Ügyelj számítógéped biztonságára!

Pšenáková Ildikó[1], Szabó Tibor[2]

[1]ildiko.psenakova@gmail.com
VÚSO S.R.O., BRATISLAVA, SZLOVÁKIA
[2]tszabo@ukf.sk
UKF FSŠ NITRA, SZLOVÁKIA

Absztrakt. Hogyan tudja megvédeni az egyszerű felhasználó a saját számítógépét az arra irányuló támadásoktól? Mire kell figyelnie böngészés közben, hogy biztonságban tudja adatait? Ezekre és sok más kérdésre is megtalálják a választ azok a nem informatikus felhasználók, akik részt vesznek, ill. vettek a „Számítógépes biztonság" című e-learninges kurzuson, melynek néhány eredményét tárgyalja a tanulmány.

1. Bevezetés

Ma már szinte nincs olyan foglalkozás, munkahely, ahol ne használnának számítógépet, de otthonainkban is mindennapi használati tárggyá vált a számítógép. Az is tagadhatatlan tény, hogy szinte nincs olyan számítógép, amely ne tudna kapcsolódni a világhálóhoz. Az internet tette lehetővé az ún. „home office"-t (távmunkát), a távoktatást (e-learning), az egyszerű és szinte mindennapos kapcsolattartást rokonainkkal, ismerőseinkkel, barátainkkal, de a számítógépes hálózatnak és az internetnek köszönhetően intézhetjük banki számláinkat, mindennapi ügyeinket, böngészhetünk, szükséges adatokat kereshetünk, sőt a szórakozási igényeinket is kielégíthetjük.

Sajnos azonban van az internetnek árnyoldala is. Nem ismeretlenek a számítógép és az internet felhasználói számára például a számítógépes vírus, spam, phishing, hacker, cracker és hasonló szavak. Miközben gyanútlanul szörfözünk a neten, vagy olvassuk e-maileinket, kiváló célpontjai lehetünk a kíváncsiskodó hackereknek, vagy a kimondottan rosszindulatú crackereknek. Az ilyen és hasonló tevékenységeket a számítógépes zsargonban támadásoknak vagy behatolásoknak nevezik. Ezek a nem kívánt behatolások vagy behatolási próbálkozások révén illetéktelenek kezébe kerülhetnek személyes és fontos adataink, fotóink, de akár a bankszámlánkhoz való belépési adataink is. Ezért nagyon fontos, hogy ügyeljünk számítógépünk biztonságára és tegyünk meg mindent az adatlopás megelőzése érdekében.

Sokan azonban addig nem tesznek szinte semmit sem számítógépük biztonságáért, míg nem lesznek ilyen támadás áldozatai. Utólag aztán már elgondolkodnak, hogy mit kell tenniük, hol keressenek segítséget és gyakran szakemberhez fordulnak. De sokan megoldják a problémát egy antivírus szoftvert telepítésével. Tudjuk viszont, hogy önmagában a szoftver nem elég a baj megelőzésére, hiszen az nem képes megakadályozni a tudatlan vagy jóhiszemű felhasználót például abban, hogy egy e-mailben jött felkérésre elküldje a jelszavát vagy akár más adatokat olyan személynek, aki rendszergazdának adja ki magát. Egy másik gyakori példa, hogy egy „álhonlap" űrlapját kitöltve tudtunkon kívül adjuk ki adatainkat (phishing). Az ilyen és még sok más támadás sikeres elhárítása csak akkor lehetséges, ha a kiszemelt áldozat felismeri a fenyegető veszélyt, vagy legalábbis gyanút fog. Ehhez azonban a felhasználónak legalább egy minimális tudással kell rendelkeznie a számítógépes biztonságról.

A fentiekben taglalt problémák ösztönöztek minket arra, hogy létrehozzunk egy LMS (Learning Management System) rendszerben működő e-learning kurzust, amelyben tananyag formájában dolgozzuk fel az adott problémakört a laikus (nem informatikus) felhasználók szá-

mára. A kurzus elvégzése, illetve a tananyag elsajátítása után olyan tapasztalatokkal rendelkeznének a résztvevők, amelyek segítenék őket az ezt követő időszakban a támadások felismerésében.

2. A projektről

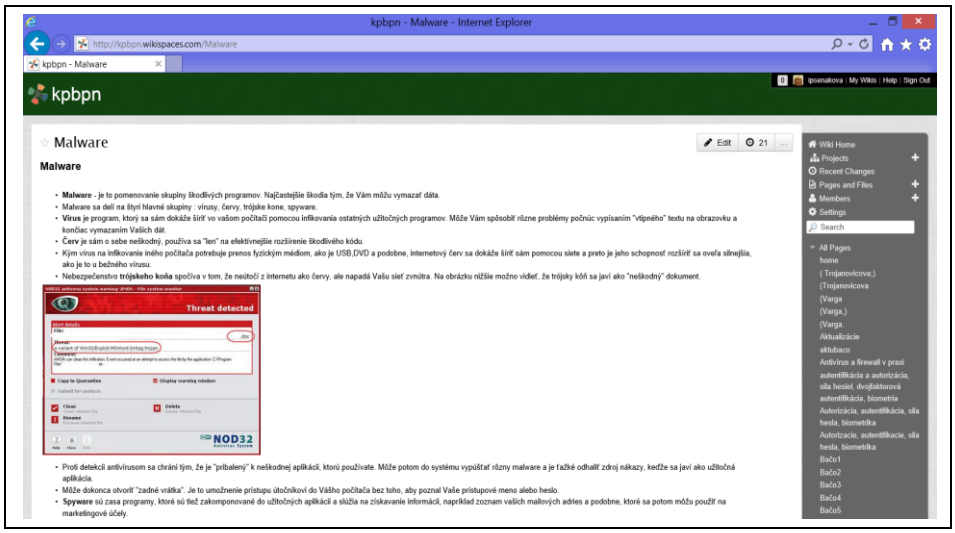
A Nyitrai Konstantin Filozófus Egyetem (KFE) Közép-európai Tanulmányok Kara (KETK) a Kassai Műszaki Egyetem Elektrotechnikai és Informatika Karával karöltve, 2011-ben pályázatot nyújtott be a Szlovák iskolaügyi, tudományos, kutatási és sport minisztérium Kultúrát és oktatást támogató hivatalához (KEGA- Kultúrna a edukačná grantová agentúra) azzal a céllal, hogy megszerezze a kurzus megvalósítására és a szükséges tananyag elkészítésére a szükséges pénzügyi támogatást. A pályázat sikeres lett, igaz némi pénzcsökkentéssel, és a két évre tervezett projekt munka 2012 januárjában el is indult.

Pályázatunk legfontosabb feladatai: elkészíteni a laikus (nem informatikus) felhasználók számára a „Számítógépes biztonság" című kurzust, annak témaköreit, tartalmát, kiválasztani és feldolgozni a szükséges tananyagot és azt beépíteni egy általunk választott elektronikus oktatási keretrendszerbe.

A projektben három nyitrai és három kassai egyetemi oktató vett részt, akik informatikus tanár, ill. számítógép mérnöki végzettséggel rendelkeznek. Mindegyikük rendelkezik informatikai szakmai illetve pedagógiai ismeretekkel is. A Nyitrai partnerek otthon vannak a módszertani, ergonómiai kérdésekben, foglalkoznak az e-learninges oktatás előnyeivel és hátrányaival, mind a pedagógus, mind pedig a diák szemszögéből, mivel a pedagógusképzés széles spektrumával állnak kapcsolatban az általános iskolától a középiskoláig, a humán szakosok képzésétől a természettudományos képzésig. A Kassai résztvevők feladata lett a témakörök megfelelő tartalommal való feltöltése, a tartalom szakszerűségének biztosítása, ill. a tartalom aktuális bővítése és az e-learninges oktatási keretrendszerbe való beépítése.

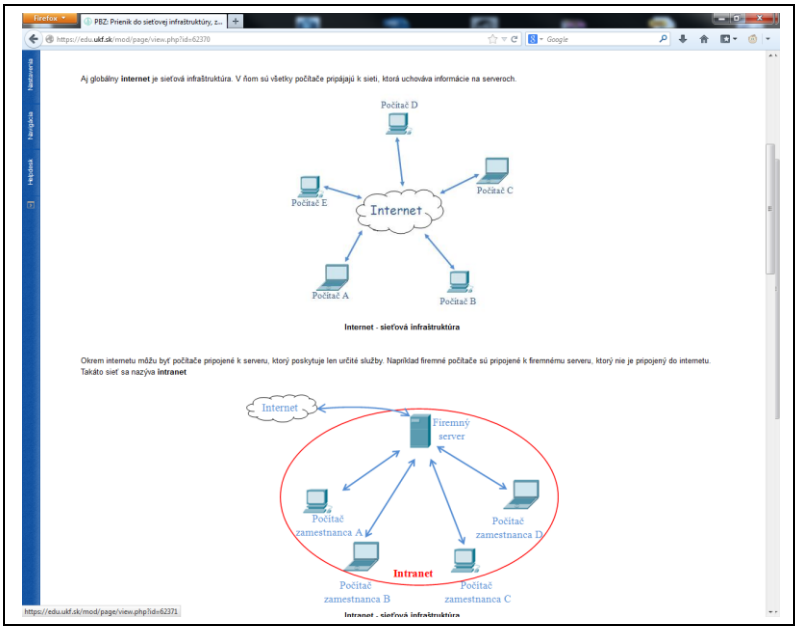
A projekt eredeti elképzelése az volt, hogy a tananyagot és a kurzust nem informatikus egyetemi oktatók részére készítjük el és ők is fogják kipróbálni azt. Ilyen oktatók a nyitrai karon vannak többségben, ezért adott volt a kurzusban résztvevők köre. Mivel ez kevésnek bizonyult, úgy döntöttünk, hogy megpróbáljuk bevonni leendő pedagógus hallgatóinkat is. Ekkor jött az ötlet a kassai diákok „kihasználására" (,akik leendő mérnök informatikusok) és bevontuk őket a kurzus tananyagának elkészítésébe. Ez a tevékenység nekik is javukra vált, mivel bővíthették tudásukat a számítógépes biztonság témakörében és próbára tehették esetleges pedagógusi képességeiket, adottságaikat is. Mindkét „segítő" csoport a harmadik évfolyam diákjaiból állt összse.

A projekt első lépése a kurzus témaköreinek (moduljainak) meghatározása volt. Ez után következett az egyes modulok tartalommal való feltöltése és az e-learninges tananyag elkészítése. Mivel a két kutatócsoport tagjai egymástól helyileg Szlovákia különböző pontjain tevékenykednek, ezért segítségül hívtuk a Wikispaces webes alkalmazást. A Wikispaces Classroom nagyon jól felhasználható olyan szövegek elkészítéséhez, melyeken egyidejűleg több szerző is dolgozik, ezen kívül jól használható közös projektek megoldásában is. [1] Az alkalmazás használatával létrehoztunk egy munkafelületet, ahol a tanárok és a diákok is kölcsönösen kommunikálhattak és ezt a rendszer használtuk fel a kurzus témaköreinek tananyaggal való feltöltésére.



1. ábra: Példa a Wikispaces közös munkafelületre és tananyagrészre

Az LMS keretrendszer kiválasztása szinte adott volt, mivel a szlovákiai egyetemeken a minisztérium által csakhogy nem „előírt” az LMS Moodle, amely az egyetemeken ingyenesen működik. A projektben résztvevő egyetemek is ezt használják, ezért a kidolgozott tananyag ebbe a rendszerbe lett beépítve.



2. ábra: Példa az LMS Moodle-ben megjelenő tananyag egy részére

3. A tananyag

A kurzus témaköreit a következőképpen határoztuk meg [2]:

- Bevezetés a számítógépes biztonságba laikusok számára
- Veszélyek
  - emberek (támadók típusai)
  - fizikai biztonság
  - adatvesztés
  - adatlopás
  - számítógéppel való visszaélés
  - berendezések eltulajdonítása (számítógép, műszaki felszerelés)
  - identitáslopás
  - szolgáltatásmegtagadás (Denial of Service)
  - webes támadások
- Támadások megvalósítására alkalmazott módszerek (támadók által használt technikák)
  - pszichológiai manipuláció (Social Engineering)
  - jelszavak lopása, hitelesítések és jogosultságok feltörése
  - adatlopás (kommunikáció lehallgatása,...)
  - behatolás a hálózati infrastruktúrába, kiskapu (backdoor)
  - malware (vírusok, férgek, spyware, adware, trójai faló)
  - rootkitek
  - puffer túlcsordulás (buffer overflow) - fertőzött képek, dokumentumok
  - hoax
- Biztonsági intézkedések a vészhelyzetek esetén, fenyegetések megszüntetése (fenyegetések elleni védelem)
  - Oktatás
  - Biztonságpolitika
  - Biztonsági, védelmi célokat szolgáló programok (vírusirtó, tűzfal)
  - Szoftverek rendszeres frissítése
  - Hitelesítés és jogosultság (jelszavak erőssége, biometria)
  - Titkosítás, digitális aláírás
  - Tanúsítványok
  - Védelmi infrastruktúra
  - Szteganográfia
- Jogalkotási kérdések, szabálysértések.

A feldolgozott tudásanyag az on-line kurzusban szövegből, képekből és animációkból alkotott tananyagként jelenik meg. A vizuális elemek segítik a tananyag érthetőségét, megértését és növelik a tananyag elsajátításának gyorsaságát.

4. A kurzus

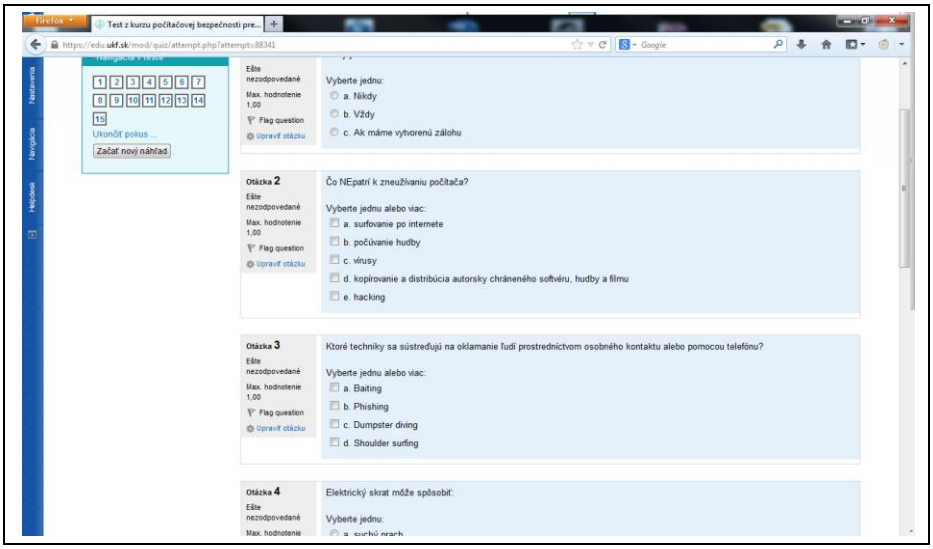
A projektben előkészített kurzus első kipróbálása (tesztelése) a nyitrai karon történt. Az előbb már említettek elvek szerint a résztvevői a kar nem informatikus (Magyar nyelv és irodalom, Szlovák nyelv és irodalom, Hungarológia, Testnevelés, Pedagógia illetve Biológia, Zoológia, Matematika, stb.) oktatói voltak, akiknek szaktudásuk nem kötődik az informatikához vagy más műszaki

tudományokhoz, de pedagógiai munkájuk folyamán szinte napi szinten használniuk kell a számítástechnikát és az információs rendszereket. A kar viszonylag kis létszámú pedagógust foglalkoztat, ezért a harmadéves hallgatókkal bővítettük a résztvevők listáját. Természetesen a diákok választásánál is figyelembe vettük a laikus jelzőt, és így a tanári szakos (Óvó és tanító képző szak, Biológia, Matematika, stb.), ill. a nem tanári szakos (Kétnyelvű ügyvitelszervező, Regionális turizmus) diákokra esett a választás. Így teljes biztonságban mondhatjuk, hogy a kurzus részvevői nem tartoztak a számítógép biztonságával foglalkozó szakemberek csoportjába.

Minden résztvevő hozzáférést kapott az oktatási portálon (https://edu.ukf.sk/) található LMS Moodle rendszerhez és magához az on-line kurzushoz, amely a „Počítačová bezpečnosť“ azaz a „Biztonságos számítógép” címet kapta. A tananyag (2. ábra) elsajátítására két hét időt kaptak a résztvevők. A webes elérésnek köszönhetően ezt meg tudták tenni a munkahelyükről, vagy akár otthonról is. A két hét alatt részt vehettek személyes konzultációkon, ill. bekapcsolódhattak az LMS Moodle rendszerben kialakított fórumba is.

A tanulásra az a tény is ösztönözte a résztvevőket, hogy tudomásuk volt arról, hogy a kurzus befejezéseképpen egy tesztet kell megoldaniuk. A teszt segítségével azt akartuk megtudni, milyen mértékben sikerült a résztvevőknek megérteniük és elsajátítaniuk a tananyagot, és hogyan értékelték magát a kurzust, ill. annak formáját.

A teszt szintén az LMS Moodle rendszerben volt kialakítva. A teszten a résztvevők személyesen („face to face” formában) vettek részt a kar számítógépes termében egy adott napon két csoportra osztva, a terem 18 személyes befogadóképessége miatt. Ezzel azt akartuk elérni, hogy mindenki egyforma feltételek mellett tudjon dolgozni és persze ellenőrizhető legyen, hogy segítség nélkül oldotta meg a feladatokat. Örvendetes számunkra az, hogy a kurzus minden résztvevője részt vett a teszten



3. ábra: Példa az LMS Moodle-ben megjelenő teszt egy részére

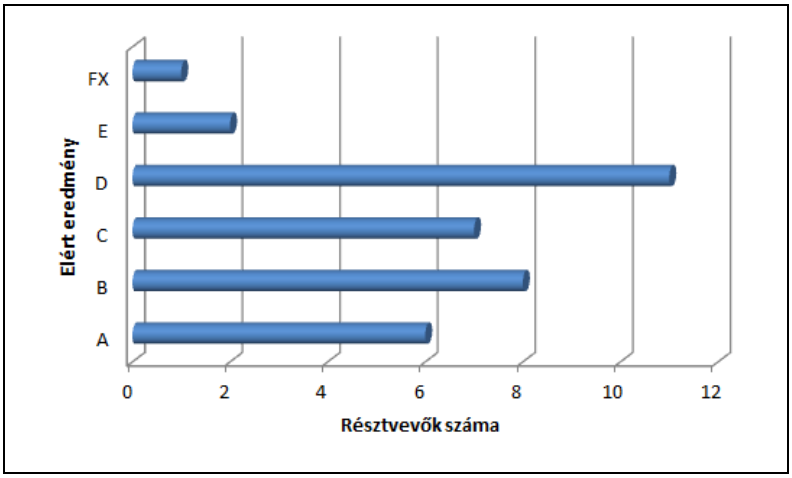
5. A kurzus néhány eredménye

A kurzus befejező tesztjére 170 kérdést készítettünk, amelyek közül véletlenszerűen választott ki a rendszer 15 kérdést, így biztosítva a tesztek különbözőségét minden résztvevő számára. A kérdések többsége zárt típusú, vagyis egy vagy több jó választ kell megjelölni a felkínált vála-

szokból. Azért döntöttünk az ilyen típusú kérdések használata mellett, mert sokkal egyszerűbb a tesztek kiértékelése és az LMS Moodle környezet is támogatja. Ráadásul, ha a tesztet írónak felkínáljuk a lehetséges választ, válaszokat, sokkal könnyebbnek, egyszerűbbnek érzik a megoldást és kevésbé izgulnak. Ezzel a teszttel ugyanis nem elriasztani akartuk a kurzus résztvevőit, hanem épp ellenkezőleg a célunk az volt, hogy felkeltsük az érdeklődésüket, tudatosítsuk az ilyen kurzus elvégzésének a szükségességét.

Minden helyes válasz 1 pontot ért akkor is, ha egy adott kérdésen belül több helyes válasz volt. Tehát az elérhető maximum pontszám 15 volt. Amiatt, hogy a teszt folyamán minden résztvevőnél a kérdéseknek más és más kombinációja jelent meg, nem lehetséges külön az egyes kérdések kiértékelése, például a legnehezebb és legkönnyebb kérdés sem választható ki.

A kurzus abszolválását sikeresnek tekintettük, ha a résztvevő a tesztben legalább 60%-ra teljesített (legalább 9 pontot ért el). Csupán egy résztvevőnek nem sikerült teljesítenie a minimálisnak megszabott ponthatárt (53%-os eredményt ért el). Majd az eredményeket osztályoztuk A-FX értékelő skála alapján, mely a 4. ábrán látható.



4. ábra: A teszt eredményeinek eloszlása

A teszt eredményeinek értékelése folyamán, még más érdekes információkat is feldolgoztunk, melyek az 1. táblázatban találhatók [3].

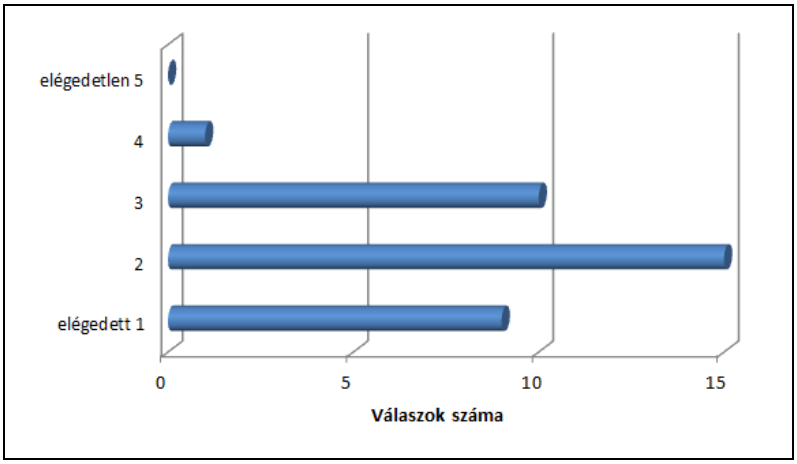
Résztvevők száma	35 személy	
Az elért eredmények átlaga	12,22 pont	81 %
Átlag alatti eredmények száma	14 személy	40 %
Átlag feletti eredmények száma	21 személy	60 %

1. táblázat: A teszt kiértékelésének néhány eredménye

Kíváncsiak voltunk a résztvevők véleményére is, ezért a teszt biztonsági kérdésekkel foglalkozó részén túl lehetőséget kaptak kifejezni a véleményüket is, így még két nyitott kérdésre is válaszolniuk kellett. (Kurzus pozitívumai? Kurzus negatívumai?) A vélemények kiértékeléséből leszűrhetjük, hogy a többség egyetértett abban, hogy a kurzus több fogalmat is érthetővé, ismertté tett számukra a számítógépes biztonság világából.

A kurzust tartalmi szempontból megfelelőnek találták, viszont szakmai szempontból nehezen tudtak véleményt nyilvánítani (negatívum), mivel hiányzik az összehasonlítási alapjuk és a tárgyalt problémakörben sem jártassak. Az e-learninges tanulási formát pozitívumnak tekintették, mivel olyan egyéni időbeosztásban tanulhattak, amely a legmegfelelőbb volt számukra.

Végül azt is értékelhették, hogy mennyire voltak elégedettek magával a kurzussal. Ezt egy zárt kérdés segítségével valósítottuk meg, melyben az 1 (elégedett) – 5 (elégedetlen) felosztási skálát alkalmaztuk. A feldolgozott eredmény az 5. ábrán látható.



5. ábra: A résztvevők elégedettségének kiértékelése

6. Befejezés

Közös projektünk (ami lassan végére ér) legfontosabb célja volt, létrehozni egy olyan elektronikusan elérhető (on-line), számítógépek biztonságos használatával foglalkozó kurzust, amely teljes mértékben megfelel az e-learninges oktatás követelményeinek. A másik nagyon fontos szempont, amit figyelembe vettünk az volt, hogy a kurzus nem számítástechnikai szakembereknek készül, ezért a tananyag elkészítésénél jobban ügyeltünk a szövegek egyszerűségére és érthetőségére. A tananyagba besoroltuk a számítástechnika alapfogalmait is, de elsősorban azokat, amelyek az adott témához kötődnek, hogy ezzel is bővítsük a résztvevők informatikai tudását és segítsük a tananyag megértését, elsajátítását.

A teszt eredményei is mutatják, hogy a kurzus elnyerte résztvevők tetszését. Remélhetőleg a jövőben megismerve az információs rendszerekben leselkedő potenciális veszélyeket és az azokat kivédő lehetőségeket, sokkal jobban fognak figyelni a számítógépük biztonságára

Irodalom

[1] http://www.wikispaces.com/

[2] I. Pšenáková et al: *Course Content of Computer Security*, ICETA 2012: IEEE 10th International Conference on Emerging eLearning Technologies and Applications, Slovakia. Technical University of Košice (2012): ISBN 978-146735122-5, 317-320

[3] J. Genči et al: *Some Results of the Pilot Course of Computer Security for Non-professionals*, ICETA 2013: IEEE 11th International Conference on Emerging eLearning Technologies and Applications, Slovakia. Technical University of Košice (2013): ISBN 978-1-4799-2161-4, 365-368

Acknowledgment

This paper has been supported by the grant KEGA026UKF-4/2012, granted by Cultural and Education Grant Agency (KEGA), Ministry of Education of Slovak Republic.