HADMÉRNÖK
VÉDELEMINFORMATIKA
18. évfolyam (2023) 4. szám 129–146.
DOI: 10.32567/hm.2023.4.9

Hankó Viktória[1]

Információbiztonság a női munkavállalók aspektusából I.[2]

Information Security from the Perspective of Women Employees I

Absztrakt

A 21. században az információbiztonság, kiberbiztonság kiemelt fontosságú. Ezen területek szakemberállománya vizsgálatának szükségessége is hangsúlyozza a terület aktualitását – különös tekintettel a nemi megoszlásra, bérezés kérdésére, illetve ezek alakulására, okaira. A tanulmány első részében az információbiztonság és az ahhoz kapcsolódó fogalmak ismertetése mellett a szerző bemutatja a már szakmában dolgozó férfiak és nők jelenlegi szakmai helyzetét, motivációit. Ez egy kérdőíves kutatás keretében valósult meg. Emellett a közösségi média egyre növekvő szerepe is megjelenik a tanulmányban. Ehhez kapcsolódóan az aktuális trendek bemutatása történik szentimentanalízis segítségével.

Kulcsszavak: információbiztonság, munkaerőpiac, közösségi média

Abstract

In the 21st century, information security and cybersecurity is a top priority. The need to examine the workforce in these fields also underlines the importance of this area, particularly in terms of gender distribution, pay and its evolution and causes. In the first part of the article, the author describes the current professional situation and motivations of men and women already working in the field, in addition to the concepts of information

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

[2] A cikk a Innovációs és Technológiai Minisztérium ÚNKP-21-2-II-NKE-46 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.

security and related concepts. This was done through a survey. Besides, the growing role of social media is also reflected in the study. In this context, current trends are presented by means of a sentiment analysis.

Keywords: information security, labour market, social media

Bevezetés

A 21. század az internet, az informatika világa, így az információbiztonság és a kiberbiztonság is a mindennapjaink része. Az elterjedt prekoncepció szerint a számítógépes játékok, illetve a programozás inkább a fiúk érdeklődési körébe tartozik, így számukra vonzóbb lehet a szakma a későbbi pályaválasztás során. Ennek következményeként kialakult egy sztereotípia, amely az informatikai kompetenciákat inkább a férfiakhoz köti, mintsem a nőkhöz – ezzel további kihívásokat állítva a fiatal lányok elé, mint például női példaképek azonosítása az informatika területéről. Egyre több tanulmány és internetes cikk születik, amelynek a témája a nők megjelenése az információbiztonsági szektorban. Ezek között találkozhatunk olyanokkal is, amelyek régebbi sikereket ismertetnek például a programozás területén, valamint olyanokkal is, amelyek az aktuális helyzetet mutatják be felmérések eredményeiként. A statisztikák évről évre jobb eredményt mutatnak, ennek egyik mozgatórugója lehet, hogy világszinten különböző szervezetek működnek mentorálási lehetőséggel azon fiatal vagy éppen idősebb hölgyek számára, akik a pályára lépnének.

A kutatás célja felmérni és feltárni a nők elhelyezkedésének problémáját az információbiztonsági szektorban, illetve azokat a kihívásokat, amelyekkel szembesülnek. Elsősorban a már a szektorban dolgozók motivációját mérem fel. Továbbá kitérek a jelenlegi helyzetükre is, különös tekintettel a bérezésre, illetve a diszkriminációra, valamint kiemelten a bemenetelre, az előmenetelre és a pályaelhagyás alakulására. Ezen kérdések vizsgálatát kérdőíves kutatáson keresztül valósítom meg. Annak érdekében, hogy a másik nem álláspontját is feltárjam a nemek közötti egyenlőség munkahelyi helyzetével kapcsolatban, a kérdőíves kutatás keretében nemcsak női, hanem férfi szakértőket is megkérdeztem. Emellett a közösségi médiában megjelenő különböző nemzetközi kulcsszavak vizsgálatát végzem el, hogy feltárjam a téma megítélést.

Kutatási módszertan

Elsődlegesen a releváns a hazai és nemzetközi szakirodalmat dolgoztam fel. Ezekben az információbiztonság, kiberbiztonság és informatikai biztonság terminológiai különbségeinek meghatározása mellett megjelenik az információbiztonsági terület fejlődése, jelenlegi tendenciái, valamint szakmai összetétele – hazai és nemzetközi szinten. A cikk második pillérét a kérdőíves kutatás képezi. A feltett kérdések elemzését az IBM SPSS szoftver segítségével végzem el. A vizsgálat során kiválasztott kérdések közötti kapcsolat vizsgálata pedig kereszttábla-elemzéssel, illetve klaszterelemzéssel történt. Továbbá a közösségi médiában megjelenő trendek is fókuszba kerülnek a szentimentanalízis keretében.

Információbiztonság mint munkaerőpiaci szakterület

A nemzetközi szakirodalom szinonimaként használja az információbiztonság, a kiberbiztonság és az informatikai biztonság szavakat. Valóban van átfedés és hasonlóság a fogalmak között, azonban nem teljesen ugyanazt jelentik. A NIST 800-59 irányelve alapján az információbiztonság az információk és információs rendszerek védelmét jelenti a jogosulatlan hozzáféréstől, felhasználástól, nyilvánosságra hozataltól, megzavarástól, módosítástól vagy megsemmisítéstől a bizalmasság, sértetlenség és rendelkezésre állás biztosítása érdekében.[3] Muha Lajos és Krasznay Csaba úgy fogalmaz, hogy az információbiztonság alatt a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben vagy bármilyen más módon kezelt információk védelmét értjük.[4] Jeremy Hilton és Yulia Cherdantseva megfogalmazásában az információbiztonság általános definíciójában öt pontot szükséges kiemelni, amelyek a következők:

1. Nincsenek korlátozások az információ típusára vonatkozóan. Tág értelemben az információbiztonság bármilyen formájú vagy típusú (például elektronikus, papír, verbális, vizuális) információval foglalkozik.
2. Tartalmazza az információk védelmét szolgáló összes műveletet. Így nemcsak a technikai műveletekkel foglalkozik, hanem az információfeldolgozás, -tárolás vagy -továbbítás során szükséges védelmi műveletek sokféleségével is.
3. A nemkívánatos események listája széles és nyitott. A definíció kifejezetten felsorolja a lopást, kémkedést és az információ megrongálását, de nem korlátozódik ezekre.
4. Az általános definíció nem tartalmaz olyan biztonsági célokat, mint a bizalmasság, sértetlenség, rendelkezésre állás vagy bármi más. A tudományág fő célja tehát – a harmadik ponttal összhangban – az átfogó információvédelem, és nem csupán több, előre meghatározott biztonsági cél elérése.
5. Az információbiztonság magában foglalja az előre megtett intézkedéseket. Ezért nemcsak a már megtörtént nemkívánatos események elemzésével kell foglalkoznia, hanem az ilyen események előrejelzésével és azok valószínűségének felmérésével is.[5]

Ennek egy részterületét képezi az informatikai biztonság, amely az informatikai rendszerekben kezelt adatok és az azokat kezelő rendszer(ek) védelmét jelenti, ebből kifolyólag nem a teljes információs rendszerre, csupán annak valamennyi elemére terjed ki.[6]

Mindemellett a kiberbiztonság a NIST megfogalmazása alapján kibertérben megjelenő támadókkal szembeni védekezés képességét jelenti.[7] Ezzel szemben Magyarország Nemzeti Kiberbiztonsági Stratégiájában

[3] Barker 2003.
[4] Krasznay–Muha 2014.
[5] Cherdantseva–Hilton 2014.
[6] Muha 2008.
[7] Paulsen–Byers 2019.

„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez, működtetéséhez"

definícióval találkozhatunk.[8] Mindkét fogalom a kiberteret említi, amely a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét foglalja magában.[9] A fogalmi evolúció párhuzamosan zajlott a NATO kiberbiztonsággal kapcsolatos stratégiai fejlődésével, amelyben a szakemberképzés hangsúlyos elemként jelenik meg.[10] A magyar kibervédelem rendszeréről elmondható, hogy rendkívül szerteágazó, amelyben meg kell teremteni egy tudásbázist, amely különböző kérdésköröket kell tartalmazzon: stratégiai, jogi, vagy akár szervezeti, működési ismereteket.[11]

A fent említett definíciókból látható, hogy valóban van átfedés a fogalmak között, azonban az információbiztonság egy szélesebb terület, amely mind az informatikai biztonság, mind pedig a kiberbiztonság elemeit lefedi.

A munkaerőpiac bemutatása

Az előző fejezetben feltártak alapján elmondható, hogy igen széles területről van szó, amelynek fő eleme – annak elnevezéséből is adódóan – a biztonság és a védelem megteremtése, fenntartása. Ennek megvalósítása a területen dolgozó szakemberállomány – vagy legalább egy részének – a feladata. Elmondható továbbá, hogy az információbiztonság az utóbbi években mind a tudományos kutatásban, mind az ipari gyakorlatban előtérbe került. A hatékony biztonsági műveletek támogatásához többre van szükség, mint pusztán technikai megoldások sokaságára. Az emberi tényezőt kulcsfontosságúnak kell tekinteni ebben az iparágban.[12] Emellett fontos megjegyezni, hogy az információbiztonsági szektorban nem feltétlenül mindenki biztonsági tesztelő, valamint a területen dolgozók közül sem mindenki tölti minden idejét a biztonsággal kapcsolatos problémákkal.[13] Ebből fakadóan multidiszciplináris területről beszélhetünk, és az emberek gyakran több kalapot viselnek (remélhetőleg mindenki fehéret[14]), miközben ugyanazt a szerepet töltik be. Lehet a munkakör oktató, aki megtanítja az irodai dolgozókat, illetve további munkatársakat hogyan végezzék el a feladataikat anélkül, hogy szükségtelen biztonsági kockázatoknak tennék ki a szervezetet, mint például az utcán talált pendrive vállalati számítógépbe helyezése.

[8] Magyarország Nemzeti Kiberbiztonsági Stratégiája 2013.
[9] Magyarország Nemzeti Kiberbiztonsági Stratégiája 2013, 3. pont.
[10] Bányász–Krasznay–Tóth 2021: 130–149.
[11] Krasznay 2017.
[12] Hámornik–Krasznay 2017.
[13] Tóth 2022: 224.
[14] Angolul „white hat hacker", vagyis etikus hacker.

Mellettük jelen vannak a programozók, akiknek idejük nagy részét a kódok áttekintése teszi ki, amellyel szerencsés esetben a potenciális támadók előtt fedezik fel a biztonsági réseket. Továbbá lehet a szektorban valaki újságíró is, aki az aktuális kockázatok leírása mellett elemzéseket készít az iparági trendekről.[15] Vannak továbbá a biztonsági műveleti központok, azaz a Security Operation Center-ek vagy SOC-ok, ahol a csapatok a technológiát használják a feladatok közös elvégzésére, céljaik elérésére.[16]

A munkahelyek, foglalkozások, készségek és profilok esetében különféle hivatkozásokat találhatunk a munkaerőpiacon. Ezek közül a legismertebbek a European Skills, Competences, Qualifications and Occupations, azaz a készségek/kompetenciák, képesítések és foglalkozások európai osztályozása (a továbbiakban: ESCO), az Európai Unió (a továbbiakban: EU), új munkaerő-osztályozás, az e-CF vagy az 16234-es európai szabvány. Az ESCO osztályozásán belül az információs és kommunikációs technológiai (a továbbiakban: IKT) foglalkozások között találhatjuk meg az információbiztonság, kiberbiztonság területén megjelenő munkaköröket, amely a következőképpen alakul.

1. táblázat: Munkakörök megnevezése, leírás

Munkakör megnevezése	**Munkakör leírása**
Biztonsági tesztelő	Behatolásvizsgálatot, valamint biztonsági sebezhetőségi értékeléseket hajt végre az elfogadott módszereknek és protokolloknak megfelelően. Különböző biztonsági szempontok alapján elemzi a rendszereket.
IKT-audit menedzser	Felügyeli az információs rendszerek, platformok és működési eljárások ellenőrzéséért felelős IKT-auditorokat a hatékonyság, a pontosság és a biztonság érdekében kialakított vállalati normákkal összhangban. Felméri és értékeli a szervezet IKT-infrastruktúráját kockázati szempontból, valamint ehhez kapcsolódóan ellenőrzéseket vezet be. Továbbá a jelenlegi rendszerváltozások/frissítések végrehajtására vonatkozóan, illetve a kockázatkezelési ellenőrzésekre javaslatot tesz.
IKT-auditor	Információs rendszerek, platformok, valamint üzemeltetési eljárások ellenőrzését végzi, összefüggésben a vállalat által meghatározott hatékonysági, pontossági és biztonsági szempontokkal. Emellett az IKT-audit menedzserhez hasonlóan ő is ellenőrzi az IKT-infrastruktúrát és ellenőrzéseket vezet be, valamint javaslatokat tesz.
IKT biztonsági adminisztrátor	Megtervezi és végrehajtja azokat a preventív intézkedéseket, amelyek hiánya szándékos támadás, lopás vagy korrupcióból származó információk és adatok kiszivárgásához vezethetne.

[15] Hughes 2019.
[16] Hámornik–Krasznay 2017.

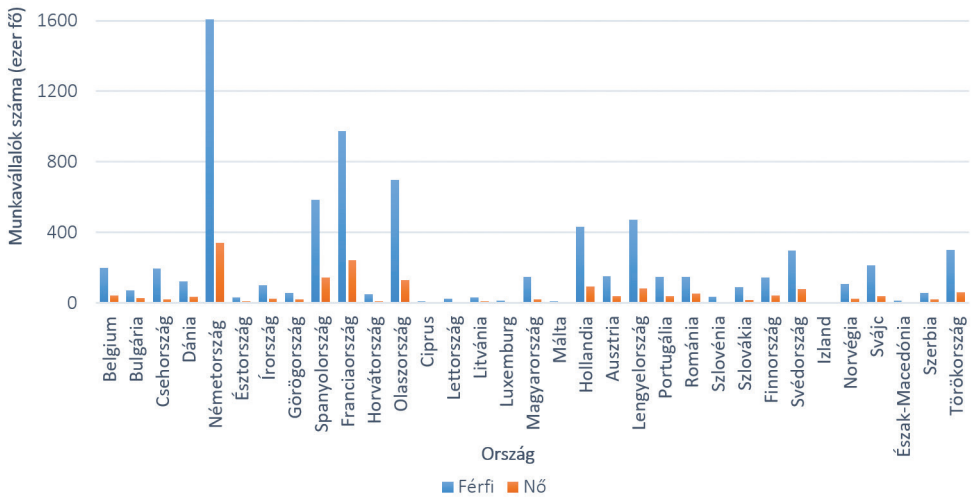
Munkakör megnevezése	Munkakör leírása
IKT biztonsági igazgató	Védi a céginformációkat, valamint a munkavállalók adatait a jogosulatlan hozzáféréssel szemben. További feladata az információs rendszer biztonságpolitikájának meghatározása. Kezeli a biztonságos telepítést az információs rendszerekben, és az információk rendelkezésre állását is biztosítja. CISO néven is ismert.
IKT biztonsági menedzser	Javasolja és végrehajtja a szükséges biztonsági frissítéseket. Emellett a tanácsadás, támogatás, valamint tájékoztatás is a munkája részét képezi a képzés és tudatosítás mellett.
IKT biztonságtechnikai tanácsadó	Javaslatot tesz és hajt végre, amelynek célja az adatokhoz és programokhoz való hozzáférés ellenőrzése. Továbbá a biztonságos információcserét is elősegíti.
IKT katasztrófaelhárítás menedzser	A szervezet kiberbiztonságának, ellenálló képességének és egy katasztrófa utáni helyreállítás képességének fejlesztése érdekében modelleket, irányelveket, módszereket, technikákat és eszközöket kutat, tervez és fejleszt.
IKT-tanácsadó	Tanácsot ad a meglévő eszközök és rendszeres használatával kapcsolatban optimalizálás szempontjából amellett, hogy ajánlást tesz üzleti projektek, technológiai megoldás fejlesztésére, illetve megvalósítására. Továbbá részt vesz az IKT-megoldások kiválasztásában és értékelésében is.
Szoftvermenedzser	Felügyeli a rendszer beszerzését és annak fejlesztését amellett, hogy a végrehajtott szoftvermegoldások és projektek eredményét, minőségét is nyomon követi.

Forrás: az ESCO alapján a szerző szerkesztése

A munkakörök meghatározása után szükséges nevesíteni azt is, hogy hány emberről beszélhetünk ebben a szektorban, illetve a nemek közötti arányok bemutatása további, különböző kérdéseket vethet fel.

2020-ban az EU-ban mintegy 8 400 000 fő dolgozott IKT-szakemberként. A legtöbben (1 900 000 fő) Németországban vállaltak munkát, ahol az uniós szakemberek több mint egyötödét (23,1%) foglalkoztatták. A sorban második Franciaország, ahol 1 200 000 főt tett ki a szakemberállomány (az EU létszámának 14,5%-a), ezt követte Olaszország, ahol 800 000 fő (9,8%) dolgozott IKT-szakemberként. Magyarország esetében 319 200 főről beszélhetünk, ez az EU-s szakemberállomány 3,8%-át teszi ki.[17]

[17] Eurostat é. n.



1. ábra: az IKT-szektorban dolgozók száma 2020-ban
Forrás: az Eurostat alapján a szerző szerkesztése

Kiemelendő – ahogy az az 1. ábrán látható –, hogy az EU-ban IKT-szakemberként foglalkoztatottak túlnyomó többsége férfi, arányukat tekintve 2020-ban 81,5% volt, ami 1,5 százalékponttal alacsonyabb, mint 2011-ben. Csehországban (89,7%), Máltán (89,0%) és Magyarországon (87,7%) 2020-ban 10 IKT-szakemberből 9 férfi volt. Míg a többi uniós tagállam többségében 10 IKT-szakértőből körülbelül 8 férfi volt, addig Bulgária (71,8%), Görögország (73,5%) és Románia (73,8%) voltak azok a kivételek, ahol a férfiak aránya nem érte el a 75%-ot. Bulgáriában az IKT-szakemberek 28,2%-a 2020-ban nőkből állt, ami a legmagasabb arány az uniós tagállamok között. Görögországban és Romániában az összes IKT-szakember körülbelül egynegyedét, 10 másik uniós országban pedig az összes IKT-szakember egyötödét vagy annál is többet tettek ki a nők. Abszolút értékben számolva Németországban 2020-ban több mint negyedmillió női IKT-szakembert (340 400 fő) foglalkoztattak. Ez messze a legmagasabb női foglalkoztatási szint, mivel Franciaország (244 500 fő), Spanyolország (144 500 fő) és Olaszország (130 500 fő) voltak azok a tagállamok, ahol 100 000 fő vagy annál több a női IKT-szakember.[18]

A területen dolgozók motivációja, tapasztalatai – empirikus vizsgálat

Egy afrikai kutatás[19] során gyűjtött adatokból három domináns szempont rajzolódott ki az IKT-szektor mellett döntő dél-afrikai nők körében. Ezek a következők voltak:

[18] Eurostat é. n.
[19] Makola–Kgosinyane 2020.

- tudatos választás és szerencsés véletlen: ebben az esetben saját döntésről számoltak be a résztvevők, illetve a munkáltatóik által biztosított foglalkoztatási lehetőségeket említették, valamint néhány résztvevő jelezte, hogy véletlenül került az IKT-ágazatba;
- érdeklődés és szenvedély: a résztvevők ebben az esetben azt jelezték, hogy az IKT iránti érdeklődésük, amely a szenvedélyükké vált, ösztönözte őket arra, hogy belépjenek az ágazatba;
- társadalmi és családi befolyás: a résztvevők fele arról számolt be, hogy a család és a társadalom befolyásolta őket abban, hogy belépjenek az iparágba – ez magában foglalta szüleik foglalkozását is. A családtagok és a kortársak hatása mellett többen a média befolyását is említették.

Ez a kategorizálást vettem alapul a kérdőíves kutatásom adatainak csoportosítására.

A kérdéssor alapját a BCS, The Chartered Institute for IT 2014 májusában indított kampányának kérdőíve adta. A kampány célja az volt, hogy több nőt ösztönözzenek az információbiztonsági területre való belépésre. A felmérést a szervezet online végezte, személyre szabott meghívás alapján. Ennek során az Egyesült Királyságban élő mintegy 5000 szervezeti tag (véletlenszerűen kiválasztva), illetve szintén az országban működő BCSWomen tagjai voltak jogosultak a kitöltésre. Ebből összesen 771 válasz érkezett a kitöltési időszakban, amely 2014. január 2-től 2014. február 15-ig tartott – tehát 12%-os válaszadási arányról beszélhetünk.

A kitöltők 79%-a úgy érezte, hogy előnyös lenne, ha több nő lenne a szektorban. Emellett a válaszadók több mint fele úgy gondolta, a nőknek nehezebb visszatérni a pályára. Bérezés és előmenetel tekintetében a megkérdezettek nagy része úgy vélte, hogy a férfiak számára jobb lehetőségek adottak. Az információbiztonsági karrierhez a válaszadók szerint leginkább technológia iránti érdeklődés, logikai szemléletmód és általános IT-ismeretek szükségesek.[20]

Az általam reprezentált kérdőív arra a kérdésre ad választ, hogy hazai szinten a szektorban dolgozók milyen tapasztalatokkal rendelkeznek, és mi motiválta őket a pályaválasztás során, valamint ők hogyan motiválnának fiatalokat, hogy ezt a területet válasszák. Ennek megválaszolásához a kérdőív első részében a demográfiai adatok mellett a beosztásra és a munkakörre is rákérdeztem. A felmérés második részében a munkával kapcsolatos motivációval kapcsolatban tettem fel kérdéseket, végül a harmadik részben a hangsúly a foglalkoztatottak munkakörülményeire került. Az adatfelvétel 2021. november 30. és 2022. március 30. közötti történt. Eddig a dátumig 52 (n = 52)[21] kitöltés érkezett. A kitöltők száma az adattisztítási folyamatot követően 52 fő maradt, ebből 15 nő volt (28,8%). Ez alapján a férfiak 71,2%-os arányt képviselnek.

A kitöltők által megnevezett munkakörök alapján megalkottam a következő szakmatérképet:

[20] BCS 2014.

[21] Az alacsony kitöltésszámot vélhetően az indokolja, hogy a célcsoport privacyérzékenysége magas. Több megkeresés is érkezett, hogy többek szerint a demográfiai adatok alapján könnyen profilozhatók, így nem töltötték ki a kérdőívet.

2. ábra: Szakmatérkép
Forrás: a szerző szerkesztése

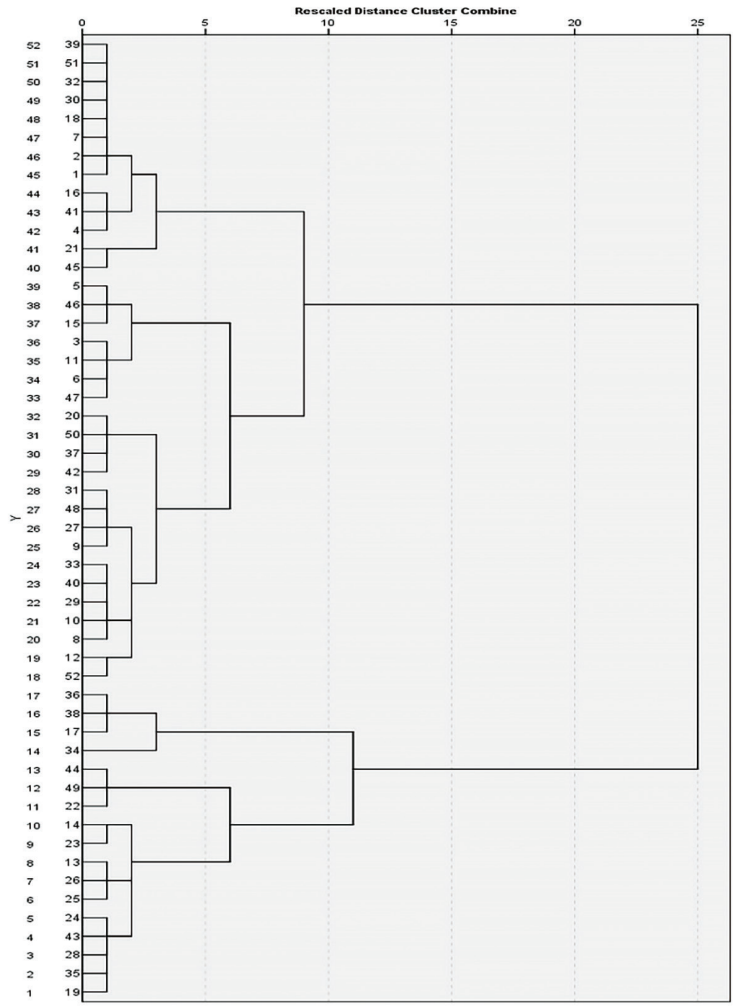
Az ábráról leolvasható, hogy a kitöltők között a férfiak tekintetében – kék és lila színű feliratok – az IBF,[22] CISO[23] és a Tanácsadó volt a legtöbbet említett pozíció, a nők esetében – fekete színű feliratok – az IBF, a Security Tester és Analyst,[24] valamint a Tanácsadó, Információbiztonsági szakértő volt a legnépszerűbb.

Ezt követően Spearman-féle korrelációs vizsgálatot folytattam le, amely azt mutatja meg, hogy az egyik változó nagysága milyen mértékben határozza meg a másik változó nagyságát, valamint az összefüggés irányát és erősségét.[25] Ennek során a legtöbb kérdés között közepesnél erősebb szignifikáns kapcsolat volt kimutatható. A klaszterelemzés az adatok csoportosítását jelenti úgy, hogy figyelembe veszi az egyedek egy meghatározott ismérvrendszerben felvett értékeit. Ennek alapján csak azon változók vonhatók be, amelyeknél közepesnél gyengébb kapcsolat nem mutatható ki.[26] Így a klaszterelemzésbe az alábbi három változót vontam be:

1. Általánosságban mennyire érzi magát motiváltnak a munkahelyén?
2. Mennyire érzi biztosnak (hosszú távon) a jelenlegi munkahelyét?
3. Ön szerint mennyire könnyű vagy nehéz a nők számára visszatérni az IT-/információbiztonsági/kiberbiztonsági munkakörbe a karrier megszakítása vagy szüneteltetése után?

Elméleti megfontolások alapján úgy tűnhet, hogy az 1. és 2. változó között erős kapcsolat van, azonban az elvégzett korrelációs vizsgálat alapján megállapítható, hogy 0,515, ami közepesen erős kapcsolatot mutat.

[22] Elektronikus információs rendszer biztonságáért felelős személy.
[23] IKT biztonsági igazgató.
[24] Biztonsági tesztelő és elemző.
[25] *Spearman korreláció* é. n.
[26] Mitev–Sajtos 2007.



3. ábra: Kapott dendogram
Forrás: a szerző szerkesztése

Ezután az alacsony kitöltési szám okán hierarchikus klaszterelemzést végeztem Ward-eljárással[27] és négyzetes euklideszi távolságmérték[28] alkalmazásával. A kapott dendogram[29] alapján három klasztert azonosítottam, ezek elnevezését és jellemzőit a 4. ábra tartalmazza.

[27] Minden egyes klaszterre kiszámolják az összes változó átlagát, majd minden megfigyelési egységre kiszámítják az euklideszi távolságot. Mitev–Sajtos 2007: 295.

[28] Távolságmérő eljárás, amelyben két pont távolsága, a pontok különbségének négyzetének gyökével egyezik meg. Lásd: http://mialmanach.mit.bme.hu/fogalomtar/euklideszi_tavolsag

[29] A dendogram a klaszterelemzés eredményét grafikus formában ábrázoló diagram. Láthatók rajta a csoportosulási pontok, amelyek a hozzájuk tartozó klaszterekkel beazonosíthatók. Mayer 2016.

Elégedetten biztosak	Középutasok	Elégedetlen bizonytalanok
□ általánosságban motiváltnak érzi magát a munkahelyén; □ biztosnak érzi (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.	□ közepesen motiváltnak érzi magát a munkahelyén; □ közepesen biztosnak érzi (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.	□ nem igazán érzi motiváltnak magát a munkahelyén; □ nem érzi feltétlen biztosnak (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.

4. ábra: Klasztereket és jellemzőiket összefoglaló táblázat
Forrás: a szerző szerkesztése

A kialakított klaszterekben az „elégedetten biztosak" 13 főt, a „középutasok" 22 főt, míg az „elégedetlen bizonytalanok" 17 főt számláltak. A csoportok kialakítását követően további változókat vontam be, úgymint a kitöltő neme, valamint arra a kérdésre adott válasza, hogy szerinte előnyös lenne-e, ha több nő dolgozna a területen. Klaszterek tekintetében 6-6 nő a „középutasok", illetve az „elégedetlen bizonytalanok", míg 3 nő az „elégedetten biztosak" csoportjába tartozik. Emellett az is elmondható, hogy a legmagasabb arányban a „középutasok" és az „elégedetten biztosak" tagjai tartanák előnyösnek, hogy több nő dolgozzon a területen. A nők esetében arányait tekintve többségben vannak, akik szerint előnyös lenne, mindazonáltal azt is ki kell emelni, hogy a női válaszadók arányát tekintve 20% egyáltalán nem támogatja, 26,6% pedig nem biztos benne, hogy kívánatos lenne, ha többen lennének a területen.

Ezt követően kereszttábla-elemzést végeztem, amely során a nemek és a bérezés véleménye közötti kapcsolatot vizsgáltam. Ez arra ad választ, hogy a kitöltők meglátása szerint van-e különbség a férfi és a női munkavállalók bérezése között. A *khi-négyzet-próba* két minőségi változó közötti kapcsolat vizsgálatát teszi lehetővé, azaz arra ad választ, hogy van-e szignifikáns kapcsolat a két változó között.[30] Ennek során a nullhipotézis az, hogy a két változó között nincs szignifikáns összefüggés, ezt akkor fogadjuk el, ha a kapott érték nagyobb, mint 0,05. Az alternatív hipotézis az, hogy van a két változó között kapcsolat, ez akkor igazolódik be, ha a kapott érték kisebb vagy egyenlő, mint 0,05. Az elemzés lefuttatását követően a kapott eredmény 0,222, így nincs kapcsolat. Ebből következik, hogy a nemek és a bérezési, juttatási körülmények között nem mutatható ki összefüggés a vizsgált minta válaszai alapján. A vélemények alapján megállapítható, hogy a férfiak és nők szerint nincs különbség a bérezési, juttatási feltételek között a szektorban.

[30] *Khi-négyzet-próba jelentése és alkalmazása az SPSS-ben* é. n.

Az általam készített kérdőív válaszai alapján két csoportba tudom besorolni a válaszokat:

- Tudatos választás és szerencsés véletlen: a válaszadók között többen írták, hogy a hivatástudat vezérelte a választás során, illetve a saját karriercélok is megjelentek a már korábbi szakmai tapasztalatok mellett.
- Érdeklődés és szenvedély: a válaszok nagy része ebbe a kategóriába tartozik – informatika, szabványok, valamint a rendvédelmi érdeklődés is motivációs tényező.

Emellett fontos kiemelni, hogy a válaszok nagy részében megjelent az újszerűség, illetve a folyamatos tanulás, fejlődés tényezőként. Pár válaszadó a „jó fizetés"-t is megemlítette.

Közösségi média

A webdesign és a motiváció kapcsolata fentebb már szóba került, azonban nem érdemes elmenni a közösségi média jelentősége mellett sem. Érdemes kitérni rá, hogy a közösségi média használatát háromféleképpen osztályozzák. Elsősorban a barátok, rokonok és kollégák közötti kapcsolattartásra használják, másodsorban pedig az öröm és az érzelmi élmények affektív szükségletkielégítésére. A harmadik a kognitív használat, amikor az emberek a közösségi médiát arra használják, hogy információt, tudást gyűjtsenek.[31] Számos közösségi hálózati alkalmazás áll rendelkezésre – amelyet szervezetek hivatalos célokra használhatnak –, mint például a Facebook, a WhatsApp, a YouTube, a Twitter, a blogok, a Skype és a fényképmegosztó oldalak. Ezen túlmenően néhány speciális és privát közösségi hálózatot is használhatnak a szervezetek kommunikációjára,[32] mint például a „Yammer", míg a szervezetek kis része podcastot, second life-ot és Pinterestet használ.[33] Ezek a médiumok nemcsak a munkavállalók közötti kommunikációra használhatók, hanem a nyilvánosság számára is elérhetőséget is biztosíthatnak a szervezet felé – platformot kínálva a különböző tevékenységek, valamint mentorprogramok bemutatására is. Az elemzésnél figyelembe lehet venni az eszközök közötti kapcsolatokat is.[34]

Hatékonyságot tekintve egy tanulmány[35] megállapításai szerint az informatikai szektorban a belső toborzás, a közösségi média, az állásközvetítő tanácsadók és a munkaerő-vadászat a mérsékelten hatékony toborzási formák. A vállalatok toborzási stratégiáit és gyakorlatát befolyásoló belső tényezők közül a vállalat imázsa és a munkahelyi élet minősége a legjelentősebb tényezők. A külső tényezők közül a társadalmi-gazdaságiak befolyásolják leginkább a toborzási gyakorlatot, amelyet a gazdaságban a foglalkoztatási ráta követ. A válaszadók többsége elégedett az informatikai vállalatoknál alkalmazott toborzási gyakorlatokkal és eljárásokkal.

[31] Ali-Hassan – Nevo – Wade 2015: 65–89.
[32] Farkas 2023: 11–30.
[33] Macnamara–Zerfass 2012: 287–308.
[34] Bederna–Szádeczky 2021: 51–66.
[35] Singh–Kamal 2019.

Ez azt jelenti, hogy a kiválasztott vállalatok – TCS, Infosys, Wipro, HCL Technologies and Cognizant Technology Solutions Corporation – pozitív és hatékony toborzási gyakorlatokat követnek.

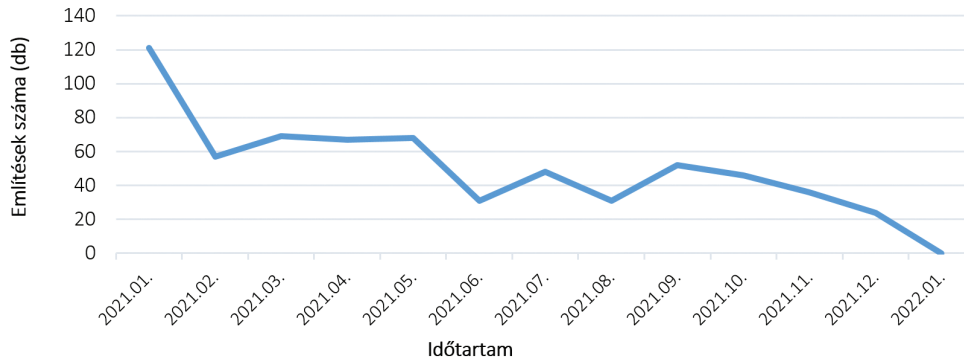
Ezzel szemben egy másik tanulmány[36] eredményei mást mutatnak. Ebben az esetben a toborzási folyamat során olyan innovatív eszközöket vettek igénybe vállalatok, mint például a Facebook, Twitter vagy a LinkedIn. A felmérés eredményeként kiderült, hogy a toborzók 94%-a nagyon kedveli a közösségi oldalakon való hálózatépítést annak érdekében, hogy a tehetségeket hatékonyan kutassák fel. Ettől eltekintve a toborzási szoftverek, illetve a pályázókövető rendszer is segít a folyamat hatékonyságának növelésében. Ennek eredménye, hogy az informatikai vállalatok 70%-a alkalmazza a pályakövetési rendszert a jelölt önéletrajzának elemzéséhez. Ez a szoftver segíthet a tehetségek kiválasztásában, felkutatásában azáltal, hogy elemzi a jelentkezők dokumentumait, keresve a kapcsolatot az előírt feltételek, tapasztalatok, valamint a korábbi munkavállalói tevékenység között. Ezáltal ellenőrizhető a jelentkező tapasztalata, illetve biztosítható a törvényeknek való megfelelőség is.

Trendek és megítélés

Az említett platformokon megjelennek különböző trendek, amelyhez szorosan kapcsolódnak a közösségimédia-adatok (például a követők vagy like-ok számának alakulása) összegyűjtésének, mérésének és értelmezésének folyamata, azaz a közösségimédia-elemzés. Ez a social listening, vagyis a közösségimédia-figyelés egy része, amely során az online beszélgetések nyomon követése folyik annak érdekében, hogy egy adott személyről, márkáról stb. való vélemény, megítélés kiderüljön.[37] Ehhez a SentiOne szoftvert használtam, amely 70 nyelven beszélő, az egész világot lefedő szöveganalitikát alapul vevő social listening szoftver. Hasonló módszertan alkalmazásával vizsgálta Bányász Péter, Tóth András és László Gábor tanulmánya a koronavírus-oltásokkal kapcsolatos állampolgári attitűdöt.[38] A keresett kulcsszót valós időben, vagy akár 3 évre visszamenőleg monitorozza, elemzi a különböző platformokon – internetes fórumok, blogok, közösségi média, weboldalak – közzétett szövegekben. Több mint 20 milliárd adat érhető el, ennek két nagy csoportját a cikkek, valamint a felhasználók által készített tartalmak adják. Ez utóbbiakhoz automatikusan érzelmi besorolást rendel a rendszer – pozitív, negatív vagy semleges besorolás a saját fejlesztésű algoritmus által. Az eredményeket különböző diagramok formájában ábrázolja a szoftver, valamint lehetőséget biztosít a tartalmak, posztok, cikkek és az említések egyenkénti vizsgálatára és kategorizálására.[39]

A #womeninit kifejezést futtattam 2021. január 1. és 2022. január 1. közötti időszakban. Ez idő alatt 650 releváns poszt jelent meg, ebből 163 pozitív, 11 negatív és 476 semleges besorolással. Ezek időszakos megoszlását a következő ábra tartalmazza:

[36] Jose–Asha 2019.
[37] *A social listening alapjai* é. n.
[38] Bányász–Tóth–László 2022: 99–125.
[39] SentiOne é. n.

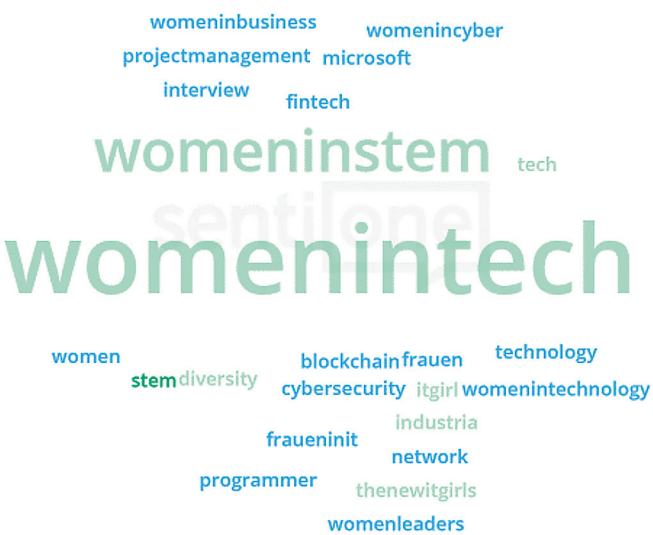


5. ábra: #womeninit kifejezés említésének alakulása
Forrás: a SentiOne alapján a szerző szerkesztése

A kiugró pontok esetében egyrészt a Dell Technologiesnál a nemzetközi nőnap alkalmából írtak egy posztot, amelyben egy sokszínűbb és egyenlőbb világ teremtését említik. Emellett kiemelkedő, amikor Franciaországban az Oracle, az IBM, a Salesforce és a Microsoft élén női vezetőket említenek. Megjelenési platform tekintetében elmondható, hogy a legtöbb poszt a Twitteren született (70,77%), valamint az Instagram (16,46%) és a Facebook (12,62%) mellett egyéb weboldalakon (0,15%) is találkozhatunk ezzel a taggel.

Kiemelendő, hogy a megosztó nemét tekintve a férfiak vannak többségben, ennek megoszlását a következő ábra mutatja:

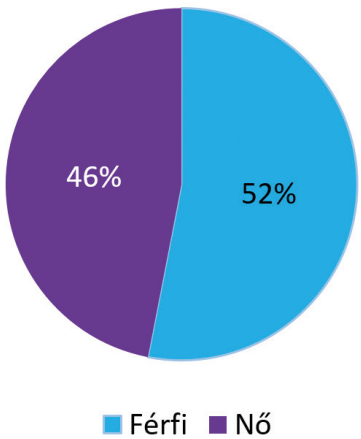
Jól látható, hogy a férfi tartalommegosztók vannak többségben, ennek oka valószínűsíthetően az, hogy az oldalt kezelő neme férfi.



6. ábra: Tartalmat megosztók nemi megoszlása
Forrás: a szerző szerkesztése a SentiOne alapján

A program további legfontosabb 25 kulcsszót is megjelenít az eredeti #womeninit tag keresése mellett. Így minél gyakoribb a megjelenés, valószínűsíthetően annál fontosabb. Ezeket a következő szófelhő tartalmazza.

Az ábra alapján elmondható, hogy a korábbi fejezetekben megjelenő kifejezésekkel gyakran találkozhatunk, úgymint a STEM, vagy éppen a kiberbiztonság, azaz a cybersecurity. Emellett a Microsoft vállalat vagy a női vezetők (womenleaders), vagy egyszerűen a nők a technológiai szektorban (womenintechnology) kéz a kézben járnak.



7. ábra: Kapcsolódó kifejezések
Forrás: SentiOne

Összegzés

Összegezve a leírtakat, elmondható, hogy egy igen szerteágazó és kihívásokkal teli területről van szó. Érdeklődéstől függően találhatunk műszaki vagy akár kevésbé műszaki munkaköröket is. A nemek arányát tekintve a nők továbbra is kisebb arányban vannak jelen az információbiztonság, kiberbiztonság területén. Több felmérésben, cikkben olvashatók ennek különböző okai, az egyik jellemző a nem azonos bérezési, juttatási körülmények.

Ebből fakadóan egy kérdőíves kutatás keretében vizsgáltam a hazai információbiztonsági, kiberbiztonsági szektorban dolgozók motivációját és tapasztalatait – többek között – ezzel a kérdéssel kapcsolatban. A kitöltők nemi megoszlásának aránya már jelzésértékű ebben az esetben – jelentősen kevesebb nő válaszadó volt. Az eredmények alapján elmondható, hogy a klaszterekbe való besorolást követően hozzáadott változók – válaszadó neme, előnyös lenne-e, ha több nő dolgozna a területen – azt mutatják, hogy akik elégedettek és hosszú távon biztosnak érzik a jelenlegi munkahelyüket, inkább támogatják a nők bevonását, mint azok, akik kevésbé elégedettek és biztosak a jelenlegi munkahelyükben. A bérezési, juttatási körülmények tekintetében elmondható, hogy a válaszadók meglátásai szerint a nők és a férfiak azonos díjazással

rendelkeznek – a kereszttábla-elemzés eredményei szerint. Mindemellett a terület választásának motivációját vizsgálva megfigyelhetők azonosságok az említett afrikai tanulmány kategorizálásával, azonban a társadalmi és családi befolyás a kitöltők esetében nem releváns tényező. A minta nagysága miatt általános következtetés nem vonható le, azonban további kiterjesztett kutatás során megfelelő alapként szolgálhat. Elmondható, hogy a közösségi média platformjainak is egyre növekvő szerepe van, amelyet a gyakran alkalmazott kapcsolattartás mellett akár toborzásra is használhatnak egyes vállalatok. Mindemellett a népszerűsítés, információátadás is megjelenik a különböző oldalakon. A trendek szorosan kapcsolódnak egymáshoz, így a #womeninit kulcsszó kapcsán találkozhatunk a #womenintehcnology vagy akár a #womenleaders kifejezésekkel is. A semleges értékeket leszámítva a megítélése inkább pozitív ezeknek a kifejezéseknek a platformokon, amelyek közül a legjellemzőbb a Twitter, mellette pedig az Instagram és a Facebook.

Irodalomjegyzék

A social listening alapjai [é. n.]. Online: https://sentione.com/hu/eroforrasok/social-listening

Ali-Hassan, Hossam – Nevo, Dorit – Wade, Michael (2015): Linking Dimensions of Social Media Use to Job Performance: The Role of Social Capital. *The Journal of Strategic Information Systems,* 24(2), 65–89. Online: https://doi.org/10.1016/j.jsis.2015.03.001

Bányász Péter – Krasznay Csaba – Tóth András (2021): A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO: A szövetség helyzete és feladatai.* Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 130–149.

Bányász Péter – Tóth András – László Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom,* 22(1), 99–125. Online: https://doi.org/10.22503/inftars.XXII.2022.1.6

Barker, William C. (2003): Guideline for Identifying an Information System as a National Security System. *National Institute of Standards and Technology,* 2003. augusztus. Online: https://doi.org/10.6028/NIST.SP.800-59 ; DOI: https://doi.org/10.6028/NIST.SP.800-59

BCS (2014): *Women in IT Survey.* Online: www.bcs.org/media/4446/women-it-survey.pdf

Bederna, Zsolt – Szádeczky, Tamás (2021): Modelling Computer Networks for Further Security Research. *Security and Defence Quarterly,* 36(4), 51–66. Online: https://doi.org/10.35467/sdq/141572

Cherdantseva, Yulia – Hilton, Jeremy (2014): Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals. In Portela, Irene Maria – Almeida, Fernando (szerk.): *Organizational, Legal, and Technological Dimensions of Information System Administration.* Hershey: IGI Global, 167–198. Online: https://doi.org/10.4018/978-1-4666-4526-4.ch010

Eurostat [é. n.]: *ICT Specialists in Employment.* Online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika, 11–30.

Hámornik, Balázs Péter – Krasznay, Csaba (2017a): A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. In Nicholson, D. (szerk.): *Advances in Human Factors in Cybersecurity.* [H. n.]: Springer, Cham. 224–236. Online: https://doi.org/10.1007/978-3-319-60585-2_21

Hámornik, Balázs Péter – Krasznay, Csaba (2017b): Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics. *Academic And Applied Research In Military And Public Management Science,* 16(3), 73–92. Online: https://doi.org/10.32565/aarms.2017.3.5

Harpeet, Singh – Kamal, Roop (2019): Recruitment Practices in IT Sector: A Study of Employees Perspective. *Pramana Research Journal,* 9(1), 318–323.

Hughes, Matthew (2019): *Women Are Only 24% of the Infosec Workforce. Now Go Follow Them on Twitter.* Online: https://thenextweb.com/news/women-are-24-of-the-infosec-workforce-now-follow-some-of-them

Jose, Sajin – Asha, P. (2019): Innovation in Recruitment and Talent Acquisition: A Study on Technologies and Strategies Adopted for Talent Management in IT Sector. *International Journal Of Marketing & Human Resource Management,* 10(2), 1–8. Online: https://iaeme.com/MasterAdmin/Journal_uploads/IJMHRM/VOLUME_11_ISSUE_2/IJMHRM_11_02_002.pdf

Khi-négyzet-próba jelentése és alkalmazása az SPSS-ben [é. n.]. Online: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba/

Krasznay Csaba (2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10(3), 38–53.

Krasznay Csaba – Muha Lajos (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Macnamara, Jim – Zerfass, Ansgar (2012): Social Media Communication in Organizations: The Challenges of Balancing Openness, Strategy, and Management. *International Journal of Strategic Communication,* 6(4), 287–308. Online: https://doi.org/10.1080/1553118X.2012.711402

Makola, Sizile – Kgosinyane, Esther (2020): How Women End Up in the Information Technology Sector: The Perspectives of South African Women. *Academy of Strategic Management Journal,* 19(4).

Mayer Annamária (2016): *A dendogram fogalma, jellemzői.* Online: https://spssabc.hu/diagram-keszitese/dendogram

Mitev, Ariel – Sajtos László (2007): *SPSS kutatási és adatelemzési kézikönyv.* Budapest: Alinea.

Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle,* 17(4), 137–156.

Paulsen, Celia – Byers, Robert (2019): Glossary of Key Information Security Terms. *National Institute of Standards and Technology.* Online: https://doi.org/10.6028/NIST.IR.7298r3

SentiOne [é. n.]: *Tudásbázis.* Online: https://sentione.com/hu/tudasbazis

Spearman korreláció [é. n.]. Online: https://spssabc.hu/ketvaltozos-elemzes/spearman-korrelacio/
TÓTH András (2022): *A digitális állam információbiztonsági kihívásai.* Budapest: Ludovika.

Jogi forrás

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Online: https://njt.hu/jogszabaly/2013-1139-30-22.1