Közigazgatás-szervező hallgatók információbiztonság-tudatossága

Törley Gábor

pezsgo@inf.elte.hu
ELTE IK

Absztrakt. A 2012-es PISA felmérés eredményei megmutatták, hogy a digitális írástudásban romló tendenciát mutató országok közül Magyarország egyike azoknak, ahol a legnagyobb romlást tapasztalták a leggyengébb tanulók teljesítményében. A közelmúlt kutatásai szerint a non-profit és helyi önkormányzati szervezetek alacsony biztonságtudatossági szinttel rendelkeznek, és tréningek segítségével lehet megfelelni az információbiztonsági szabályoknak és rendelkezéseknek. Más tanulmányok rámutattak arra, hogy kapcsolat van a fogalmak ismerete és a viselkedés között. Empirikus vizsgálatom eredményei azt mutatták, hogy a vizsgált hallgatók alacsony tudatossági szinttel rendelkeznek, könnyen feltörhető jelszavakat használnak, nem tudják, mely biztonsági protokollt érdemes otthoni vezeték nélküli hálózat esetén használni. Minél több tanórájuk volt információbiztonság témaköréből, annál jobb eredményt értek el a kérdőív alapján. Ez különösen igaz azokra, akik érettségit tettek informatikából.

Kulcsszavak: oktatás, információbiztonság-tudatosság, közigazgatás, empirikus kutatás, Magyarország

1. Bevezetés

A PISA felmérés eredményei szerint (2012.), a digitális írástudásban negatív tendenciát mutató országok közül Magyarország egyike azoknak, ahol a legnagyobb romlást tapasztalták a leggyengébb tanulók teljesítményében. A magyar tanulók 32%-a alacsonyan teljesített a digitális írástudás terén. [11] az online biztonsággal és információbiztonsággal kapcsolatos fogalmak részei az digitális írástudás definíciójának. [5]

Az ESET Magyarország felmérése szerint több mint 1 millió magyar netező belép veszélyes weboldalakra, a vírusirtója jelzése ellenére, sőt, a világhálón járók 10%-a szánt szándékkal kapcsolja ki a védelmi szoftvert. A 18-29 éves korosztályra, a teljes minta 17%-ra legjellemzőbb ez. Közöttük vannak azok a fiatal nők és férfiak, akik első évfolyamos hallgatóként kezdik meg egyetemi tanulmányaikat [3]. Ezek nem meglepő eredmények. Az alacsony szintű digitális írástudás alacsony szintű biztonságtudatosságot eredményez.

Információbiztonsági szakértők általában egyetértenek abban, hogy az emberek (a humán faktor) a legnagyobb forrásai az információtechnológia-biztonsághoz köthető problémáknak. A statisztikák szerint a biztonsági események többsége belsős emberek okozzák, és az okozott kár sokkal magasabb lehet, mint ha egy kívülről támadó hekker jutott be volna a rendszerbe. [12]

Empirikus kutatásomban bemutatom az Államtudományi és Közigazgatási Kar[1] elsős hallgatóinak átlagos információbiztonság-tudatosság szintjét. Feltárom az eredmények mögötti okokat és az összefüggéseket, végül megoldási javaslattal állok elő az információbiztonság-tudatosság

[1] Nemzeti Közszolgálati Egyetem, Budapest

szintjének növelésének érdekében, különös tekintettel a középiskolai és az egyetemi alapszakos képzésre.

2. Irodalmi áttekintés

Nemeslaki és Sasvári [10] végzett feltáró kutatást annak érdekében, hogy összehasonlítsák az üzleti valamint a közigazgatási szektor információbiztonság-tudatosságát. Eredményeik azt mutatták, hogy a mikro- és kisvállalkozásoknál, valamint a non-profit és helyi önkormányzati szervezeteknél alacsony a biztonságtudatosság szintje. Az ilyen szervezeteknél dolgozó munkavállalók csak részben vannak tudatában a veszélynek, és általában tudják, hogy meg kellene felelniük bizonyos biztonsági alapelveknek, alkalmazniuk kellene azokat, de további oktatásra, képzésre van szükségük a területet illetően. Általában a magasabb szintű digitális írástudással rendelkezők alacsonyabb kockázati kategóriába tartoznak, mint az üzleti szektorban dolgozó társaik. Azonban a kutatás szerzői azt vallják, hogy az információbiztonság-tudatosság és a digitális írástudás közötti kapcsolat további vizsgálatokat igényel.

Bulgurcu és társai biztonságtudatossági képzéseket javasolnak, amelyek segítik az információbiztonsági szabályoknak és rendelkezéseknek való megfelelést [1]. Mivel Magyarország Kormánya a nemzetbiztonságot, ebbe beleértve a kiberbiztonságot, az e-kormányzati stratégiájának középpontjába helyezte, azok az emberek, akik a közigazgatásban fognak dolgozni, alap- és mesterképzésen, kezdve az alapfogalmaktól, képzést szükséges kapniuk az adatvédelem, adatbiztonság és biztonságtudatosság témakörökből. Mivel ez a terület része az általános digitális írástudásnak, véleményem szerint, egy alapképzést elvégzett hallgatónak általában rendelkeznie kellene az alapokkal ezeken a területeken.

Van der Walt és társai [13], illetve Kruger és társai [9] szerint, valakinek az információbiztonsággal kapcsolatos szókincse a témához (területhez) kapcsolódó ismerős szavakból jön. Egy ilyen szókincs az idővel fejlődik, bővül, és ezzel tudja egy ember kifejezni és megszerezni az új tudást, tudáselemeket. Erre a megközelítésre alapozva, Kruger és társai [9] készítettek egy kérdőívet, amely két részből állt – az elsőben a szókincset, a másodikban a válaszadók viselkedését vizsgálták. Az eredmények azt mutatták, hogy kapcsolat van a fogalmak ismerete (szókincs) és a viselkedés között, illetve hogy a szókincs, azaz a fogalmak ismeretének tesztelése támogatja a speciális, akár problémás területek meghatározását a biztonság oktatásának számára.

Krasznay és Törley [8] rövid betekintést nyújtottak a hazai középiskolai oktatásról. Megmutatták, hogy a nagyobb tankönyvkiadók mintatamtervei kb. a tanórák 4-5%-át használják fel adatbiztonság és adatvédelem oktatására 5-12. évfolyamon. Az óraszámok és annak aránya is nagyon alacsony.

3. Módszertan

Egy 41 kérdésből álló kérdőív készült el 2016. februárjában. Öt kérdéscsoportot tartalmaz: egyszerű állításokat az információbiztonság-tudatosságról, kérdéseket a középiskolai tanulmányokról, elméleti, gyakorlati és demográfiai kérdéseket. A célcsoport az Államtudományi- és Közigazgatási Kar első évfolyamos hallgatói voltak. Ők még sosem találkoztak információbiztonság-tudatossági képzéssel a karon, így ez a kérdőív mérni tudja a hallgatók bemeneti tudását adatvédelem és információbiztonság témaköreiből.

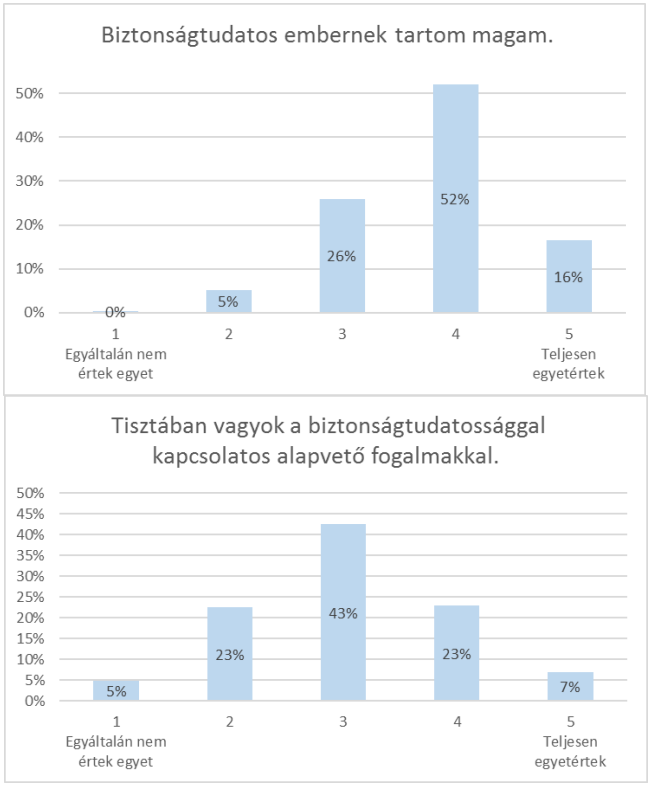
A kérdőív fő célja, hogy meghatározza azokat a területeket, témaköröket, amelyek nem kerültek lefedésre a középiskolai tanulmányok alatt., kapcsolatot találni az elméleti és gyakorlati kérdések, illetve a középiskolai tanulmányok között, valamint megmérni, hogy mennyire jól

jósolják meg a hallgatók a biztonságtudatossági szintjüket, azaz milyen kapcsolat van az információbiztonság-tudatosságról szóló egyszerű állítások és a kérdőív összesített eredménye között.

4. Eredmények

231 első évfolyamos hallgató töltötte ki a kérdőívet (az évfolyam 90%-a), 34%-uk férfi és 66%-uk nő. 81%-uk 19-20 éves.

Két egyszerű állítást kellett értékelniük a hallgatóknak (ezek az ún. „tudatosság-állítások”): (1) Biztonságtudatos embernek tartom magam, (2) Tisztában vagyok a biztonságtudatossággal kapcsolatos alapvető fogalmakkal (1. ábra).



1. ábra: A „tudatosság-állítások” önértékelésének eloszlása

A hallgatók nagy többsége (68%) azt gondolja, hogy biztonságtudatos, de jelentős hányaduk (43%) nem igazán tudja vagy bizonytalan afelől, hogy melyek a biztonságtudatosság alapfogalmai. Ez azt jelenti, hogy inkább élményeik vannak, mintsem valós tudásuk. Ez a bizonytalanság hatással volt az elméleti kérdések átlagára, amely mindössze 36% volt, ellentétben a gyakorlati kérdések átlagpontszámával, amely 63% volt.

Összevetve a magukat biztonságtudatosnak gondoló hallgatók eredményét azokéval, akik nem gondolják magukat annak (a legkisebb négyzetek módszerével), arra jutottam, hogy magukat magasabban értékelők szignifikánsan jobban teljesítettek a gyakorlati kérdéseknél (*koeffici-*

ens=0,555, *p*=0,04<0,05, ceteris paribus♣) és a jelszóhasználat témakörében (*koefficiens*=0,268, *p*=0,005<0,05, ceteris paribus) de ennek ellenére, szignifikánsan rosszabbul teljesítettek a vezeték nélküli hálózatok kérdéseinél (*koefficiens*=–0,138, *p*=0,034<0,05, ceteris paribus). A többi témakörnél (közösségi hálózatok, okostelefonok biztonsága) nem tapasztaltam szignifikáns különbséget.

Azok a hallgatók, akik biztosnak gondolták a tudásukat az alapfogalmakkal kapcsolatban, (az elsőévesek 30%-a) szignifikánsan több pontot értek el az elméleti és gyakorlati kérdéseknél összesen, mint más hallgatók (*koefficiens*=0,712, *p*=0,038<0,05, ceteris paribus).

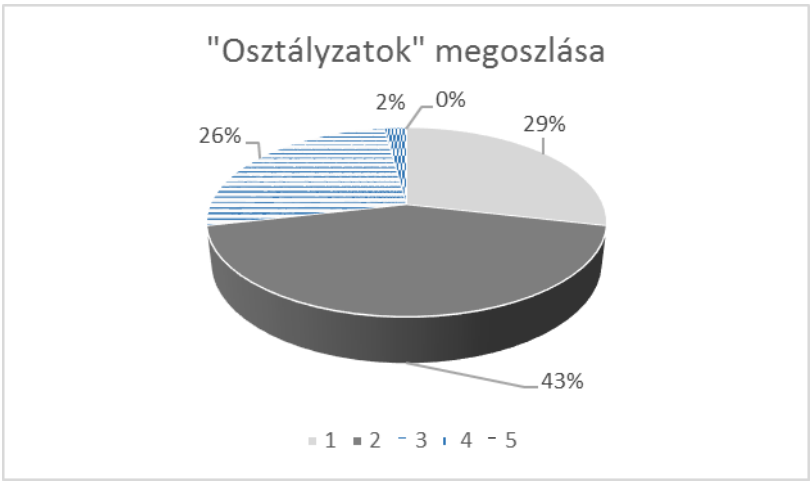
A kérdőív hét elméleti kérdést tartalmazott az alapfogalmakról (a kerettanterv alapján) és 17 kérdés arról, hogy a hallgatók hogyan viselkednének gyakorlati szituációkban (közösségi hálózatok biztonsági kérdései, okostelefonok biztonságos használata, jelszóhasználat, vezeték nélküli hálózatok, számítógépek, internetböngészők, valamint az adatvédelem gyakorlati használata). Minden helyes válasz egy pontot ért. A pontozási rendszer az alábbi volt (1. táblázat):

Jegy	Ponthatár
1	0%
2	50%
3	62%
4	75%
5	88%

1. táblázat: Pontozási rendszer

Ha ez a kérdőív egy valódi teszt lett volna, akkor a hallgatók 29%-a megbukott volna, 43%-uk 2-est, 26%-uk 3-ast és 2%-uk 4-est kapott volna. 5-ös „osztályzat” nem született volna. (2. ábra).

♣ *Ceteris paribus* vagy *caeteris paribus* (latin kifejezés) jelentése: egyébként azonos körülmények, feltételek között, vagy minden más egyenlősége mellett.



2. ábra: „Osztályzatok” eloszlása

A hallgatók több, mint 88%-a csak az ismerőseivel, zárt csoporttal vagy önmagával osztja meg a személyes adatait és bejegyzéseit. Ennek ellenére 26%-uk megoszt különleges és érzékeny személyes adatokat (vallás, szexuális orientáció, politikai nézetek). Az Infotv. [2] szerint [7], „különleges adat: a faji eredetre, a nemzetiséghez tartozásra, *a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre*, az érdekképviseleti szervezeti tagságra, *a szexuális életre vonatkozó személyes adat*”[3]. Ez a fajta adat akkor kezelhető „az adatkezeléshez az érintett írásban hozzájárul vagy törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli”.[4] A hallgatók több, mint negyede „eldobja” ezt a védelmet, mert vagy nem tudják, vagy nem törődnek azzal, hogy mely személyes adataik tartoznak a különleges, érzékeny adatok közé.

Csak a hallgatók 38%-a használja biztonságosan a jelszavait. A kiértékelési módszer szerint azt jelenti, hogy a jelszavak tartalmaznak kis- és nagybetűket, valamint számokat; nem értelmes szó; nem utal személyes adatra és több, mint 8 karakterből áll vagy legalább 40 karakterből áll.[5] Erre a csoportra igaz az is, hogy csak 29%-uk (az egész minta mindössze 11%-a) használja ezeket az elveket a jelszó emlékeztetőikre. Ez azt jelenti, hogy a hallgatók 89%-a úgy gondol a jelszóemlékeztetőre, mint valamiféle felhasználói támogatásra, ahelyett, hogy a jelszavuk jelszavaként kezelnék. A jelszavak 22%-a és a jelszóemlékeztetők 42%-a utal személyes adatra. A tanulók nagy hányada könnyen feltörhető jelszót használ az e-mail címükhöz.

[2] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

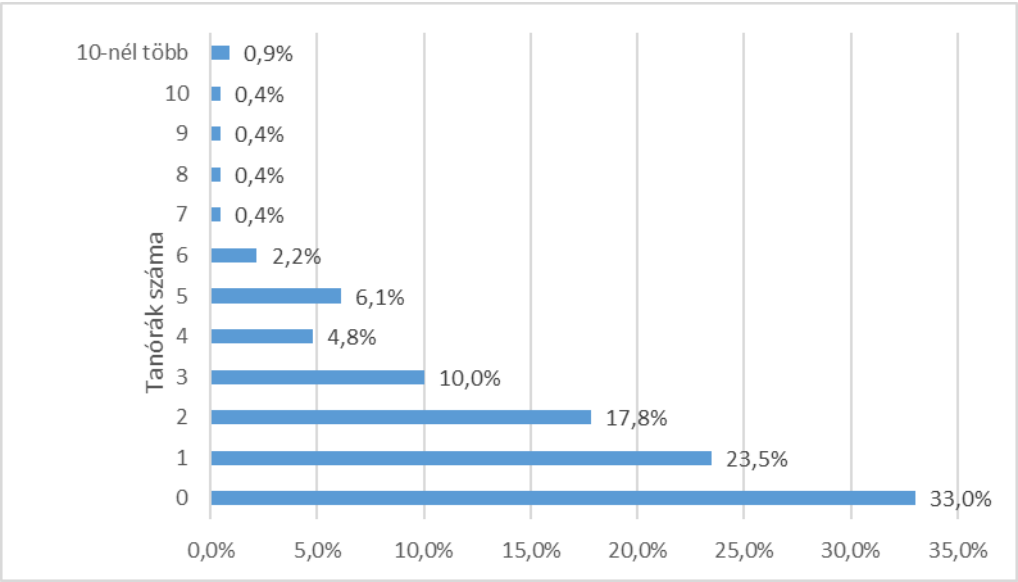
[3] Infotv. 3.§ 3. a)

[4] Infotv. 5.§ (2) a)-b)

[5] A jelszótárolás módját nem vizsgáltam, ugyanis a cél az volt, hogy kiderüljön, hogyan gondolkodnak a hallgatók a saját jelszavuk képzéséről. Természetesen, a biztonságos jelszóhasználat része a biztonságos tárolás is.

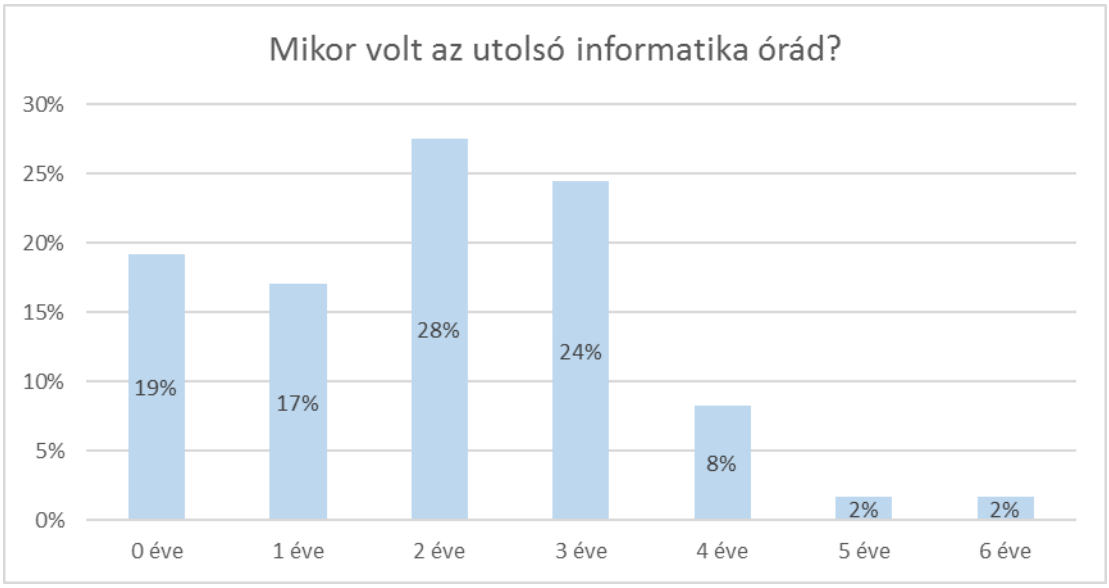
A hallgatók 31%-a nem használ semmilyen biztonsági beállítást az okostelefonjukon, 24%-uk gondolja azt, hogy „az ujjammal elhúzom a kis lakatot” biztonsági beállítás, holott ez nem igaz. Android telefonokon ez jelenti azt, hogy a felhasználó alapértelmezetten hagyta a beállítást.

A harmadik ábra szerint, minden harmadik hallgatónak egy órája sem volt adatvédelemből és információbiztonságból középiskolában. Több, mint a felüknek (56,5%) egy vagy kevesebb órája volt ezekből a témából, ami nagyon kevés. Ez az adat ismét megmagyarázza azt, hogy a hallgatók miért bizonytalanok az elméleti tudásukban (1. ábra). Összevetve azok eredményeit, akiknek 4 vagy több órájuk volt adatvédelemből és adatbiztonságból (a minta 16%-a) a többiekével (a legkisebb négyzetek módszerével), arra jutottam, hogy ez a 16%-nyi hallgató szignifikánsan több pontot ért el a gyakorlati kérdéseknél (*koefficiens*=0,766, p=0,027<0,05, ceteris paribus).



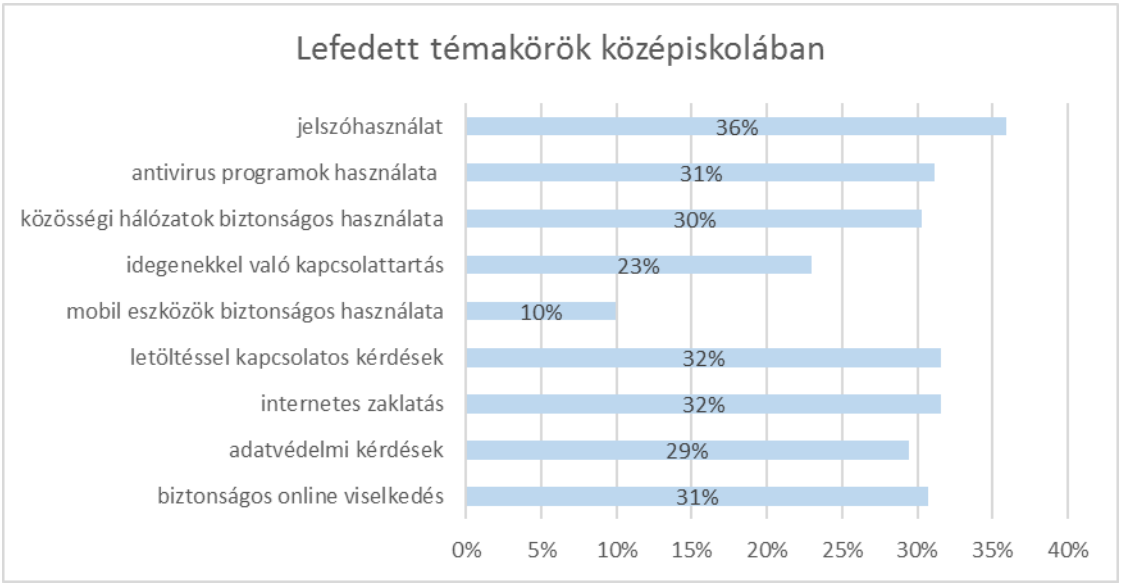
3. ábra: Összesen hány tanórád volt adatvédelemből és adatbiztonságból középiskolában (9-12. évfolyam)?

Az informatika gyorsan fejlődik, ezért a tudás érvényessége csökken az évek múltán tanulás vagy gyakorlás/gyakorlat nélkül. A 4. ábra megmutatja, hogy a hallgatók 36%-ának 0 vagy 1 éve volt a legutolsó informatikaórája, tehát kb. a hallgatók harmadának van friss tudása.



4. ábra: Hány éve volt az utolsó informatikaórád? válaszainak megoszlása

A Eurodyce jelentése (2011) [4] definiálja az adatvédelem és az adatbiztonság főbb témaköreit: biztonságos online viselkedés, adatvédelmi kérdések, internetes zaklatás, letöltéssel kapcsolatos kérdések, mobil eszközök biztonságos használata, idegenekkel való kapcsolattartás, közösségi hálózatok biztonságos használata, Antivirus programok használata, jelszóhasználat. Megkérdeztem a hallgatókat, mely témakörökről tanultak. Az 5. ábra mutatja a válaszok eloszlását.

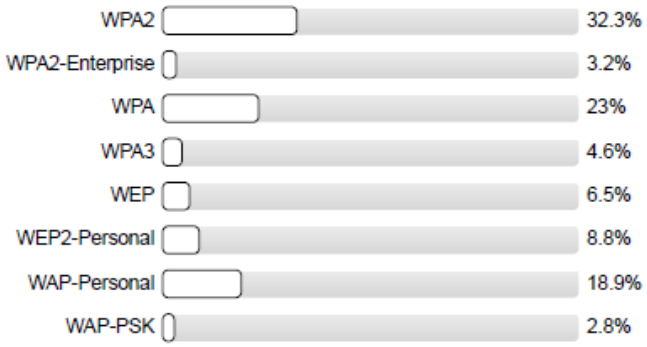


5. ábra: Középiskolában tanult témakörök megoszlása

Az értékek nagyon alacsonyak, különösképpen a „mobil eszközök biztonságos használata”. A hallgatók 36%-a tanult a helyes jelszóhasználatról, mégis csak 26%-uk használja azokat biztonságosan. Nem találtam kapcsolatot a fenti válaszok és az összesített eredmények között.

A hallgatók inhomogén tudással rendelkeznek a fenti témakörökből. 55%-uk csak kettő vagy kevesebb témát tanultak a [4] által definiált főbb témákból. Ennek oka lehet a kiegyensúlyozatlan helyi informatika tanterv. Ez azt jelenti, hogy minden második hallgató nem rendelkezik biztos alapokkal adatvédelem és adatbiztonság terén. Ezért az egyetemi képzésüket a kezdetektől, az információbiztonság-tudatosság alapfogalmaitól kell elkezdeni.

Volt kérdés a vezeték nélküli hálózatok biztonságával kapcsolatban. Azt kérdeztem a hallgatóktól, hogy melyik az ajánlott biztonsági protokoll otthoni vezeték nélküli hálózat esetén. Csak 32,3%-uk tudta a helyes választ (6. ábra).



6. ábra: Melyik az ajánlott biztonsági protokoll otthoni vezeték nélküli hálózat esetén?

A hallgatók közel 30%-a nem biztonságos protokollt választott, illetve egyharmaduk olyan protokollt, amely nem is létezik. Ez azt jelenti, hogy a hallgatóknak nincsen megfelelő elméleti tudásuk ebben a témakörben, és általában nem ellenőrzik a vezeték nélküli hálózati beállításukat az mobil eszközükön/számítógépükön/wifi routerükön, egyszerűen „csak használják” azt, mint egy szolgálatást. A tudás hiánya magában foglalja a megtévesztés lehetőségét.

A válaszok alapján a hallgatók 20%-a tett középszintű, 1%-uk emelt szintű érettségit informatikából. Ezeknek a hallgatóknak pozitív attitűdjük és/vagy tehetségük lehet ehhez a tantárgyhoz. Összevetve az informatikából érettségizettek eredményét (bármilyen szinten) azokkal, akik nem tettek érettségit ebből a tantárgyból (a legkisebb négyzetek módszerét használva) arra jutottam, hogy azok, akik informatika érettségit tettek szignifikánsan jobb eredményt értek el az elméleti és gyakorlati kérdéseket összevetve, mint a többiek (*koefficiens*=1,07, p=0,005<0,05, ceteris paribus) és ez igaz csak a gyakorlati kérdésekre is (*koefficiens*=0,823, p=0,007<0,05, ceteris paribus). Ezeknek a hallgatóknak biztosan több órájuk volt informatikából (az érettségi miatt), így az eredmény visszautal a 3. ábrára. A hallgatók felkészültsége (és az extra tanórák) jobban hatottak a gyakorlati tudásukra, mert nem találtam kapcsolatot az érettségire vonatkozó kérdésekre adott válaszok és az elméleti kérdések eredményei között.

5. Következtetések

Véleményem szerint a középiskolai és egyetemi tantervekben, valamint a tankönyvekben élesebben el kellene különíteni az *adatvédelemnek* és az *adatok védelmének* jelentését. Míg az *adatvédelem* „a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét” jelenti [6],

addig az *adatok védelme* alatt azokat a védelmi módszereket értem, amelyeket az érintett, valamint az adatkezelő védelme érdekében az adatokon hajtanak végre. Az adatvédelem központi szereplője az adatalany, az adatok védelmének fő fókuszában pedig az adat áll. Tehát az informatikai biztonság fogalmát két oldalról, jogi és műszaki oldalról is meg lehet közelíteni, és valójában ugyanaz a célja a két megközelítésnek: az adatalany adatai legyenek biztonságban. Ezt az egységes megközelítést érdemes átadni a középiskolában és egyetemen is.

A kérdőív eredményei azt mutatják, hogy az első évfolyamos hallgatók bemeneti információbiztonság-tudatosság tudása és szintje alacsony. Ezért fontos az egyetemek szerepe, különösen azoké, akik a közigazgatásba, illetve informatikai területre képeznek leendő munkavállalókat. Mivel a biztonságtudatosság ismereteinek érvényessége gyorsan csökken, rendszeres évenkénti képzésekre lenne szükség legalább az informatikai eszközöket használó munkahelyeken. A munkaadók általában gyakran reaktív módon válaszolnak egy-egy biztonsági eseményre, holott preventív és reaktív módszerek együttes alkalmazására van szükség, és a preventív módszerek között van az oktatás és a képzés [2].

Másik fontos következtetése a kérdőívnek, hogy kiegyensúlyozott tantervre van szükség a közép- és felsőoktatásban, illetve az egyéb munkahelyi képzéseken. A kiegyensúlyozatlan tanterv „fehér foltokat" eredményez az ismeretekben. A tanulmány bemutatta melyek azok a területek, amelyeket le kell fednie a felsőoktatásnak és a munkahelyi képzéseknek.

Rengeteg munkavállaló kezeli mások személyes adatát. Ez ugyanúgy igaz egy adatbázis üzemeltetőjére, mint egy közigazgatásban dolgozóra. Akkor tudják ezek az emberek mások adatát biztonságosan kezelni, ha a saját magukéra vigyázni tudnak. Hiszem, hogy a biztonságtudatosság egy gondolkodásmód, ami tanítható és tanulható. Ahogy kutatások és nemzetközi tapasztalatok megmutatták, leggyakrabban az emberi tudatosság, tudás és konkrét készségek hiánya az oka a hekkertámadásnak, szabályok áthágásának, adatok veszélyeztetésének és rendszerleállásoknak. Tudatosabb viselkedéssel ezek a veszélyhelyzetek elkerülhetőek lehetnek.

A magyarországi Safer Internet Program jó példa arra, ahogy szerepet vállal az általános és középiskolai diákok biztonságtudatosságának fejlesztésében. 6500 diák internetbiztonsági képzése kezdődik meg a Vodafone Digitális Iskola Programban, köszönhetően a 2016. októberében aláírt megállapodásnak.

Irodalom

[1] B. Bulgurcu, H. Cavusoglu, I. Benbasat: *Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness*, in: MIS Quarterly. Vol. 34. Issue 3. (2010.) pp. 523-548.

[2] J. D'Arcy, A. Hovav: *Deterring internal information systems misuse*, Communications of the ACM, 50(2010), 113-117.

[3] ESET Magyarország (2011): *A kíváncsiságunk fertőz* - http://www.eset.hu/hirek/kivancsisagunk_fertoz?back=/hirarchivum%3Fpage%3D9 – Letöltve: 2016. november 1.

[4] Eurodyce. *Key Data on Learning and Innovation through ICT at School in Europe 2011*, European Commission, Education, Audiovisual and Culture Executive Agency, ISBN-978-9-2920-1184-0, 2011. - http://eacea.ec.europa.eu/education/eurydice/documents/key_data_series/129en.pdf Letöltve: 2016. november 1.

[5] J. Fraillon, W. Schulz, and J. Ainley. *International Computer and Information Literacy Study assessment framework*. Amsterdam, the Netherlands: International Association for the Evaluation of Educational Achievement (IEA) (2013.), https://www.acer.edu.au/files/ICILS_2013_Framework.pdf - Letöltve: 2016. november 1.

[6] Nemzeti Adatvédelem és Információszabadság Hatóság: *Adatvédelmi értelmező szótár* - http://www.naih.hu/adatvedelmi-szotar.html - Letöltve: 2016. november 1.

[7] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[8] Cs. Krasznay, G. Törley. *E-safety, privacy and information security: Requirements in Public Administration* In: Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Alexander Prosser (Eds.) Central and Eastern European eGov Days 2015: Indepedence Day: Time for a European Internet? pp. 431-441, Austrian Computer Society, Vienna, Austria ISBN 978-3-85403-308-0

[9] H. A. Kruger, L. Drevin. T. Steyn. *A vocabulary test to assess information security awareness*, Information Management & Computer Security, Vol. 18 Iss: 5 (2010), pp.316-327.

[10] A. Nemeslaki, P. Sasvári. *Empirical analysis of information security awareness in the business and public sectors of Hungary*, In: Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Alexander Prosser (Eds.) Central and Eastern European eGov Days 2015: Indepedence Day: Time for a European Internet? pp. 405-418, Austrian Computer Society, Vienna, Austria ISBN 978-3-85403-308-0

[11] OECD: *Main Results from the PISA* 2012 Computer-Based Assessments, in Students, Computers and Learning: Making the Connection, OECD Publishing 2015., Paris

[12] J. Pescatore: *High-Profile Thefts Show Insiders Do the Most Damage*, Gartner First Take (2002.), https://www.gartner.com/doc/379171/highprofile-thefts-insiders-damage - Letöltve: Letöltve: 2016. november 1.

[13] M. van der Walt, K. Maree, S. Ellis: *A mathematics vocabulary questionnaire for use in the intermediate phase*, South African Journal of Education, No. 28 (2008.), pp. 489-504.