STUDY OF PREPAREDNESS AGAINST INDUSTRIAL ESPIONAGE AMONG HUNGARIAN ORGANIZATIONS

AZ IPARI KÉMKEDÉSSEL SZEMBENI FELKÉSZÜLTSÉG VIZSGÁLATA A MAGYAR SZERVEZETEK KÖRÉBEN

MÉSZÁROS Alexandra Ágnes[1] – TICK Andrea[2]

Abstract

In the recent dynamic economic environment, industrial espionage is a serious threat to innovative organizations. From the viewpoint of this study, industrial espionage is the acquisition of competitors' trade secrets using unethical or illegal tools, to increase the organization's competitiveness and reduce the cost and time of R&D&I activities. The purpose of this research is to reveal how Hungarian organizations manage the threat of industrial espionage. This study also aims to explore what level of risk industrial espionage is considered at Hungarian organizations and whether they make efforts to prevent becoming a victim of it. During the quantitative research, the data was collected using questionnaires, the number of respondents involved in this study was 273. Based on the results Hungarian organizations are well aware of the problem and make effort to prevent the threat of industrial espionage. However, according to the results, organizations do not consider industrial espionage as high risk.

Keywords

industrial espionage, information safety, business information, innovation

Absztrakt

Napjaink dinamikusan változó gazdasági környezetében az ipari kémkedés magas kockázatot jelent az innovatív szervezetek számára. A kutatás szempontjából az ipari kémkedés a versenytársak üzleti titkainak etikátlan vagy illegális eszközökkel való megszerzése, melynek a céljai a saját versenyképesség növelése és a K+F+I tevékenységek költség- és időigényének csökkentése. A kutatás célja feltárni, hogy a magyar szervezetek mennyire vannak tudatában az ipari kémkedés jelentette fenyegetésnek, milyen fokú kockázatként tartják számon, továbbá tesznek-e preventív lépéseket a negatív hatások elkerülése érdekében. A kvantitatív kutatás során az adatgyűjtés kérdőív segítségével történt. A kutatás eredményei alapján (n=273) a magyar szervezetek tudatában vannak az ipari kémkedés jelentette kockázatnak, továbbá törekednek annak megelőzésére. Azonban az eredmények arra engednek következtetni, hogy a megkérdezettek nem tartják magas kockázatnak, hogy a szervezet ipari kémkedés áldozatává váljon.

Kulcsszavak

ipari kémkedés, információbiztonság, üzleti információ, innováció

[1] meszaros.alexandra@uni-obuda.hu | ORCID: 0000-0003-3652-0203 | PhD student, Óbuda University | PhD hallgató, Óbudai Egyetem

[2] tick.andrea@uni-obuda.hu | ORCID: 0000-0002-3139-6509 | associate professor, Óbuda University, Keleti Károly Faculty of Business and Management, Department of Management and Quantitative Methods | egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar, Módszertani és Menedzsment Intézet

BEVEZETÉS

Az ipari kémkedés a legrégebbi üzleti tevékenységek közé sorolható, és bár a módszerek jelentős átalakuláson mentek keresztül az évszázadok során, a tevékenység a mai napig szerves része a gazdaságnak. A történelem első dokumentált esetéért egészen az időszámításunk előtti 4. századig kell visszatekinteni, amikor Kína selyemhernyó tenyésztési és selyem készítési titkait megfigyelték, ellopták és alkalmazni kezdték Japánban, Koreában, Indiában és Európa szerte [1]. Az ipari kémkedés történetének egy másik jelentős esete a 19. század során zajlott, amikor a Brit Birodalomhoz tartozó Kelet-Indiai Társaság felbérelt egy botanikust, hogy tudja meg Kína tea termesztési titkait, aminek eredményeként India történelmi versenyelőnyt szerzett Kínával szemben a tea piacán [2]. Egy másik, napjainkban is aktívan zajló példa az ipari kémkedésre Kína, amely évtizedek óta működtet egy minden elképzelhető eszközt magában foglaló, alaposan kidolgozott rendszert a külföldi technológiák felkutatására és megszerzésére, hogy azt saját, versenyképes termékeivé transzformálja az eredeti tulajdonos teljes kompenzációjának hiányában [3, 4].

Kétség nem fér hozzá, hogy napjaink dinamikusan változó gazdasági környezetében a legnagyobb érték az információ. Az a piaci szereplő képes a versenyképesség megtartására, illetve fejlesztésére, akinek rendelkezésére áll az innovatív üzleti információ. Ennek a megszerzési módja elméletileg a külső környezet elemzéséből, és a belső K+F+I tevékenységekből összetevődő, hosszú és költséges folyamat. A gyakorlatban azonban ez a tevékenység gyakran megy végbe etikátlan, illegális eszközök felhasználásával. A versenyben maradásért a vállalatok hatalmas összegeket fektetnek az innovációs tevékenységbe, amely rendkívül vonzó azon szereplők számára, akik hajlandók etikátlan vagy illegális eszközökhöz nyúlni. Az ipari kémkedés a versenytársak üzleti titkainak illegális eszközökkel való megszerzése, melynek okai a saját versenyképesség növelése és a K+F+I tevékenységek költségeinek és időigényének csökkentése. A gazdasági célú ipari kémkedés jelensége nem egy modern probléma, azonban a digitális forradalom csak tovább fokozta, amelynek hatására az üzleti titok illegális eltulajdonításához már nincs szükség speciális eszközökre. A fejlődés, továbbá a hozzáférés egyszerűsödése felbátorítja a gazdasági entitásokat az információ lopásra, amihez az is nagyban hozzájárul, hogy a tevékenység biztonságosan végezhető úgy, hogy az elkövető meg sem jelenik személyesen az információ fizikai tárolásának helyszínén, vagy akár az adott országban. A jelenséget súlyosbítja, hogy bizonyos térségekben szemet hunynak az illegális üzleti információgyűjtési módszerek fölött, mivel felismerték, hogy abból profitálnak a helyi vállalatok [5].

Az ipari kémkedés témakörében kevés a rendelkezésre álló magyar nyelvű szakirodalom. Ennek oka, hogy a probléma nehezen vizsgálható. A legtöbb esetben hónapok telnek el, mire észreveszi az adott szervezet, hogy valaki jogtalanul eltulajdonította és felhasználta az immateriális tulajdonát. Amennyiben felismeri, hogy ipari kémkedés történt, akkor sem biztos, hogy a szervezet jelenti az esetet annak negatív következményeitől tartva. Abban az esetben, ha hivatalos úton vizsgálják a történteket, az információt bizalmasan kezelik, ami megnehezíti, hogy átfogó kutatás készüljön a témáról. Magyarországon is hasonló fenyegetésekkel kell szembenézni a szervezeteknek, mint más fejlett országokban működő vállalatoknak. Hatalmas mennyiségű üzleti információt tárolnak digitalizálva, közvetlen internetes hozzáféréssel. Kockázatot jelent a mobiltelefonok és más okos eszközök jelenléte. Sok magyar gazdasági entitás nincs tisztában a szabadalmaztatás folyamatával, vagy nem képes megfizetni annak magas költségeit. Amennyiben a termék még fejlesztési folyamatban van,

a szabadalmaztatás kérdése még komplexebb, mivel az újdonság még változhat, majd a megújult terméket ismét szabadalmaztatni szükséges. Az ipari kémkedés kockázatát növelheti, hogy Magyarországon bizonyos tudásintenzív iparágakban kevés a kimagaslóan jó szakember, tudásuk megszerzéséért folyamatos a verseny a vállalatok között. A szervezet érintettjeinek elégedettsége, lojalitásának kérdése is kockázati tényező.

KUTATÁSI KÉRDÉSEK ÉS MÓDSZERTAN

Az elmúlt években az ipari kémkedés gyakoriságában, és az általa okozott negatív hatásokban jelentős növekedés volt megfigyelhető, amely már nem csak az egyéni szervezetre, hanem a teljes globális gazdaságra hatást gyakorol. A probléma kutatását indokolja, hogy jelenlegi környezetben az ipari kémkedés valós és magas kockázatot jelent a szervezeteknek. A vállalatok vezetői számára fontos a probléma felismerése, és megértése, hogy lépéseket tudjanak tenni a jövőbeni ipari kémkedésből eredő veszteségek elkerülése érdekében. A kutatás célja átfogó képet adni, hogy a magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyének, milyen fokú kockázatként tartják számon, továbbá, hogy tesznek-e megelőző lépéseket a negatív hatások elkerülése érdekében.

A kvantitatív vizsgálat során a következő kutatási kérdések kerültek megfogalmazásra:

K1: A magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyeinek?

K2: A magyar szervezetek tesznek-e preventív lépéseket az ipari kémkedés kockázatával szemben?

K3: A magyar szervezetek milyen fokú kockázatnak tartják az ipari kémkedést?

Az adatgyűjtés online és papír alapú kérdőívek alkalmazásával ment végbe. A papír alapú megoldás a kitöltési hajlandóság növelése érdekében történt. A szerzők tapasztalata alapján a papír alapú módszer adatgyűjtési szempontból hatékonyabb a kézből-kézbe történő átadás, továbbá a személyes kontaktus miatt. A mintába olyan szervezetek kerültek kiválasztásra, amelyeknél magas az innovációs hajlam. A kutatás szempontjából feltételezhető, hogy azok a szervezetek, amelyek a nyereséges működés érdekében időt és költségeket áldoznak az innovációs tevékenység támogatására, kiemelten vonzók a versenytársaknak, így magas az ipari kémkedés kockázata. Az innovatív szervezeteknél a versenyelőnyt biztosító üzleti információ áramoltatása és felhasználása része az operatív feladatok ellátásának, ami további információbiztonsági kockázatokat vet fel. A kutatás során az elsődleges cél a felső-, és középvezetők megkérdezése volt majd bevonásra kerültek az alkalmazottak, mivel egy teljesen más nézőpontot képviselnek a kutatás szempontjából. Bár a minta mérete (n=273) miatt az eredmény nem tekinthető reprezentatívnak, azonban szektor szempontjából heterogén összetétele okán a kutatás jó alapot ad további vizsgálati irányok definiálásához. A minta 12 szektort foglalt magában, melyeket az 1. táblázat ismertet a Demográfiai adatok fejezetben. A gyűjtött adatok SPSS szoftver alkalmazásával kerültek elemzésre.

SZAKIRODALMI ÁTTEKINTÉS

A digitális technológia innovációja soha nem látott ütemben haladt az elmúlt évtizedekben, melynek eredményeként ma már az Ipar 4.0 által definiált környezetben működnek a vállalatok. Ez a napjainkban is jellemző, dinamikusan változó technológiai környezet

a megszámlálhatatlan előnye mellett, számtalan negatív hatással befolyásolja a gazdaság szereplőit. Az Ipar 4.0 adaptálásának hajtőerői között azonosítható a termelékenység és hatékonyság növelésének lehetősége, a piaci verseny, a cégvezetés elvárásai, ugyanakkor figyelembe kell venni az előrehaladott digitalizáció teremtette ipari kémkedés új szintjét és kockázatait [6]. Az ipari kémkedés egy interdiszciplináris megközelítésű probléma, amelynek nincsen egy standard, általánosan elfogadott definíciója [1, 5, 7]. Az ipari kémkedés egy szervezet üzleti titkainak vagy más bizalmas információjának rossz szándékkal való engedély nélküli megszerzése [8], olyan illegális és etikátlan tevékenységeket foglal magában, amely során a szervezet szisztematikusan összegyűjti, elemzi és kezeli a versenytársakra vonatkozó információkat azzal a céllal, hogy versenyelőnyhöz jussanak velük szemben [9] Az ipari kémkedés célja üzleti titkok szerzése vállalatoktól vagy kormányzati szervektől, hogy egy másik vállalat vagy állam profitáljon belőle [7].

Az egyik legkritikusabb üzleti döntés, hogy az adott szervezet elkezdje-e tevékenységét egy bizonyos iparágban. Ma már bevett gyakorlatnak számít, hogy a vállalkozások értékes és bizalmas információkat gyűjtenek a célpiacon versenyző szervezetekről a piacra lépési döntés meghozatala előtt [10]. Az a piaci szereplő, amelyik elsőként képes adaptálni a piacon a legújabb digitális technológiát anélkül, hogy időt és forrásokat költenek kutatásra és fejlesztésre, potenciális globális előnyt élveznek magas költségek nélkül [11]. Az egyre kiélezettebb globális versenyben, ahol a vállalatot a rendkívül gyorsan változó piaci lehetőségekre reagálva képesek csak profitot termelni, az üzleti titkok, információ és szellemi termékek felhasználása és védelme kulcsfontosságú a siker szempontjából [5]. Abban az esetben amikor a szervezet sem belső forrásból, sem külső nyilvános (nyílt) forrásból nem képes vagy nem hajlandó erősfeszítéseket tenni a szükséges információ megszerzéséért, akkor folyamodik ipari kémkedéshez [12]. Az elkövető szempontjából az üzleti információ és innováció lopásának szignifikáns előnyei vannak a fejlesztéssel szemben. Nem csak az az előnye, hogy a minősített anyagok és innovációk hozzájárulnak a szervezet képességeinek a fejlesztéséhez, hanem az így megtakarított költségek átcsoportosíthatók egyéb gazdasági vagy társadalmi projektekre [13].

Ahogy egyszerűsödik a kivitelezés módja, azzal arányosan tapasztalható, hogy egyre több szervezet bátorodik fel élni a törtvényt sértő információszerzési módszerekkel [10]. A digitális forradalom okozta információbiztonsági kockázat nem csak abból ered, hogy a szervezetek hatalmas mennyiségű értékes információt tárolnak elektronikusan, és ezek a rendszerek csatlakoznak az internethez, hanem ennek hatására az ipari kémkedés sokkal biztonságosabb és kevesebb kockázatot jelent az elkövető számára [14]. A problémát tovább élezi, hogy a fejlődő országokban szemet hunynak az illegálisan szerzett üzleti intelligenciával való gazdálkodás fölött, mivel ráébredtek, hogy az növeli a térség gazdasági teljesítményét [5, 15]. Ezt felismerve a fejlett országok folyamatosan erőfeszítéseket tesznek a szellemi tulajdonjog védelmére vonatkozó törvényeik erősítésének érdekében, mivel ipari kémkedést motiváló tényezők között található a szellemi jogokat védő törvények gyengesége [16], továbbá az innováció szorosan összefügg a fejlődéssel, és meghatározó tényező az ország versenyképességének szempontjából [15]. Azonban a problémát tetézi, hogy egyre növekszik az állami szereplők részvétele a technológiák illegális eltulajdonításában [13]. A főbb szektorok, melyek leginkább ki vannak téve a kevésbé fejlett országok által támogatott ipari kémkedésnek a repülőipar, a telekommunikáció, a biotechnológia, energiaipar, az elektromos ipar, és a hadiipar [13, 16]. A jelenséget már lehetetlen az országok

önálló, koordinálatlan fellépéseivel kezelni, eredményeket elérni egy globális közösségként, közösen elfogadott stratégiát és szabályokat alkalmazva, holisztikusabb szemléleten keresztül lehetne [15].

Az ipari, gazdasági célú kémkedés egy súlyos bűncselekmény, amely zavaros és nehezen áttekinthető felépítése ellenére globálisan hatalmas materiális és immateriális károkat képes okozni a szervezeteknek, azonban jelenség elleni fellépések mégsem hoznak komolyabb előrelépést [17]. A szervezetek, melyek áldozatul esnek ennek az etikátlan tevékenységnek, a negatív hatásokról félve nem mutatnak hajlandóságot az eset jelentésére, ritkán történik meg az ipari kémkedés hivatalos úton való kezelése [7, 14]. A probléma annyira súlyos, hogy a számtalan nyilvánosságra kerülő ipari kémkedéssel kapcsolatos eset csak a jéghegy csúcsát teszi ki [18]. Akár elkövető, akár áldozat a szóban forgó szervezet, amennyiben az eset nyilvánosságra kerül, magas a kockázata, hogy elveszíti az érintettek bizalmát, ami a részvények árának esését okozhatja [14], ezenfelül az a tényező is visszatartja a szervezeteket az ipari kémkedés gyanújának jelentésétől, hogy a nyomozás esetleg más, általuk elkövetett illegális gyakorlatot is a felszínre hozhat [7]. Ezt igazolja, hogy a szervezetekre globálisan jellemző, hogy bármilyen összeget hajlandók megfizetni a lopott ipari, kereskedelmi és marketing titkokért a saját versenyképességük fenntartása érdekében [11]. Továbbá az is megnehezíti a tevékenység által okozott veszteség valós értékének meghatározását, hogy hónapok vagy évek telnek el, mire a szervezet észreveszi, hogy ipari kémkedés áldozatául esett. Amennyiben az ipari kémkedés esetének hivatalos kivizsgálására kerül sor, szigorúan korlátozó titoktartási szerződések kerülnek aláírásra, ami ebben az esetben azt jelenti, hogy az elkövető és az áldozat valós kiléte jellemzően nem kerül napvilágra [14].

Az üzleti információk és titkok jogtalan eltulajdonítására napról napra újabb és modernebb módszerek állnak az erre hajlandó gazdasági entitások rendelkezésére. Kétségtelen, hogy a tevékenység művészete és módszerei sokat változtak az évtizedek során, de a lényege változatlan maradt, avagy az ellopott információt nem védték megfelelően [19]. Az IT fejlődésével párhuzamosan fejlődtek a digitálisan tárolt anyagok védelmét biztosító szoftverek, azonban az információ védelmét nem szabad csak a digitálisan tárolt titkok védelmére korlátozni. Egy darab papírra leírt információ ellopása is hatalmas károkat képes okozni, mivel az ipari kémek gyakran dolgoznak információ morzsákból, ami nagyon fontossá teszi minden információ védelmét, függetlenül annak a tárolási módjától [1]. A legegyszerűbb módszer a nyílt forrású információk felhasználása, amelyek könnyen megszerezhetők többek között szakmai kiállításokon, a közösségi médiából vagy folyóiratokból. Klasszikus és hatékony taktikák a versenytárs szemetét átnézni értékes információkat keresve, a konkurencia termékének megvásárlása és lemásolása, vagy a munkavégzés helyszínén elhelyezett fizikai eszközzel való megfigyelés [7]. A szervezeteknél az üzleti titkokat általában olyan eszközökön tárolják, amelyekhez hozzá lehet férni az interneten keresztül, ezt használják ki kibernetikus bűnözők és kémek a rendszerek feltörésével, akiknek a kiléte gyakran ismeretlen marad [19]. Az információ védelem során a leggyengébb láncszem a humán tényező az emberi természet komplexitásának köszönhetően, bár ez egy kevéssé kutatott terület, mivel a probléma kutatói a legtöbb esetben technológiai megközelítésből vizsgálják az ipari kémkedést [20]. Az ipari kémkedés egyik legetikátlanabb módszere a belső munkatársak felhasználásával való üzleti titok megszerzésére, amelynek eszközei lehetnek kényszerítés, megvesztegetés vagy zsarolás [7, 19].

EREDMÉNYEK

Demográfiai adatok

A kutatás során elemzett adatok gyűjtése kérdőív alkalmazásával történt. Olyan magyar vállalkozások kerültek a mintavétel során kiválasztásra, ahol jellemző a K+F tevékenység és magas az innovációs hajlam, mivel feltételezhetően ezen a területen a legnagyobb a gazdasági célú ipari kémkedés kockázata. A vizsgálat első szakaszában a vállalatok vezetőinek megkérdezése történt, majd a következő fázisban az alkalmazottak kerültek megkérdezésre, mivel egy egészen más nézőpontot képviselnek a probléma feltárása során. A minta nagysága n=273 fő, amelyben 49% a közép- vagy felsővezető, és 47% alkalmazott, amely jó, kiegyensúlyozott arányt mutat. A kitöltők többsége, 119 fő nagyvállalkozásnál dolgozik, 90 főt foglalkoztatnak kisvállalkozások, csak 34 fő képviselte a középvállalkozásokat. A szektor megválasztása során az innovációs hajlam volt a fő szempont, továbbá azt is követelményt határoztuk meg, hogy több ágazattól történjen az adatgyűjtés, ami megfigyelhető az eredményekben is. Az 1. táblázat a megnevezett iparágakból beérkezett válaszok számát ismerteti.

Szektor	Beérkezett válaszok száma (N=273)
Autóipar	42
Gép- és műszeripar	35
Bank- és pénzügyi szektor	31
Kiskereskedelem és disztribúció	29
Szolgáltatás	29
Hadiipar	27
Információs technológia és telekommunikáció	25
Vegyi- és gyógyszeripar	18
Technológia	17
Egészségügy és biotechnológia	9
Közszféra	7
Ingatlan	4

1. táblázat: A kutatás során megkérdezett szektorok
Forrás:Saját szerkesztés, 2021, n=273

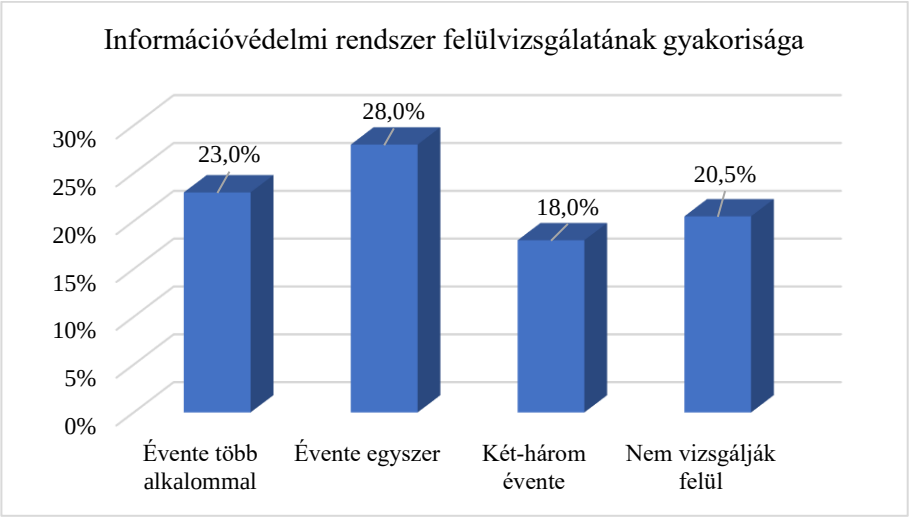
Az információvédelem humán aspektusai

A kutatás során feltárásra került, hogy a vállalatok rendelkeznek-e írott biztonságpolitikával, mivel ez keretrendszert ad a szervezet információvédelmi eszközeinek. A megkérdezettek 80%-a válaszolta, hogy a szervezet rendelkezik írott biztonságpolitikával. A nagyvállalatok 82%-a, középvállalatok 61%-a, a kisvállalatok 85%-a alkalmaz biztonságpolitikai előírásokat. A vállalkozás mérete és az írott biztonságpolitika megléte közötti kapcsolat Pearson féle khi-négyzet próbával vizsgálva közepes erősségű szignifikáns kapcsolatot mutat (χ^2= 59,267, p=0,000, Cramer's V=0,474, n=264), azaz a vállalat mérete befolyással van az írott biztonságpolitika alkalmazására. Az eredmények azt mutatták, hogy minél nagyobb a vállalkozás mérete, annál gyakoribb az írott biztonságpolitika alkalmazása. Az eredmények arra is rávilágítottak, hogy az írott biztonságpolitika megléte magában foglalja a munkavállalókkal kötött titoktartási szerződést is. A titoktartási szerződés alapvető eszköz a munkaadó kezében, mivel az ipari kémkedés legkritikusabb és legnehezebben

kontrollálható módszere a belső alkalmazottak által szándékosan elkövetett információlopás és átadás a piac egyéb szereplőjének, bár hatékonysága megkérdőjelezhető. A kutatásban résztvevő szervezetek csak 28%-ban vizsgálják a munkatárs hátterét, mielőtt hozzáférést adnak az üzleti titkokhoz és információkhoz. A nagyvállalkozások 41%-ban, a középvállalkozások 40%-ban, a kisvállalkozások 8%-ban vizsgálják a munkatársak előéletét, a megkérdezettek 18%-a jelölte a „*nem tudom*" választ a kérdésben. A khi-négyzet próba eredménye szerint a szervezet mérete és a munkatársak hátterének vizsgálata között közepesnél gyengébb szignifikáns kapcsolat van (χ^2= 59,768, p=0,000, Cramer's V=0,335, n=266), a nagyobb létszámú szervezeteknél feltételezhetően gyakoribb a háttérvizsgálat elvégzése, mielőtt hozzáférést adnak a munkatársaknak a bizalmas üzleti információkhoz.

Bár az eredmények alapján a szervezetek 80%-a rendelkezik biztonságpolitikai szabályzattal, alig több, mint a fele, 51% vizsgálja felül a rendszer aktualitását évente legalább egyszer. A rendszeres, gyakori felülvizsgálat fontossága a dinamikusan változó technológiai környezet fejlődésével arányosan növekszik, Pearson féle khi-négyzetpróba eredménye alapján a vállalat mérete és a felülvizsgálat gyakorisága között gyenge szignifikáns kapcsolat található (χ^2= 53,697, p=0,000, Cramer's V=0,259, n=266). A 2. ábra ismerteti a felülvizsgálat gyakoriságát százalékban kifejezve.

A felülvizsgálat mellett az alkalmazottak és a vezetőség folyamatos képzése és az ipari kémkedés kockázatára való felkészítése is kiemelten fontos információbiztonsági szempontból. Függetlenül attól, hogy szándékosan elkövetett cselekedet vagy véletlen hiba folytán, de a belső humán tényező legtöbb esetben hozzájárul az ipari kémkedés kockázatának növekedéséhez. Képzéssel a véletlen kialakult helyzetek jelentősen visszaszoríthatók, amit felismertek a magyar szervezetek, ugyanis a válaszadók 64%-a évente legalább egy alkalommal képzi a munkavállalókat az üzleti titkok biztonságos használatáról és tárolásáról. A kisvállalkozások 15%-a, a közepes vállalkozások 18%-a, a nagy vállalkozások 13%-a tart információbiztonsági képzést a belső érintetteknek évente egynél több alkalommal. . A vállalkozás mérete és a képzés gyakorisága közötti kapcsolat Pearson féle khi-négyzet próbával vizsgálva közepesnél gyengébb szignifikáns kapcsolatot mutat (χ^2= 115,191, p=0,000, Cramer's V=0,325, n=264).



2.ábra: Az információvédelmi rendszer aktualitás felülvizsgálatának gyakorisága
Forrás: Saját szerkesztés, 2021, n=266

Információvédelmi eszközök

A kutatás során feltárásra kerültek a szervezetek fizikai beléptető megoldásai. Az ipari kémkedés szempontjából a beléptető rendszer feladata az illetéktelen behatolások elleni védelem. A kutatásban résztvevő magyar szervezetek 79,5%-a alkalmaz beléptető rendszert a munkavégzés helyszínén, amelynek jelentős része, 72%-a belépőkártya. A megkérdezett alkalmazottak 70,5%-a tartja az alkalmazott beléptetőrendszert biztonságosnak, ezzel szemben a vezetők csak 43%-ban. A megkérdezett pozíciója és a véleménye között a kérdésben, khi-négyzetpróba eredménye alapján közepesnél gyengébb szignifikáns kapcsolat van (χ^2= 29,393; p=0,000; Cramer's V=0,332; n=264), a Kendall féle tau-b mutató (τ_b=-0,186; p=0,000) szignifikáns negatív kapcsolatot jelez, vagyis az alkalmazottak szerint biztonságosabb a beléptető rendszer, mint a vezetők véleménye alapján. A kapott eredményből az a következtetés vonható le, hogy a vizsgált probléma szempontjából a vezetőket nagyobb felelősség terheli, hogy megvédjék a szervezet versenyelőnyét biztosító üzleti információt, így számukra relevánsabb kérdés a beléptető rendszer megbízhatósága. A válaszadók 21%-a nem alkalmaz beléptető rendszert, amely megnöveli a külső behatoló általi információ lopás kockázatát. A kutatásban résztvevő kis- és középvállalkozások 27%-ban, a nagyvállalkozások 6%-ban nem alkalmaznak beléptető rendszert, a vállalkozás mérete és a beléptető alkalmazása között a khi-négyzetpróba eredménye alapján közepes erősségű szignifikáns kapcsolat van (χ^2= 128,978; p=0,000; Cramer's V=0,402; n=252), amely arra mutat rá, hogy a nagyobb méretű szervezeteknél jellemzőbb a beléptető rendszer alkalmazása.

A munkavégzéshez használt számítógépek védelmére 95%-ban használnak jelszót a megkérdezett szervezetek. A vizsgálat kiterjedt a szervezetek által alkalmazott titkosított adattátolási módszerekre, a kérdésben a Pearson féle khi-négyzet értéke χ^2= 80,635; p=0,000. A vizsgálat eredményeit a 2. táblázat ismerteti.

Vállalkozás mérete	Titkos adattárolás eszköze				
	Felhő	Külső eszköz	Szerver	Számítógép	**Összesítve**
Egyéni vállalkozó	2	8	15	15	**18**
Kisvállalkozás	37	29	48	15	**82**
Középvállalkozás	13	6	35	6	**35**
Nagyvállalkozás	55	53	95	33	**116**
Összesítve	**107**	**96**	**193**	**69**	**251**

2. táblázat: A szervezetek által alkalmazott titkosított adattárolási megoldások.
Forrás: Saját szerkesztés, 2021, n=251

A 2. táblázatban ismertetett eredmények összehasonlító értékelését a 3. táblázat ismerteti. A megkérdezett egyéni vállalkozók az adatok titkosított tárolására használnak külső eszközt és szervert is, azonban leggyakrabban az üzleti információ számítógépen való titkosított tárolását részesítik előnyben. A kisvállalkozások titkosított adattárolási megoldásainál nem található szignifikáns különbség. A középvállalkozások a szerveren való tárolást alkalmazzák leggyakrabban. A vizsgált nagyvállalkozások titkosított adattárolási megoldásai között nem található szignifikáns különbség, a megkérdezett eszközöket jellemzően alkalmazzák.

Vállalkozás mérete	Titkos adattárolás eszköze			
	Felhő (A)	Külső eszköz (B)	Szerver (C)	Számítógép (D)
Egyéni vállalkozó		A	A	ABC
Kisvállalkozás				
Középvállalkozás			B	
Nagyvállalkozás				

3. táblázat: A szervezetek által alkalmazott titkosított adattárolási megoldások összehasonlítása.
Forrás: Saját szerkesztés, 2021, n=251

A gyűjtött adatok elemzése során készült olyan vizsgálat, amelybe bevonásra kerültek a „*nem alkalmazunk titkosított adattárolási eszközt*” válaszok. A vizsgálat során készült összehasonlító elemzésben az egyéni vállalkozók bár leggyakrabban a számítógépen való titkosított adattárolási megoldást alkalmazzák, a külső eszköz és a szerver mellett hasonló arányban jelent meg a nem alkalmaznak ilyen megoldást válasz. A kisvállalkozók esetében a nem alkalmaznak titkosított adattárolási megoldást volt a szignifikánsan leggyakrabban előforduló válasz. Ez az eredmény azonban nem azt jelenti, hogy a kisebb létszámú szervezetek nincsenek tisztában az ipari kémkedés kockázatával, hanem a szervezetek infrastruktúrájának kiépítettségére vonatkozóan lehet következtetéseket levonni.

A szervezetek 92%-ban biztosítanak mobil eszközöket a munkavégzéshez, amelyeket ugyanebben az arányban használhatnak a munkatársak az otthonukban. Ez a megoldás bár az ipari kémkedés szempontjából kockázatos, az megemlítendő, hogy az adatfelvétel időszaka során a COVID-19 járvány miatt a magyar szervezetek jelentős részében volt otthoni munkavégzés. A válaszadók 80 %-a tarthatja magánál a magán mobiltelefonját bekapcsolt állapotban tárgyalások, meetingek alkalmával. A jelenlegi gazdasági környezetben, amikor a mobiltelefonok egy olyan ablakot nyitnak, amelyen át külső szereplők betekinthetnek, és azonnal tudomást szerezhetnek a szervezeten belüli innovációs tevékenységről, a

mobiltelefonok jelenléte tárgyalásokon és megbeszéléseken kiemelt kockázatot jelent az ipari kémkedés szempontjából.

Az eredmények elemzése során összehasonlításra került a vezetők és az alkalmazottak véleménye a vizsgált problémával kapcsolatban, mely pontos eredményeit a 4. táblázat ismerteti. A vezetők fele, 51%-a gondolja úgy, hogy a szervezet biztonságosan tárolja az üzleti titkokat és információt, a megkérdezett alkalmazottak 82%-a szerint biztonságos az alkalmazott adattárolási megoldás. A kérdésben a khi-négyzet próba eredménye közepesnél gyengébb erősségű kapcsolatot mutat (χ^2= 36,675; p=0,000; Cramer's V=0,376; n=259), a Kendall féle tau-b mutató (τ_b=-0,335; p=0,000) szignifikáns negatív kapcsolatot jelez.

A megkérdezett közép- és felsővezetők 25%-a tartja magas kockázatnak, hogy a piac szereplői ellopják és felhasználják a szervezet versenyelőnyét biztosító üzleti információt és titkokat, az alkalmazottak a vezetőknél többen, 41%-ban tartják magas kockázatnak a definiált problémát. A megkérdezettek véleményében az ipari kémkedés kockázatáról a khi-négyzet próba eredménye szintén közepesnél gyengébb kapcsolatot mutat (χ^2= 20,797; p=0,000; Cramer's V=0,283; n=259), a Kendall féle tau-b mutató (τ_b=-0,221; p=0,000) szignifikáns negatív kapcsolatot mutat.

A vezetők 52%-a szerint a szervezet képes kivédeni egy ellenük irányuló ipari kémkedési kísérletet. Az alkalmazottak a vezetőknél magasabb arányban, 67%-ban gondolják úgy, hogy a szervezet fel van készülve a külső, információlopás céljából megkísérelt támadásokra. A megkérdezettek véleménye között a szervezet felkészültségéről közepesnél gyengébb szignifikáns kapcsolat mutatható ki (χ^2= 24,052; p=0,000; Cramer's V=0,305; n=259), a Kendall féle tau-b mutató (τ_b=-0,207; p=0,000) szignifikáns negatív kapcsolatot jelez.

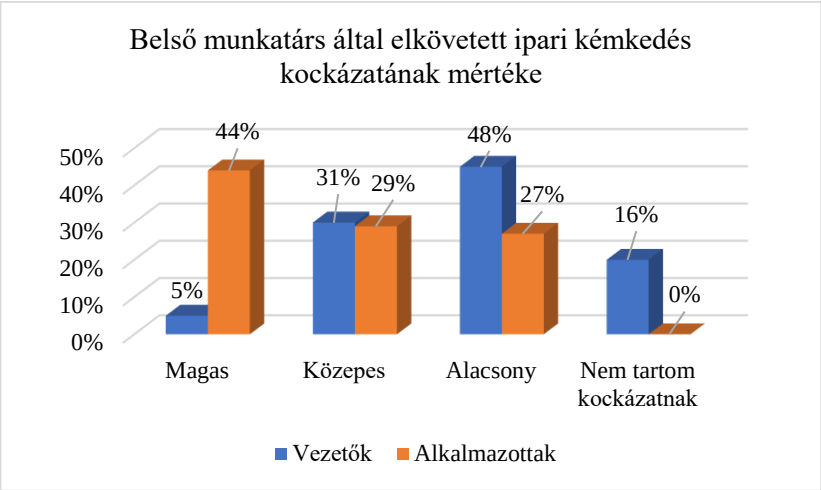
A vezetők jelentős többsége, 90%-a nyilatkozta, hogy a szervezet még nem esett áldozatul ipari kémkedésnek. Ez a magas arány igazolja a [7, 14] kutatási eredményt, mely szerint amennyiben a vezetőség tisztában van a ténnyel, hogy ipari kémkedést követtek el a szervezet ellen, abban az esetben is törekednek arra, hogy ez ne kerüljön nyilvánosságra a számtalan lehetséges negatív következmény elkerülése érdekében. A vezetők 10%-a, az alkalmazottak 29%-a gondolja úgy, hogy követtek már el ipari kémkedést a szervezet ellen. A kérdésben, hogy a szervezett esett-e már áldozatul ipari kémkedésnek, szintén közepesnél gyengébb szignifikáns kapcsolat található (χ^2= 15,519; p=0,004; Cramer's V=0,245; n=259), a Kendall féle tau-b mutató (τ_b=-0,126; p=0,026) szignifikáns negatív kapcsolatot jelez.

Állítás	Vezetők (N= 133 fő)	Alkalmazottak (N=126 fő)	Pearson χ^2	Cramer's V	Kendall's tau-b
A szervezet biztonságosan tárolja az üzleti titkokat és információkat.	51% szerint igen.	82% szerint igen	36,675 p=0,000	0,376 p=0,000	-0,335 p=0,000
A szervezet potenciális külső fenyegetésként tartja számon, hogy a versenytársak ellopják és felhasználják az üzleti információkat és titkokat.	25% szerint potenciális kockázat.	41 % szerint potenciális kockázat.	20,797 p=0,000	0,283 p=0,000	-0,221 p=0,000
A szervezet fel van készülve az ipari kémkedés kivédésére.	52% szerint igen.	67% szerint igen.	24,052 p=0,000	0,305 p=0,000	-0,207 p=0,000
A szervezet esett már áldozatul ipari kémkedésnek.	10% szerint igen.	29% szerint igen.	15,519 p=0,004	0,245 p=0,004	-0,126 p=0,026

4. táblázat: A vezetők és alkalmazottak válaszainak összehasonlítása
Forrás: Saját szerkesztés, 2021, n=273

Szervezeten belüli ipari kémkedés

A magyar szervezetek körében végzett kutatás során felmérésre került, hogy a közép- és felsővezetők, továbbá az alkalmazottak hogyan viszonyulnak a belső érintett által elkövetett ipari kémkedés kérdéséhez. Az információvédelmi rendszer leggyengébb láncszeme az emberi tényező, továbbá az ipari kémkedés nagy gyakorisággal egy belső személy közbenjárásával történik [7, 19, 20]. A két megkérdezett csoport válaszaiban jelentős eltérés tapasztalható, amelyet a 4. ábra ismertet. A megkérdezettek pozíciója és a belső érintettekbe vetett bizalom között Pearson féle khi-négyzet próbával végzett tesz eredménye alapján közepesen erős szignifikáns kapcsolat található (χ^2= 76,724; p=0,000; Cramer's V=0,542; n=259), a Kendall féle tau-b mutató (τ_b=-0,480; p=0,000) szignifikáns negatív kapcsolatot jelez. Az eredményből feltételezhető, hogy a vezetők megbíznak a szervezet belső érintettjeiben, az alkalmazottak többsége kevésbé, azonban a probléma mélyebb megértéséhez további kutatások szükségesek. A belső személy által elkövetett szándékos információlopást a vezetőség csak 5%-a, ezzel szemben az alkalmazottak 44%-a tartja potenciális fenyegetésnek. A vezetők 20%-a egyáltalán nem tartja a belső személy által elkövetett ipari kémkedést veszélynek, az alkalmazottak ezt a kérdést mind besorolták valamilyen fokú kockázatnak.



4. ábra: Belső munkatársak által elkövetett ipari kémkedés kockázatának mértéke
Forrás: Saját szerkesztés, 2021, n=259

KÖVETKEZTETÉSEK

Jelen kutatás során az ipari kémkedés fogalma a következőképpen került definiálásra: a versenytársak üzleti titkainak etikátlan vagy illegális eszközökkel való megszerzése, melynek a céljai a saját versenyképesség növelése és a K+F+I tevékenységek költség- és időigényének csökkentése. Az ipari kémkedés bár egyidős a gazdaság fogalmával, eszközrendszere jelentős fejlődésen ment keresztül, aminek eredményeként bármely entitás számára elérhető, amely hajlandó élni ezzel az eszközzel. Az egyre kiélezettebb gazdasági versenyben és a gyorsan változó piaci viszonyok között csak az a szervezet tud életben maradni, amely azonnal képes reagálni a környezetére, aminek kulcsa az információ. A vizsgálat során három kutatási kérdést került megfogalmazásra, melyek a következők:

K1: A magyar szervezetek mennyire vannak tudatában az ipari kémkedés veszélyeinek?

K2: A magyar szervezetek tesznek-e preventív lépéseket az ipari kémkedés kockázatával szemben?

K3: A magyar szervezetek milyen fokú kockázatnak tartják az ipari kémkedést?

A kutatás eredményei alapján a **K1** kutatás kérdés esetén a magyar szervezetek tudatában vannak az ipari kémkedés jelentette külső fenyegetésnek. Erre utal a rendszeresített biztonságpolitika, a munkatársak képzése, és az alkalmazott információbiztonsági megoldások. Azonban az eredményekből az a következtetés vonható le, hogy az emberi tényező jelentette belső fenyegetést a vállalatok vezetői nem tartják potenciális kockázatnak. Bár általában titoktartási szerződést kötnek, de nem végeznek háttérvizsgálatot a személyeken, mielőtt hozzáférést kapnak az üzleti információhoz. A megkérdezett vezetők több mint a fele egyáltalán nem, vagy alacsony kockázatnak tartja a belső ipari kémkedést. A **K2** kutatási kérdés esetén elmondható, hogy a magyar szervezetek törekednek az ipari kémkedés megelőzésére. Alkalmaznak információvédelmi megoldásokat, melyeket időközönként felülvizsgálnak. Jellemző, hogy az alkalmazott rendszerek használatára oktatják az érintett

személyeket. A kutatás eredményei rávilágítottak, hogy a nagy vállalatok több információvédelmi eszközt alkalmaznak a gyakorlatban mint a magyar kis- és középvállalkozások. Ez nem minden esetben enged arra következtetni, hogy a kisebb vállalatok nincsenek tudatában az ipari kémkedés veszélyének, hanem gyakran a probléma hátterében financiális, gazdasági okok és döntések találhatók. A **K3** a szervezet által érzékelt kockázat mértékére vonatkozik. A különböző kockázatok elemzése, azonosítása és csoportosítása a menedzsment feladata, akik meghatározzák annak valószínűségét és a szervezetre gyakorolt lehetséges hatását. A biztonsági rendszer nem túl gyakori felülvizsgálata, továbbá a hasonló arányú képzések arra engednek következtetni, hogy a magyar szervezetek nem tartják magas kockázatnak az ipari kémkedést. A megkérdezett vezetők fele úgy gondolja, hogy a szervezet biztonságosan tárolja az információt, továbbá fel van készülve egy esetleges ipari kémkedés kivédésére, továbbá csak a megkérdezettek 25%-a tartja számon potenciális kockázatként a szervezet ellen irányuló információlopást. A belső érintett általi ipari kémkedést a vezetők alacsony, míg az alkalmazottak magasabb kockázatnak tartják.

KONKLÚZIÓ ÉS JAVASLATOK

Az ipari kémkedés Magyarországon is fenyegeti az innovatív szervezeteket, amely több okra vezethető vissza. A K+F+I tevékenységek hosszú és költséges folyamata pénz- és időgazdálkodás szempontjából is megterheli a szervezeteket. A piacon megszerzett pozíciót megtartani, vagy növelni viszont csak versenyképes üzleti információval lehetséges. Ezek a tényezők teszik az etikátlan vagy illegális módszerekkel való információszerzést olyan vonzóvá bizonyos piaci szereplők számára. Amennyiben a szervezet versenyelőnyt biztosító üzleti információja a piacon jelenlevő másik szereplő kezébe kerül, az rendkívül súlyos anyagi és hírnévbeli károkat okozhat. A kutatás eredményei alapján a nagyobb szervezetek jellemzően több információvédelmi eszközt alkalmaznak, mint a kisebb vállalkozások. Ez azonban nem arra enged következtetni, hogy a kis- és közép vállalkozások nincsenek tudatában az ipari kémkedés jelentette fenyegetésnek, hanem financiális döntéseik során jellemzően a profit termelő tényezőket helyezik előterébe az információ védelmi beruházásokkal szemben.

Az ipari kémkedés vizsgálatánál a munkavállalók elégedettsége és lojalitása is fontos tényező. Egy külső szereplő által megtervezett ipari kémkedési kísérlet, mely során anyagi- vagy egyéb jellegű kompenzációval próbál egy belső szereplőt rávenni információátadásra, az emberi természetből fakadóan magas kockázatot jelent egy innovatív szervezetnek, amelyet nem szabad figyelmen kívül hagyni. A tudás specializálódásának eredményeként egyes ágazatokban a szakemberek értéke rendkívül megnövekedett, tudásukból hiány van a piacon. A titoktartási szerződés, mint információvédelmi eszköz, elterjed Magyarországon, de megszegése gyakran nem bizonyítható, nem szankcionálható. A problémát még komplexebbé teszi, amennyiben a magyar vállalat egy külföldi szakembert foglalkoztat, és vele szemben merül fel az ipari kémkedés gyanúja. A teljeskörű biztonsághoz javasolnánk az üzleti információhoz hozzáférő belső érintettek tevékenységének folyamatos monitorozását. Jellemző a szervezetekre, hogy az ipari kémkedés kockázatának vizsgálatakor az információs technológiai nézőpontot helyezik előtérbe, ezzel szemben javasoljuk, hogy a problémakört minél komplexebb, a humán tényezőt is magába foglaló szempontból vizsgálják. A szigetszerű információbiztonsági megoldások helyett a kutatás eredményei alapján javasoljuk a komplex, átfogó rendszerek alkalmazását. Azoknak a szervezeteknek,

amelyek jelentős értékű innovatív üzleti információt hoznak létre, tárolnak és használnak fel a munkavégzés során javasoljuk az alkalmazott információbiztonsági rendszer legalább negyedévenkénti felülvizsgálatát, és a belső érintettek oktatását, továbbá felkészítését az esetleges információbiztonsági támadásokra.

Az eredmények arra engednek következtetni, hogy a vezetők megbíznak a szervezet belső érintettjeiben, azonban az alkalmazottak többsége kevésbé. A probléma mélyebb megértéséhez további kutatások szükségesek, amely olyan tényezőket foglal magában, mint a válaszadók személyisége, és az őket körülvevő szervezeti kultúra. Az eredmény érdekes, mert a két megkérdezett csoport különböző nézőpontból vizsgálja a munkavégzés mindennapos rutinját. Feltételezve, hogy az alkalmazottak számára több lehetőség adódik megfigyelni a belső érintetteket a munkavégzés során, mint a vezetőség tagjainak, arra enged következtetni, hogy a vezetőkre jellemző a szervezeti vakság. A kérdésben a megkérdezettek neme és a belső érintettekbe vetett bizalom között elhanyagolható erősségű kapcsolat van.

A vizsgálat során az adatfelvétel 2021 tavaszán történt. A kutatás végzésének időpontjában a munkavégzés gyakorlata, Magyarországon és globálisan egyaránt, az új körülményekhez alkalmazkodva változáson megy keresztül. A megjósolható, de pontosan nem előrejelezhető változások újfajta biztonsági fenyegetéseket hoznak, amire válaszul új biztonsági megoldások születnek. A szervezet folyamatos működését és versenyképességét biztosító üzleti intelligencia védelme kiemelten fontos, függetlenül attól, hogy a munkavégzés irodában, telephelyen, gyárban, vagy amely munkakörökben ez lehetséges, otthoni körülmények között történik. Az otthoni munkavégzés számos új információbiztonsági kockázattal szembesítette a vállalatokat, akár interneten, felhőn vagy fizikai adattározón szállítják a munkavégzéshez szükséges adatokat a munkatársak. Az ipari kémkedés szempontjából ez a digitális és a fizikai adatlopást is egyszerűsítette, amely kivédésére komplex információbiztonsági rendszerek alkalmazása szükséges.

IRODALOMJEGYZÉK

[1] B. Wimmer, Business Espionage: Risks, Threats, and Countermeasures, 1. szerk., Oxford: Elsevier, 2015.

[2] S. Rose, For all the tea in China: how England stole the world's favourite drink and changed history, 1. szerk., Westminster: Penguin, 2010.

[3] W. C. Hannas, J. Mulvenon és A. B. Puglisi, Chinese Industrial Espionage, Technology Acquisition and Military Modernization, 1. szerk., London: Routledge, 2013.

[4] M. K. Lewis, „Criminalizing China," 2021. [Online]. Available: https://scholarlycommons.law.northwestern.edu/jclc/vol111/iss1/3. [Hozzáférés dátuma: 12. Szeptember 2021].

[5] T. Hou és V. Wang, „Industrial espionage –A systematic literature review (SLR)," *Computers & Security,* 98. kötet, pp. 1-12, 2020.

[6] L. Szerb, É. Komlósi és B. Páger, „Új Technológiai Cégek az Ipar 4.0 Küszöbén – A Magyar Digitális Vállalkozási Ökoszisztéma Szakértői Értékelése,"

Vezetéstudomány / Budapest Management Review, 51. kötet, 6. szám, pp. 81-96, 2020.

[7] M. Button, „Economic and industrial espionage," *Security Journal,* 33. kötet, pp. 1-5, 2020.

[8] D. A. Jameson, „The Rhetoric of Industrial Espionage: The Case of Starwood V. Hilton," *Business Communication Quarterly,* 74. kötet, 3. szám, pp. 289-297, 2011.

[9] A. Vashisth és A. Kumar, „Corporate espionage The insider threat," *Business Information Review,* 30. kötet, 2. szám, pp. 83-90, 2013.

[10] A. Barrachina, Y. Tauman és A. Urbano, „Entry with two correlated signals: the case of industrial espionage and its positive competitive effects," *International Journal of Game Theory,* 50. kötet, pp. 241–278, 2021.

[11] Y. B. Choi és W. Teresa, „The Rise of Industrial Espionage and How to Prevent It," *International Journal of Cyber Research and Education,* 2. kötet, 2. szám, pp. 9-16, 2020.

[12] E. M. Roche, „Industrial Espionage," 2016. [Online]. Available: https://www.afio.com/publications/ROCHE_Industrial_Espionage_from_AFIO_INTEL_SPRING2016_Vol22_no1.pdf. [Hozzáférés dátuma: 14. Augusztus 2021].

[13] M. Pellegrino, „The threat of state-sponsored industrial espionage," 2015. [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_26_Industrial_espionage.pdf. [Hozzáférés dátuma: 25. Szeptember 2021].

[14] K. Solberg, „Economic and Industrial Espionage at the Start of the 21st Century - Status Quaestionis," *Journal of Intelligence Studies in Business,*6. kötet, 3. szám, pp. 51-64, 2016.

[15] C. Konopatsch, „Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland," *Security Journal,* 33. kötet, pp. 83-118, 2020.

[16] S.-K. Kim, „Intellectual property right infringement, state involvement in industrialespionage, and North-South trade," *Economic Modelling,* 91. kötet, pp. 110-116, 2020.

[17] S. Knickmeier, „Spies without borders? The phenomena of economic and industrial espionage and the deterrence strategies of Germany and other selected European countries," *Security Journal,* 33. kötet, pp. 6-26, 2020.

[18] I. I. Androulidakis és F. –. E. Kioupakis, Industrial Espionage and Technical Surveillance Counter Measurers, 1. szerk., Switzerland: Springer International Publishing, 2016.

[19] N. Duckworth és E. De Silva, „Teaching New Dogs Old Tricks: The Basics of Espionage Transcend Time," *National Security: Breakthroughs in Research and Practice,* pp. 479-496, 2019.

[20] D. Ashenden, „In their own words: employee attitudes towards information security," *Information and Computer Security,* 26. kötet, 3. szám, pp. 327-337, 2018.