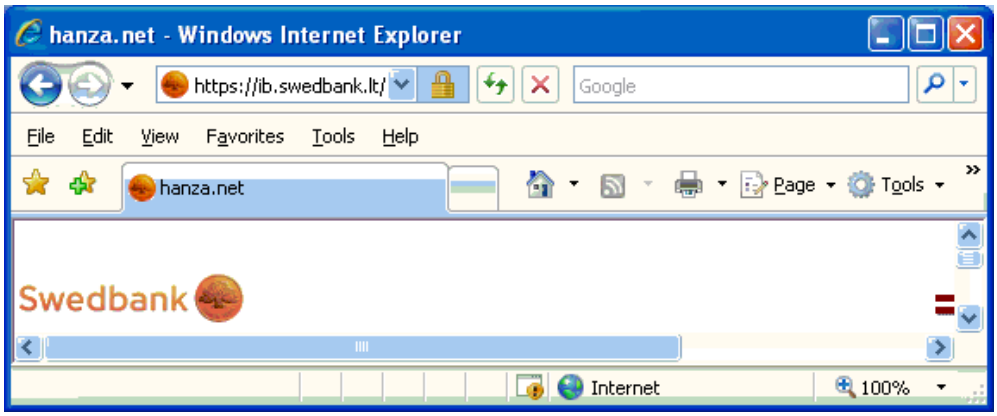
How many times you may be asked to enter security codes for single operation (login)?

1. One time
2. Two times in a row
3. Three times in a row
4. Four times in a row

Teisingas: 1

Kategorija: 4.6

This is a bank site. What shows that you are connected using safe connection?



Kategorija: 4.7

When making an Internet transaction using a debit card, what information can you be asked to input?
1. All codes from your generated codes card
2. Your car VIN number
3. One of the codes from your generated codes card or code generator
4. Your OS password

Teisingas: 3

Kategorija: 4.7

You want to buy an airplane ticket on an online ticket shop. You are asked for a credit card security number. Where do you need to look for it?
1. On the front side of your credit card
2. On the back side of your credit card
3. Login to your Internet banking account to get it
4. See your Credit Card agreement papers

Teisingas: 2

Kategorija: 4.7

You are buying antivirus online using your credit card. You have to enter security code. Where will you look for it? Click on the image

Kategorija: 4.7

You have credit card of Citi bank and you want to buy a gift on Internet. Which part of the website explains whether you can pay with your card or not. Click on the image

Kategorija: 4.8

Which exceptions should you enable, if you need to configure Microsoft Windows Firewall to allow technicians to remotely control your computer?

1. Remote Registry Service
2. Remote Administration
3. Remote Service Management
4. Remote Assistance

Teisingas: 4

Kategorija: 4.8

You want to contact the service administrator of an online store. Where will you click?

Kategorija: 4.8

You are having problems connecting to your online banking system while Internet connection is available. How will you solve these problems?

1. Call online support of the bank
2. Call to Internet provider
3. Restart your computer
4. All answers are correct

Teisingas: 1

Kategorija: 4.8

You suspect that someone has stolen your credit card information. What will you do?

1. Call police and ask to catch thieves
2. Go to online banking system and change your card number
3. Call your bank and ask to block your card
4. Do nothing and wait till thieves use your credit card and then call police to catch them

Teisingas: 3

Kategorija: 4.9

Who would you contact if you would discover or suspect dangerous or illegal content on a website?

1. Police
2. Regional hotline for illegal content
3. Website administrator
4. All options above

Teisingas: 2

Kategorija: 5.10

How long do instant messaging programs keep chat history?

1. For 1 week
2. For 24 hours
3. Depends on configuration of chat history keeping

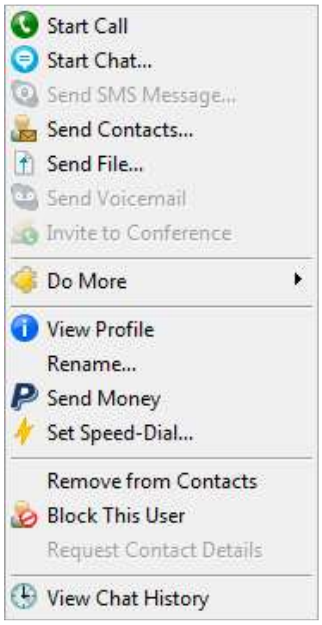
4. Instant messaging programs do not keep history
Teisingas: 3

Kategorija: 5.10

You would like to know what conversations were made using the instant messenger. Where will you look for it?
1. Recent items folder in your OS
2. Messenger history
3. Web browser history
4. Temporary Internet files folder
Teisingas: 2

Kategorija: 5.10

Where would you click to check chat history for selected Skype user?



Kategorija: 5.10

You wish to check which files were sent to your computer via instant messenger file sharing function during the last week. Which function will you check?
1. Personal profile
2. Messenger history
3. Messenger options
4. Advanced options
Teisingas: 2

Kategorija: 5.12

Which search engine you would recommend to your children?
1. www.yahoo.com
2. www.google.com
3. www.askkids.com
4. www.cracksearch.ws
Teisingas: 3

Kategorija: 5.12

Which search engine you would recommend to your children?
1. www.lycos.com
2. www.kidsclick.org
3. www.ask.com
4. go.com

Teisingas: 2

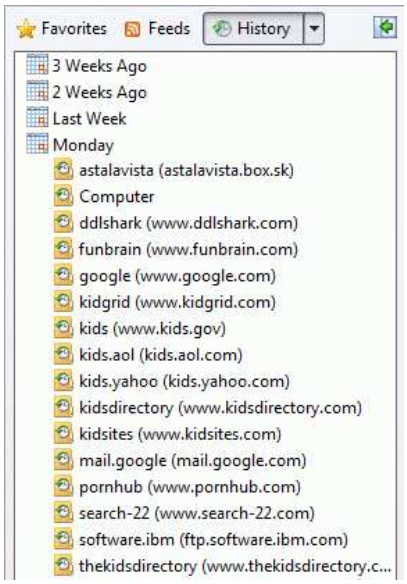
Kategorija: 5.12

Which website should not be used by children browsing the Internet?
1. http://www.cracks.am
2. kids.yahoo.com
3. www.funbrain.com
4. www.kids.gov

Teisingas: 1

Kategorija: 5.12

You are checking which web pages your child browsed on Monday. Which history item would you check in more details to see if a child browsed something inappropriate?



Kategorija: 5.13

In a moderated public forum you found a post with links inviting to visit website with nudity content. Who will you contact?
1. Message poster
2. Police
3. Forum Moderator
4. System Administrator

Teisingas: 3

Kategorija: 5.1

What is the best way to protect children online?
1. Use latest children protection software
2. Always supervise and teach children safety on Internet

3. Use latest firewall and antivirus software
4. Use children protection software with as much supervision as possible
Teisingas: 4

Kategorija: 5.1

Your child browses the web and you notice a pop-up window on the screen containing pornography. What action do you take?
1. Ask your child to leave the room, and click on the link in the pop-up page
2. Ignore the fact and pretend that nothing happened
3. Close the pop-up window
4. Talk to your child about dangers (malware, financial scams) that may be encountered browsing pornography sites
Teisingas: 4

Kategorija: 5.1

What you should talk about with your child prior allowing him to use Internet?
1. About benefits of global information network
2. About possibilities to download latest music and movies
3. About possible dangers on internet – viruses, malware
4. All answers above are correct
Teisingas: 4

Kategorija: 5.1

What you should talk about with your child prior allowing him to use Internet?
1. About safe usage of e-mail
2. About illegal content on Internet
3. About installing illegal programs
4. All answers above are correct
Teisingas: 4

Kategorija: 5.2

You have received an e-mail informing you that you have won in an Internet lottery. What action will you take?
1. Contact senders to claim your prize
2. Forward e-mail to your best friend
3. Do nothing
4. Delete the e-mail and add the sender to blocked senders list
Teisingas: 4

Kategorija: 5.2

What action should you or your child take if harassing messages are received from unknown sender?
1. Respond and help sender
2. Forward his message to other person or organization that might help them
3. Suspect scam or abuse and ignore message
4. Check message using latest software for viruses or spyware
Teisingas: 3

Kategorija: 5.2

Which measure is sufficient to ensure that a child can safely browse Internet?
1. Child should browse Internet daytime hours only
2. Child should browse using only one safe search engine only
3. Child should browse Internet only with his friends
4. None of these options is safe
Teisingas: 4

Kategorija: 5.2

Your child browses the web and you notice a pop-up window on the screen containing pornography. What action do you take?

1. Ask your child to leave the room, and click on the link in the pop-up page
2. Close the pop-up window; consider blocking pop-ups and the page that contained this particular pop-up
3. Close the pop-up window. Tell your child that you forbid him/her to view any kind of pornography sites
4. Close the pop-up window

Teisingas: 2

Kategorija: 5.3

Which one should you check to find out what Internet sites, have been opened recently?

1. Internet Explorer Favorites
2. Internet Explorer History
3. Windows Defender
4. HTTP Cookies

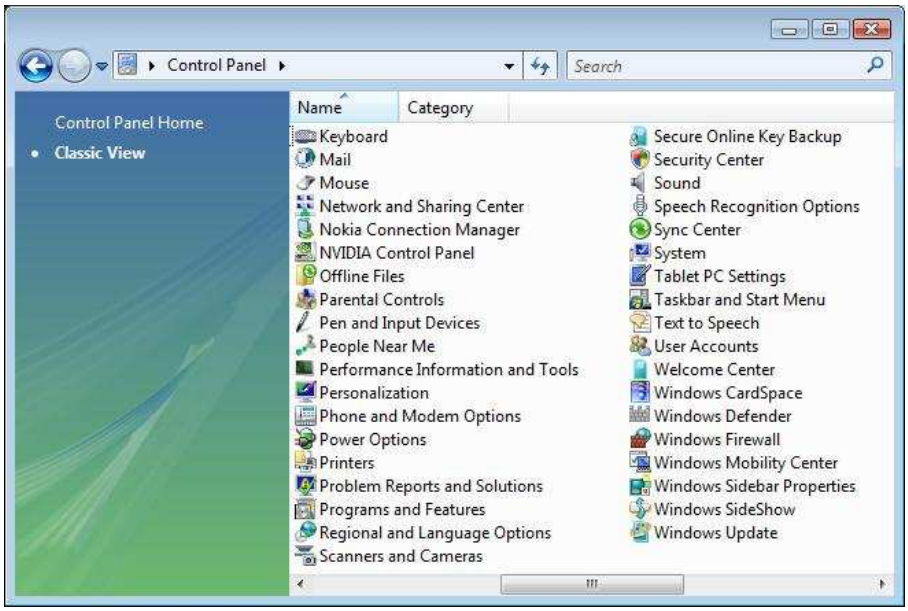
Teisingas: 2

Kategorija: 5.3

You want to view all the history of pages browsed with Mozilla Firefox. Where do you need to click?

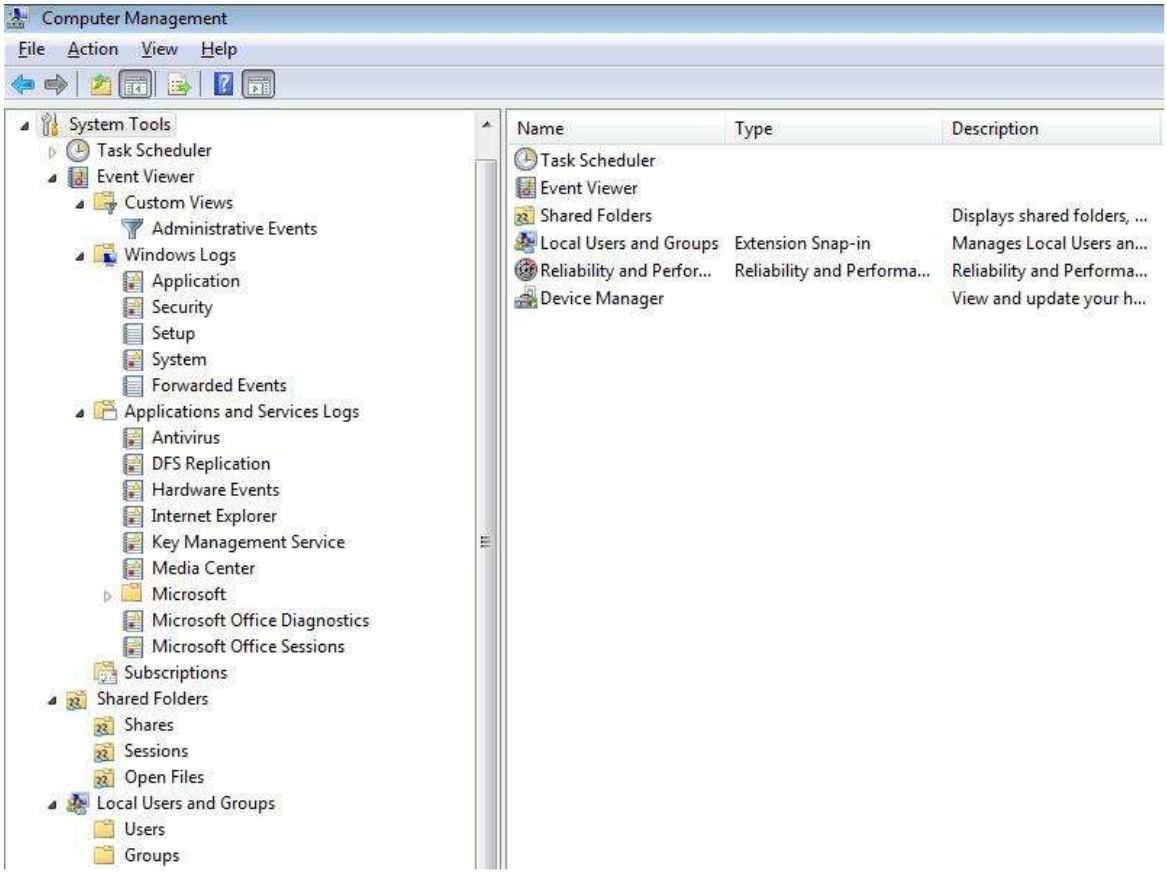
Kategorija: 5.3

You want to view all installed applications on a Windows Vista computer. Where do you need to click?



Kategorija: 5.3

You want to view what users have been connected to a Windows Vista computer. Where do you need to click?



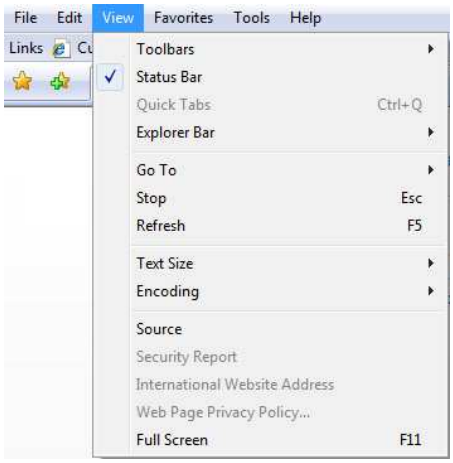
Kategorija: 5.4

What do you need to press, if you want to access Internet Explorer History?
1. Ctrl+Shift+H
2. Ctrl+H
3. Windows key+H
4. Alt+H

Teisingas: 1

Kategorija: 5.4

Which item should you use, if you want to access Internet Explorer History?



Kategorija: 5.4

Which item should you use, if you want to access Internet Explorer History?

Kategorija: 5.4

Where should you click, if you want to access Internet Temporary Files?

Kategorija: 5.5

What do you need to click, if you want to prohibit usage of Internet Explorer for a particular user? Click on a particular place in the picture.

Kategorija: 5.5

You implement Parental Controls game restrictions for your child on your computer. You select the TEEN rating game restrictions. Your child is still able to run some inappropriate games. You need to prevent access to all inappropriate games. What should you do?

1. Configure Microsoft Internet Explorer in Protected Mode
2. Configure Windows Defender to remove high alert items
3. Configure the Game Restrictions parental control to block games that have intense violence

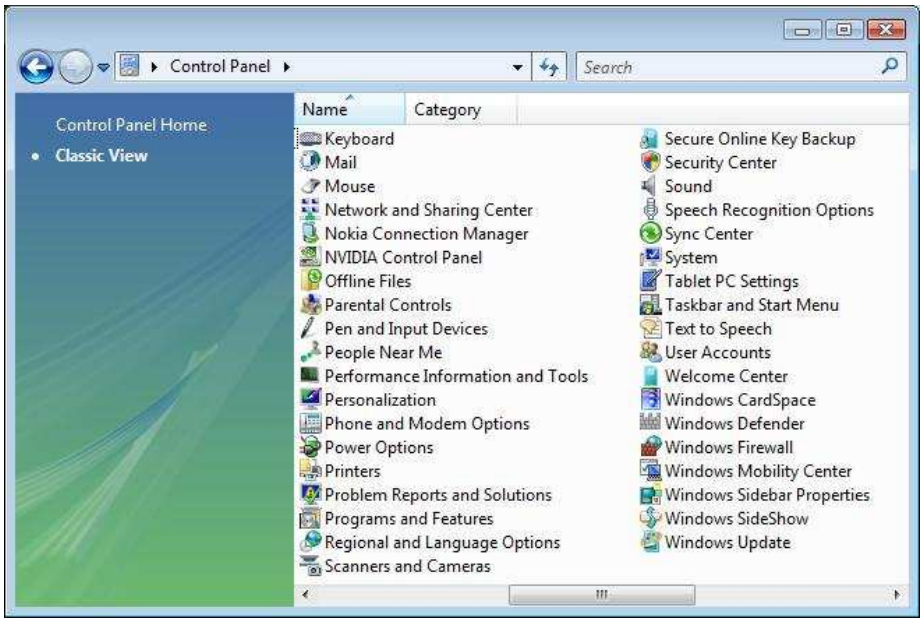
4. Configure the Game Restrictions parental control to disallow games that are not rated
Teisingas: 4

Kategorija: 5.5

You configure parental controls on your computer for your child's user account. Your child logs on with a different account and is able to access inappropriate Web sites. You need to ensure that your child cannot access inappropriate Web sites. What should you do?
1. Configure Web sites you approve of in the list of Trusted Sites of Microsoft Windows Internet Explorer
2. Use password protection for all user accounts
3. Disable the default administrator account
4. Enable Microsoft Windows Firewall
Teisingas: 2

Kategorija: 5.5

You want to block the usage of some specific programs for your child. Where do you need to click?



Kategorija: 5.6

Which one is not children protection software?
1. MS Windows Parental Controls
2. Tiscali Child Protection
3. iProtectYou
4. Skype
Teisingas: 4

Kategorija: 5.6

What can children protection software do?
1. Clean computer from viruses
2. Scan OS for updates
3. Block online chat containing inappropriate words
4. Make computer boot faster
Teisingas: 3

Kategorija: 5.6

What can children protection software do?
1. Block e-mails, if they contain inappropriate words
2. Control the list of programs that can have access to the Internet
3. Set a schedule to specify days and times when on-line activity is allowed
4. All are correct

Teisingas: 4

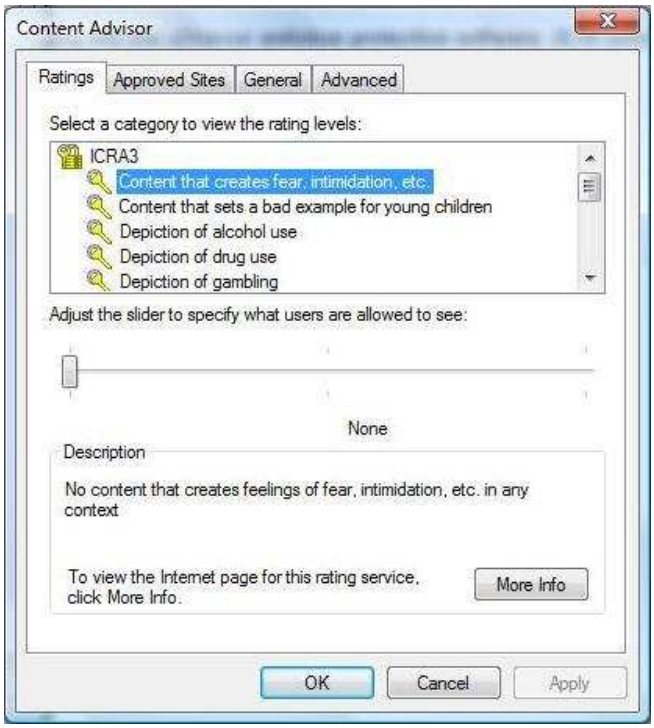
Kategorija: 5.6

What can you not do with Windows Vista Parental Controls software?
1. Restrict the websites that children can visit
2. Set time limits to control when children are allowed to log on to the computer
3. Control access to games
4. Control files that children create

Teisingas: 4

Kategorija: 5.7

What do you need to click, if you want to prohibit access to a website? Click on a particular place in the picture



Kategorija: 5.7

You are browsing a website and new windows to other websites are constantly opening. What integrated browser tool will you use to stop this?
1. Phishing filter
2. Pop-up blocker
3. Browser history cleaner
4. Favorites organizer

Teisingas: 2

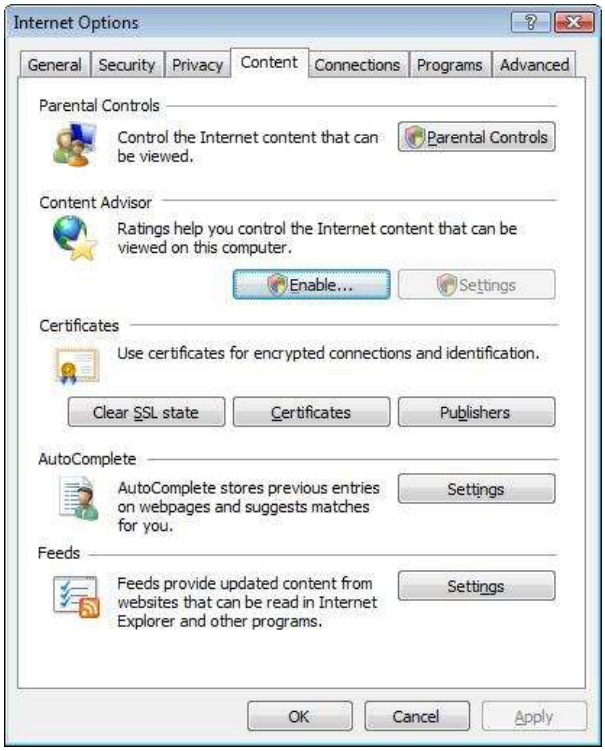
Kategorija: 5.7

How can you block specific websites using Mozilla Firefox Internet browser?
1. You can block access to a website by adding it to your Windows HOSTS file
2. You can block the cookies from the specific website, to block all sites
3. Download and use the block site add-on from Mozilla
4. All answers are correct

Teisingas: 4

Kategorija: 5.7

What do you need to click, if you want to prohibit access to websites by content? Click on a particular place in the picture.



Kategorija: 5.8

Which program from the list is defensive software?
1. Skype
2. Internet Explorer
3. Kaspersky Antivirus
4. Command Prompt

Teisingas: 3

Kategorija: 5.8

You suspect that your computer might be infected with worms. Which software from the list will help you to clean your computer?
1. BitDefender Antivirus
2. Zero Trace
3. HijackThis
4. Spyware Terminator

Teisingas: 1

Kategorija: 5.8

You want to protect your files/folders from opening. What software will you use?
1. Norton Antivirus
2. HijackThis
3. File Defender
4. Zone Alarm

Teisingas: 3

Kategorija: 5.8

Antivirus software can protect computer from unauthorized access on the network. Is this correct?
1. Not correct, firewall should be used for that
2. Correct if latest antivirus software is used
3. Correct if antivirus is used together with antispam
4. Correct if antivirus is used together with antispyware

Teisingas: 1

Kategorija: 5.9

Which program would you use to protect your computer?
1. Zero Trace
2. Ad-Aware
3. Ashampoo
4. All of these programs

Teisingas: 2

Kategorija: 5.9

You are receiving spam e-mails from random senders with links to abusive or dangerous content and illegal websites. What will you do?
1. Add each sender to blocked senders list and delete e-mail
2. Reply sender and ask to stop sending unwanted e-mails
3. Use adaptive spam blocking software to filter illegal e-mails
4. Contact sender‘s domain administrator and request him to deal with this problem

Teisingas: 3

Kategorija: 5.9

Your child has had his/her friends at home. They were playing on a computer and browsing Internet. What software will you use to check if there is any Trojan Horse software installed on your computer?
1. Antivirus software
2. Spam blocker software
3. Firewall software
4. Anti-spyware software

Teisingas: 4

Kategorija: 5.9

You want to protect your computer from unauthorized access on the network. What software will you use?
1. Antivirus software
2. Spam blocker software
3. Firewall software
4. Anti-spyware software

Teisingas: 3

e-Guardian Review Sheet

Product	e-Guardian
Module	n/a
Test No	1
Software Version Tested on	0
MQTB Reviewer Name	Frank Mockler
Review Date	2009.05.19

Phase 1

General Comments	
Branding of the programme should not be "ECDL". It would be permitted to use the "Endorsed by the ECDL Foundation" logo in conjunction with the test, however.	
There seems to be a significant lag time between questions - more than 5 secs?	
If you use Mozzilla Firefox as your browser, you cannot see the menu options on the right hand side after logging on.	

Question	Review Comment
3	Which program would you use to protect your computer? In this question, all the answers relate to proprietary software names - will these all be commonly identified by candidates?
4	How should you protect yourself from evel-minders who may steal and use client information? "evel-minders" does not make sense - "malacious individuals" would be better. Also, the third and fourth options should read "Do not"
5	"You are receiving spam e-mails from random senders with links to abusive or dangerous content and illegal websites. What will you do?" Change second part of sentence to "What should you do?"
7	Your child browses the web and you notice a pop-up window on the screen containing pornography. What action do you take? Change first sentence to "Your child is browsing the web…"

8	Which item should you use, if you want to access Internet Explorer History? Many users may have a menu button related to the favourites centre, and may navigate to history that way. Also, a standard terminology such as "Where do you click" should be used for all questions requiring an interaction.
10	What outcomes may unsafe USB media removal cause? Reword to What may be the outcome of unsafely removing USB media?
11	The pop-up blocker is enabled on your computer. How can you always view pop-ups from a Web site and still maintaining the highest level of security? Change "and still maintaining" to "while still maintaining".
12	You receive an e-mail from a person, asking you to open empty bank account on your name and give the access on this account for the person. For your help you will receive 100 USD to your other personal account. What will you do? Change to You receive an e-mail from a person, asking you to open empty bank account in your name and to give access to this account to the person. For your help you will be sent 100 USD to your other personal account. What should you do? Also, replace "me" and "my" with "you" and "your" in the options for consistency.
13	You want to block the usage of some specific programs for your child. Where do you need to click? Change to You want to prevent your child from using some specific programs. Where do you need to click?
14	Is it possible for a user with administrator account to open and read encrypted documents? Change to Is it possible for a user with an administrator account to open and read encrypted documents?
18	Which of the mentioned below belong to a definition “personal data”? Change to Which of the following is personal data? Also, the definition of personal data here seems very restrictive, and three of these would be commonly viewed as personal data.
20	What is the most likely reason that your antivirus active protection did not find the virus in an e-mail with a virus attached? Change to What is the most likely reason that your active antivirus protection did not find a virus in an e-mail attachment?
22	Which of the following statements relating to copyright and forwarding mail is correct? None of the options seems to be correct in all circumstances.
23	You want to receive MS Windows Vista updates for your computer. How can you do that? Will all candidates be using Windows Vista?
24	Which of the mentioned below is an example of a safe Internet banking site? One of the options below is using a secure http conntection. However, the url might not be safe if, for example, it was bogus and distributed by phishing.
27	What is a spyware? Change to What is spyware?
End of test	The candidate should be told explicitly that they have passed the test. The button the close the test window should also be clearly labelled.

Results tab	Will candidates have access to the specific questions that they get right or wrong after the test? This would breach test integrity. If the fail, they could however get information on the areas of the syllabus that require their revision.