Gradus Vol 8, No 2 (2021) 102-112
ISSN 2064-8014

AZ INFORMÁCIÓBIZTONSÁG JELENTŐSÉGE ÉS TÖRTÉNETE

IMPORTANCE AND HISTORY OF INFORMATION SECURITY

Győrffyné Holló Krisztina [1]*

[1] Pannon Egyetem, Magyarország
https://doi.org/10.47833/2021.2.CSV.001

Kulcsszavak:
információtörténet
információbiztonság
információvédelem
paradigma

Keywords:
information history
information security
information protection
paradigm

Cikktörténet:
Beérkezett 2021. június 22.
Átdolgozva 2021. július 04.
Elfogadva 2021. július 07.

Összefoglalás
Jelen tanulmányban az információtörténet és az információbiztonság szabályozásának mérföldköveit, az információs technológiai paradigma jelentőségét vizsgálom, tekintettel arra, hogy a virtuális világ a mindennapi életünkre is nagymértékű hatást gyakorolt. Az évszázadok során megszokott szabályokat újra kell értelmezni, és egyúttal figyelembe kell venni az információs társadalom új értékeit is.

Abstract
In this paper, I examined the milestones in the history of information and information security regulation, the significance of the information technology paradigm. The virtual world has also had a major impact on our daily lives. The rules that have been used for centuries need to be reinterpreted, taking into account the new values of the information society.

1. Bevezetés

Történelmünk több ezeréves időszaka alatt sokáig nem tulajdonítottak jelentőséget a mai értelembe vett információ fogalmának és az információbiztonság szabályozási rendszer kiépítésének. Bár az információ jelentőségét és a tudást nem becsülték alá, mégis az információbiztonsági intézkedések legfőképp technikai jellegűek voltak, és a fellelhető tudományos értekezések is leginkább az „ideák” vagy a szellemi alkotások eszméit világítja meg. Az ókori társadalmak, sőt a filozófia nagy mesterei kevésbé foglalkoztak az információ által betöltött jelentőségre, birtoklásának következményére, így előnyére vagy hátrányára.

Az elektrotechnikai fejlődés, az információelmélet kutatásának eredményei és az informatikai technológia, valamint a paradigmaváltás a különböző tudományágakban a korábbi évszázadok „nyugalmas” életviteléhez képest oly mértékű információrobbanást okozott, amely az ipari forradalom negyedik állomásához vezetett, és ipari, társadalmi, kulturális változásokat eredményezett. Az információbiztonság túlmutat egy divatos kifejezésen, és a vonatkozó szabályok felállítása és alkalmazása jelentősen befolyásolja az információs rendszerek működését. Napjainkban az információs társadalomban a rendelkezésre álló információs rendszerek és szolgáltatások létfontosságú szerepet játszanak mind a háztartásokban, mind az üzleti életben, ezért megbízhatóságuk és biztonságuk lényeges szempont.

A biztonsági események nagyságrendje, gyakorisága és hatása évről évre, mondhatjuk, exponenciális mértékben növekszik, ami súlyos fenyegetést jelent az információs társadalom működésére és tevékenységére. Az információs rendszerek a működésük akadályozására,

* Kapcsolattartó szerző.
E-mail cím: gyorffy.kriszta@gmail.com

károkozására vagy adatainak felhasználásával jogtalan haszonszerzésre irányuló szándékos és ártalmas cselekmények célpontjaivá válhatnak. Az informatikai incidensek nehezíthetik a mindennapos életet, a gazdasági tevékenységek gyakorlását, jelentős pénzügyi veszteségeket, valamint bizalomvesztést és súlyos károkat okozhatnak az európai közösségnek és a gazdasági tevékenységeknek.

A múlt század elején még semmi jel nem mutatott arra, hogy az évszázad végére egy teljesen új társadalmi rendszer fog kialakulni. A hírközléstechnika megjelenésével és rohamos fejlődésével egy olyan technikai és kulturális forradalmi változás ment végbe, amire egészen egyedi és példaértékű. Az információs társadalom fogalma a huszadik század elején még teljesen ismeretlen volt. Az információelmélet megalkotásával 1948-ban egy új korszak született. A kibernetika és a matematikai információelmélet, az információkutatás és -tudomány első, kezdeti szakasza, amely az információ olyan jelentőségét ismerte fel, amit még korábban egyáltalán nem. Claude Elwood Shannon: A Mathematical Theory of Communication (The Bell System Technical Journal), és Norbert Wiener: Cybernetics or Control and Communication in the Animal and the Machine című műve 1948-ban történelmet írt.

A tudás és az információ szerepe, jelentősége mindig meghatározó volt a gazdaság és a társadalom életében, így napjainkban a felgyorsult társadalmi, gazdasági, technológiai fejlődés folyamatai ezt a szerepet folyamatosan alakítják. Az utóbbi évszázadban fontossá vált a gyors, biztonságos elektronikus információáramlás[1] és a támogató folyamatok, technológiák mindenkori rendelkezésre állása, az egyéni tudás megszerzése, terjesztése, fejlesztése, mind a versenyszférában, mind a közigazgatásban egyaránt. A matematikus Norbert Wiener alapvető tézise, hogy a szabályozás, úgymint az információ is egy olyan meghatározó fogalom, amellyel minden rendszer – beleértve a szervezeteket is – jellemezhető.[2]

A kibernetika alapfogalmai között szerepeltethető a visszacsatolás, a homeosztázis és entrópia, de meghatározó az információ és a kommunikáció is. Bár a huszadik század közepén még alig lehetett elképzelni, de ma már biztosan tudjuk, hogy ezen meghatározások megegyeznek az információs társadalom fontosabb kulcsfogalmaival. Az információelmélet publikálása óta egy egészen új, információs társadalmi forma jött létre, amelynek központi eleme, az elektronikus rendszerek és eszközei. Ma már napjaink részévé vált ez az új technika és a munkafolyamtok szerves része, támogató pillére. Az informatikai hálózatra és azok eszközelire, rendszereire épített folyamatok nélkülözhetetlenek a mindennapi tevékenységben, így a háztartásokban és az intézményekben.

Az információs rendszerekre épült világunk oly mértékű, hogy szabályozási rendszer is társult hozzá, így például az információbiztonsági szabványok (ISO 27000 szabványcsalád) vagy az Európai Uniós rendelkezések, mint például a GDPR[3]. Az információs rendszer nélkülözhetetlen eleme az informatikai technológia és a hálózatelmélet, amely megjelenésével és elterjedésével immár az ipar 4.0 elnevezésű negyedik ipari forradalom korát éljük.[4] A negyedik ipari forradalom alapja a digitalizáció és az információ, a számítógép csupán eszköz.

Az informatika kiemelt szerepét tükrözi az elektronikus kormányzati tevékenység létrejötte, a közigazgatás-tudományhoz való kötődése. Az informatikai hálózatnak biztosítania kell az elektronikus információ rendelkezésre állását, biztonságos kezelésének lehetőségét és sértetlenségének megőrzését, amely napjaink információbiztonsági területének jelentős alapelve. Minden lánc olyan erős, mint a leggyengébb láncszeme, ez a megállapítás vonatkoztatható egy irányítási rendszerre, így annak információbiztonsági területére is.

2. Az információs technológiai paradigma

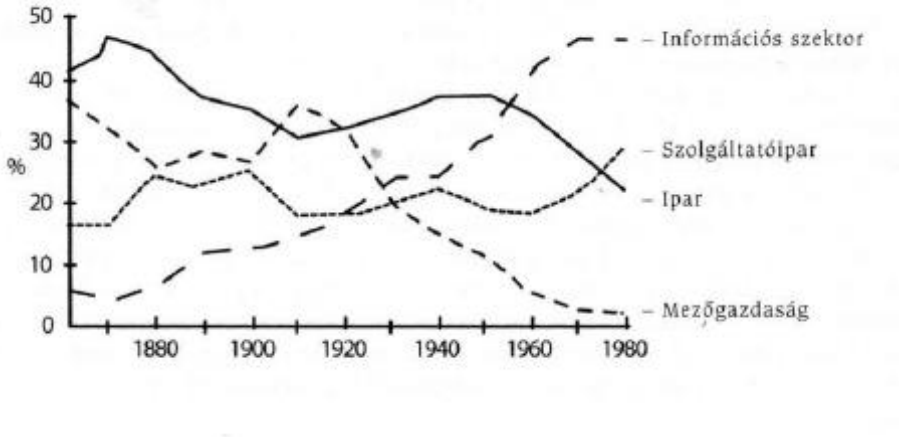
Az információ elméletben és gyakorlatban is napjaink szerves része, a kapcsolódó kutatások több szinten, így a filozófiai vagy a műszaki szintéren is megtalálhatóak. Kétségtelen, hogy ez a tudomány sok kutatót vonz, azonban nem valószínű, hogy a legtöbb ember világosan meg tudja fogalmazni, milyen az információs világhoz tartozó tudomány. Vannak, akik azt gondolhatják, hogy az elektronikus információelmélet vagy a műszaki tudományok, míg mások azt mondják, hogy egy átfogó, bonyolult értelmezés, amely foglalkoztatja az informatika, a távközlés, az elektronikus eszközök és technológiák tudomány területeinek kutatóit, valamint a genetikával foglalkozó vagy a mérnöki szakembereket is. Mivel a vélemények ettől a ponttól eltérnek, jelenleg nem lehet

egyértelmű következtetést levonni, mi az az információ és lényegében mely tudományághoz tartozik.[5]

Napjaink társadalomkutatóinak álláspontja szerint az ipari társadalomból az információs társadalomra való áttérés már az 1970-es években elkezdődött[6], ahol a hálózati társadalom a hálózat köré épül, a folyamatos információáramlást a hálózati technológiával biztosítják. Az új technológia befolyásolja a társadalom társadalmi, gazdasági és politikai szereplőinek egymáshoz való viszonyát, ezért hatást gyakorol a szereplők tevékenységeire, ezáltal egészen újfajta gazdaság, egyedi fejlődési mód jelenik meg. A gyors tájékoztatás és az információ jelentősége megnőtt, amely egyben a hálózatépítés kritikus jelzőjévé vált. Az információs társadalom egy olyan új, speciális megnyilvánulási forma, amelyben az információ előállítása, feldolgozása, továbbítása alapvető jelentőséggel bír korunk gazdasági és társadalmi rendszereiben. A fizikai és a szellemi munkaerő aránya, úgymond a szellemi vagy más néven a „tudásmunkás" megjelenésével és tömeges elterjedésével jelentősen megváltozott.

A szellemi tevékenységek, így a kutatási tevékenységek értékelése is megnőtt a termelési tevékenységben az előállított termék értékének nagy részét immár a befektetett szellemi tőke teszi ki és csak kis hányada az alapanyag. A hálózati paradigma is egészen újszerű formában mutatkozik meg, mivel a korszerű, elektronikus és interaktív kommunikációs eszközök megjelenésével és széles körű elterjedésével új megvilágításba került. A gépek elterjedése és az világ elektronikus forradalmasítása nemcsak a termelési folyamatokat rövidítette le, de az innovációs lánc idejét is. Az elektronikus hálózat a technika modernizálódásának köszönhetően belopódzott és széleskörűen, valamint exponenciális gyorsasággal szétterjedt a társadalom különböző rétegeiben, így a gazdaságban, a kultúrában, a politikában, az élet valamennyi részébe, megalkotva ezáltal a hálózat egy egészen új megjelenési formáját.[7] Az innovációs láncolat időtartamának csökkenése az infokommunikációs technológiát is érinti.

A posztindusztriális társadalomban három dimenziónak van jelentősége[8] és ezek közül is az árutermelőről a szolgáltató társadalomra váltás, valamint az elméleti tudás rendszerezésének központi szerepe a műszaki újításokban igazolja az információs technológiai paradigma elméleteket. Az új intellektuális technológia a rendszerelemzés és a döntéselmélet alapvető eszköze. A szolgáltatói társadalom megvalósulása számszerű adatokkal is alátámasztható, hiszen például az Egyesült Államok 1970-es adata szerint már a munkavállalók 65 százaléka a szolgáltatóiparban dolgozott, míg az árutermelésben vagy az építőiparban 30 százalék és a mezőgazdaságban csupán 5 százalék. Ezzel szemben az ipari társadalmak a szolgáltatások nagy részét az árutermelést kiszolgáló ágazatok, így szállítási, közmű és pénzügyi tevékenységek tették ki. (1. ábra)



1. ábra. A négy fő szektor foglalkoztatottsági aránya az USA-ban, Az információs társadalom társas keretrendszere, Daniel Bell (Információs Társadalom, I. 16., Budapest, 2001.[9]

A mai, posztindusztriális szolgáltatások már más jellegűek, jobban koncentrálódnak a humán jellegű, így az egészségügyi, szociális, oktatói, valamint a professzionális, mint például a rendszerszervezői, informatikai, közigazgatási szolgáltatásokra. Minden ágazat jelentős mértékben támaszkodik az

információs, hálózati technológiára és rendszerszervezésre, -támogatásra. A hálózati rendszerek támogatásával az elméleti tudás kodifikációja új társadalmi változást hozott, amely szellemi irányítóvá vált. A tudomány és a mérnöki tevékenység határa elmosódik, ahol a tudomány fejlődése segíti az ipart és a mérnöki eredmények további kutatásokat generálnak mind elméleti, mind gyakorlati szinten. Az elméletek összekapcsolódása és alkalmazhatósága megnőtt, új lehetőségeket, új trendet és újabb felfedezéseket, kutatásokat, szakosodást hozott.

A huszadik század második felében a megjelentek, elterjedtek és megnövekedtek a rendszerezett komplexitás elméletével foglalkozó tudományágak és módszertanok, így például az információelmélet, a kibernetika, a döntéselmélet, a haszonelmélet, a sztochasztikus folyamatok. Ezek szakterülete és tudományos kutatása olyan jelentős módszereket dolgozott ki, mint a Markov-lánc, a lineáris programozás vagy a statisztikai döntéselmélet. A tizenkilencedik század egyik meghatározó tényezője az elektromosság a huszadik században pedig a számítástechnika az az „analitikus motor", ami befolyásolta életünket. A hálózatba kötött számítástechnikai eszközök ma már minden fejlett országban elérhetőek. A számítógép lett napjaink társadalmainak igazgatási alapvető eszköze is, amely rendszerezi és feldolgozza a sokasodó tranzakciót, adatot és egyéb információt, amely például a közigazgatási irányításhoz, államigazgatáshoz is elengedhetetlen. A társadalmi kapcsolatok, tranzakciók és egyéb információk száma az elektronikus rendszerekben évről évre exponenciálisan nő, optimális kezelhetősége viszont már a jövő generáció problémája.

1. táblázat. Posztindusztriális társadalom összehasonlító táblázata, Az információs társadalom társas keretrendszere

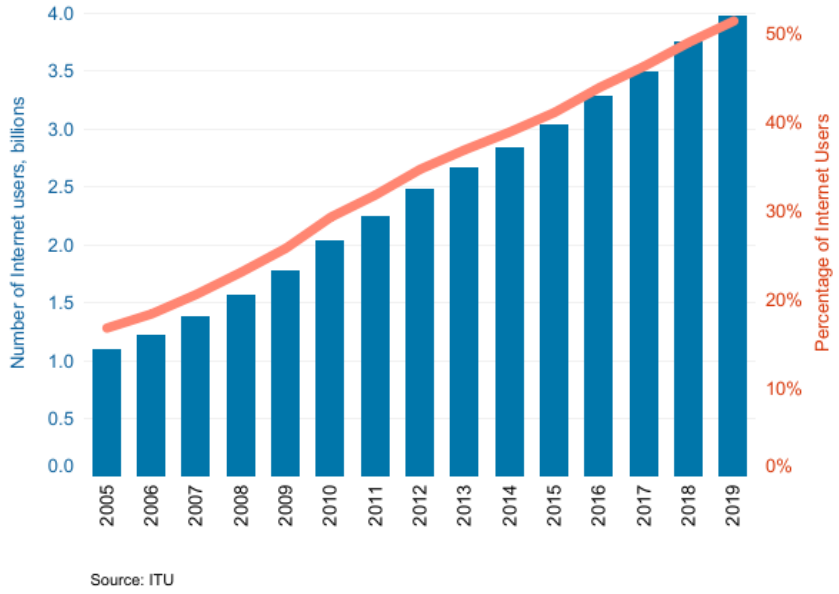
	Preindusztriális	***Indusztriális***	***Posztindusztriális***
Termelési mód	Kitermelő	Termelő	Feldolgozó; újrahasznosító
Gazdasági szektor	**Elsődleges** Mezőgazdaság Bányászat Halászat Favágás Olaj és gáz	**Másodlagos** Árutermelés Gyártás Tartós iparcikkek Nem tartós iparcikkek Építőipar	Szolgáltatások: **Harmadlagos:** Közlekedés, Közüzemek **Negyedleges:** Kereskedelem, Pénzügy, Biztosítás, Ingatlan **Ötödleges**: Egészségügy, oktatás, kutatás, kormányzat, kikapcsolódás
Átalakulást hozó erőforrás	**Természetes energia** Szél, víz, igásállatok, emberi izomerő	**Gyártott energia** Áram, olaj, gáz, szén, atomenergia	**Információ** Számítógépek, adatátviteli berendezések
Stratégiai erőforrás	Nyersanyagok	Finánctőke	Tudás
Technológia	Kézműipar	Gépi technológia	Intellektuális technológia
Tudásbázis	Kézműves, fizikai munkás, gazda	Mérnök, betanított munkás	Tudós, műszaki és professzionális foglalkozások
Módszertan	Józan ész, próba-szerencse; gyakorlat	Empiricizmus, kísérletezés	Absztrakt elméletek, modellek, szimulációk, döntéselmélet, rendszerelemzés
Időperspektíva	Múltorientált	Ad-hoc alkalmazkodó képesség, kísérletezés	Jövőorientált: előrejelzés és tervezés
Tervezés	Játék a természet ellen	Játék a mesterséges jövő ellen	Személyek közötti játék
Vezérelv	Hagyományközpontúság	Gazdasági növekedés	Elméleti ismeretek kodifikációja

Egy üzleti vagy egy közigazgatási szervezet életében egyre inkább domináns helyet foglal el az intellektuális technológia és az posztindusztriális társadalom (1. táblázat) központi tényezője az intellektuális technológia. Az információs technológiai paradigma elmélete szerint az alapanyag maga az információ, további jellemzője az áthatóság, az újabb és újabb egymásra épülő hálózati logika, amely ebből eredően nagyfokú rugalmassággal bír. A speciális technológiák növekvő konvergenciája állapítható meg, amelyek erősen integrált rendszerhez vezethetnek. Összességében megfogalmazható, hogy a „többszörösen rétegződött hálózatként a nyitottság felé tart”.[10] Az információs technológiai paradigma legfontosabb jellemzői a tudásalapúság, a horizontalitás, a hálózatiság, az adaptivitás, a tanulékonyság, az időtlenség, továbbá a kölcsönös függőség. Az elektronikus hálózatiság felgyorsult kommunikációt, térbeli távolságok összeszűkülését, a cselekvési idő lerövidülését, a határok kitolódását majd eltűnését eredményezi és ezen kívül még számos előnyt és hátrányt, amely visszahat a társadalomra, a gazdaságra és a kultúrára. A modernebb hálózatok új típusú kommunikációs és média technológiára épülnek, amely forradalmasította az eddigi technológiákat és további kulturális változásokat eredményezett. A virtuális környezet megjelenése innovatív hatással bír, már az oktatásban és a tudomány világában is érezteti hatását.

A legfiatalabb generáció interaktív táblák segítségével tanulhat és a hálózat segítségével a Föld más pontján élő hasonló korú és érdeklődésű diákokkal tarthat online kapcsolatot. A tudományok területén hatalmas változást hoz az eredmények azonnali publikálhatósága a világhálón, és azok szinte azonnali felhasználhatósága és továbbfejlesztése. Vélhetően a tudományágak társadalomban betöltött szerepe tovább fog erősödni. Az elektronikus hálózat és a gyors információáramlás hátránya, hogy néhány fiatal tudományterületen a tíz évnél régebbi publikáció elavultnak tekinthető. A dinamikusan fejlődő technikai, társadalmi és kulturális változás hatására a kutatásra fordítható idő is lerövidül.

Az elektronikus hálózat mindennapos használatával mára már megnőtt az igény arra, hogy a földrajzilag távol élő tudósok és kutatócsoportok együtt dolgozhassanak, ezen kívül természetes igénnyé vált az internet, valamint a szükséges elektronikus eszközök megléte és a szükséges megfelelő szintű szolgáltatása.

Az internet dinamikus elterjedését az ITU által készített, internetet használók számának statisztikai adata (2. ábra) igazolja.



2. ábra. International Telecommunication Union, Statistics, Internetet használók száma, 2005-2019[11]

Természetesen a nem lektorált vagy az interneten nagy mennyiségben megtalálható információk között egyre nagyobb mértékben jelennek meg nem ellenőrzött és nem megbízható adatok is, ezért

a tudományos ellenőrzésnek vagy önellenőrzésnek tovább kell erősödnie. Az internet logikája a szabadság eszméjén alapul, amely a mondás szerint „azt tehetünk, amit csak akarunk, akkor és úgy, amikor csak akarjuk”. A virtuális világban ez is csak egy illúzió, mivel a dezinformációnak ebben a környezetben is vannak következményei, de egészen más jellegű, mint egy „face-to-face” kapcsolat esetében. A túlzott szabadság teret enged az anomáliáknak, mivel a virtuális világ bármely típusú avatarja felhasználható, így egy közösségi oldalon bármilyen korú, kinézetű személyiség felhasználható. A résztvevők tudatosan alkalmazhatják az eltérő személyiségeket. Ugyanakkor egyes esetben a külső megjelenés lényegtelen, például egy közösségi csoport kialakulásában és összetartó erejében a bizalom, az, ami felértékelődik, és az összetartó erő kulcsfontosságú tényező lehet.

3. Az információbiztonság jelentősége

Az információvédelem és az információbiztonság szabályozásának kialakulása, fontossága elsősorban a katonai rendszereknél jelentkezett és alkalmazás szempontjából a II. Világháborúban komoly áttörést jelentett egy-egy katonai művelet esetében. Tekintettel arra, hogy az információ – tudás – hatalom hármas lényegi összefüggéseket tartalmaz, a fontos vagy titkos információt – bár ilyen módon az ókorban még nem azonosították – megfelelő biztonsággal kellett ellátni, tehát védelem alá kellett helyezni. Már az ókorban is fontos szerepet játszott az információk megszerzésére vagy annak megakadályozására irányuló tevékenység, a mai szóhasználattal élve az információvédelem.

Az információ védelmére irányuló törekvések már a beszéd megjelenésével egy időben, az emberi társadalmak kialakulásával egyidős tevékenység, hiszen már akkor népszerű tevékenységnek számított az információ „eltulajdonítása”, mivel így próbálták meg ellesni a vadászati szokásokat, a túlélési lehetőségeket vagy az ehető növények termesztésére vonatkozó praktikákat.[12]

Az információbiztonság története tehát az ősidőkig visszavezethető. Bár a társadalmi és kulturális fejlődéssel a rendelkezésre álló és megszerezhető információk köre, a jelkészletek megjelenésével és az írás elterjedésével megjelenési formája folyton változott, és ennek megfelelően a vonatkozó információmegszerzéshez és annak megakadályozásához tartozó módszerek is állandóan változtak[13], de a lényegét tekintve, miszerint a védelem és a biztonság a birtokosa számára fontos, tulajdonképpen változatlan maradt. Az ókori társadalmak fejlődése során a különböző jelekből, strukturált közlési mód, az írás megjelenésével már rögzített formában is rendelkezésre állt az információ, így könnyebben tárolhatóvá, másolhatóvá vált, ezáltal átlépve az addigi szavak és emlékezőképesség megőrzésének korlátait.

Mai napig rendelkezünk ókori írásos emlékekkel, amelyek segítenek megfejteni az akkori társadalmi és mindennapi élet sajátosságait, örökíthetik a hagyományokat és a tudományos, filozófiai és jogi álláspontokat, kutatási eredményeket. Az írás megjelenése elősegítette az ókori társadalmak fejlődését, az irányításban és a működésben meghatározó szerepet töltött be. Az írástudó emberek kiemelkedő rangot kaptak. Az írástudók alacsony száma egyfajta védettséget jelentett, mivel csak kevesen voltak képesek elolvasni és megfelelően értelmezni a küldemények információtartalmát. Az írás megőrzése elősegítette az információ pontos, eredeti tartamlának tárolását és továbbítását az illetékes személy részére. Az információ ilyen fajta tárolásával és továbbításával már jelentéktelenné vált a személyes jelenlét, mivel a hírnökök és a futárok, később a posta és az elektronikus hálózat betöltötte ennek funkcióját.

A szóbeli közleményeket szükség esetén az írásos forma váltotta fel. Ez természetesen nem azt jelentette, hogy a szóbeliség jelentéktelen, és teljes mértékben elvetendő. Ma is vannak jelentős szónoklatok, beszámolók, tudományos értekezések, amelyek hozzájárulnak az innovációhoz, de az írásos dokumentálás is létfontosságú megnyilvánulási forma. Az írás megjelenése, csakúgy, mint az elmúlt évtizedekben az elektronikus hálózat és annak eszközeinek megjelenése és napi szintű alkalmazása forradalmasította az információ kezelését, tárolási lehetőségét és továbbítását. Napjaink információs technológiája alkalmas arra, hogy nagy mennyiségű írott információ sértetlenül célba érkezzen és a megérkezés és olvasás tényét nyugtázza a küldő részére.

Már az ókori államokban megjelentek a kémkedési és ezzel szemben az elhárítási módszerek is. Különböző algoritmusú titkosírások, jelszavas és rejtjelezési megoldások jelentek meg, amely

vonzotta a kódmegfejtési és kódfeltörési tevékenységeket is. Az írásos információ megjelenésével és a közlemény továbbításával újfajta kockázat jelent meg, a hírvivő vagy a közlemény elfogása és jogtalan felhasználása, az üzenet kicserélése félrevezetés céljából, a címzett és a feladó megtévesztése és az információ hitelességének kétségbe vonása.

Az információ nagy mennyiségű rögzítését elősegítette a középkorban feltalált könyvnyomtatási módszer. Az újfajta információkezelési lehetőségek új biztonsági és védelmi technológiák kialakítását, használatát és intézkedéseket vontak maguk után. Védelmét tekintve a füstjelektől, az uralkodói pecséten, a megbízható futáron keresztül, a különféle kódolási típusokon át, a kriptográfia számtalan fajtájával találkozhatunk a történelem különböző szakaszaiban. Az írást csak az tudta elolvasni, aki ismerte, ők voltak a kiváltságosok. Később a kriptográfia megjelenése hasonló célokat szolgált, mégpedig, hogy egymástól távol lévő emberek biztonságos módon tudjanak üzenetet váltani. Az ókori megfelelője a szteganográfia (ún. rejtett írás). Hérodotosz számol be arról, hogy a perzsa király ellen szövetkezni akaró Hisztaiaeusz leborotváltatta a küldöncének haját, „ráírta” az üzenetet, majd megvárta, amíg a küldöncének haja újból kinő, csak így kelhetett át a határon. Ez a típusú védelmi intézkedés térben és időben is megfelelőnek bizonyult. A küldönc célba ért, leborotváltatta fejét és megmutatta az üzenetet a címzett Arisztagorasznak.[14]

A fenti megoldásokon kívül ismert még a Polübiosz-négyzet, a Caesar-rejtjel, a bibliai kódok, a grand chiffre kódja (a Napkirály, XIV. Lajos legtitkosabb üzeneteinek kódolása), Pázmány Péter és I. Rákóczi György titkosírása, a morzejelek, a Vigenère-kód (1918), a navahó nyelv használata (navahó indiánok nyelvével való kommunikálás a II. Világháborúban). Történelmünk során tehát tapasztaltuk, hogy az információt védeni kell, védelmére intézkedéseket kell megfogalmazni, és ezeket az intézkedéseket megfelelő iránymutatások mentén kell kialakítani, tehát az információkhoz illetéktelen hozzáférést meggátló szabályozásokat, folyamatokat és megoldásokat kell kialakítani. A megoldások teljesítését és hatékonyságát előre definiált módszer és folyamatleírás mentén ellenőrizni kell. Az eredményekre intézkedést kell készíteni, amelyet hatékonyan vissza kell forgatni a rendszerbe.

Védelmi módszereket fejlesztenek ki minden olyan rendszerre, amely információt és különösen személyes adatot tartalmaz, Az információvédelem másik jelentősége a fenntartás és tovább fejlesztés. A fejlesztés egy adott körfolyamat mentén hajtható vége, amelyet az információbiztonsági szabványok is megfelelően tükröznek.

Az informatika fejlődésével együtt alakult ki annak védelmi igénye is, amelyet megpróbáltak később szabályozási keretek közé illeszteni. A szabályozási törekvések immár túlmutattak a haditechnika, a hírszerzés és a védelmi intézkedések határain túl, hiszen ma már behálózza az egész ország, földrész, illetve a fejlett társadalmak infrastruktúráját, irányítását és működését is. A kommunikáció szabályozása és gyakorlati megvalósítása vonatkozik a közszolgálati és a vállalati információs rendszerekre egyaránt. Az alkalmazott megoldás az ITIL (Information Technology Infrastructure Library), ami lényegében egy szabályozás, illetve az informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan és ajánlás megnevezése. Az ITIL eredetileg BS 15000 (British Standard) jelöléssel brit szabvány és kormányzati ajánlás volt, és a közigazgatási területen meg is követelték ennek alkalmazását.

Az ITIL időközben nemzetközi szabvánnyá vált, világszerte felhasználói szervezeti támogatást meghatározó módszertanná fejlődött az informatikai infrastruktúra és informatikai szolgáltatás és annak irányítása területén. A szabványt számos nemzetközi informatikai cég is elfogadta és alkalmazta (mint például a HP – Hewlett Packard, Microsoft, vagy az IBM). Az ITIL Biztonságirányítás (Security Management) kiadvány a BS7799 brit szabványt használta utalásként, az ITIL folyamatok biztonsági irányítás kiegészítéseként.[15]

Az információbiztonság szabályozására vonatkozó jelentősebb ajánlások mai változata a Nemzetközi Szabványügyi Szervezet (International Standard Organization, ISO) és a Nemzetközi Elektrotechnikai Bizottság által jóváhagyott és kiadott ISO/IEC 27000 szabványcsalád, amelynek alapját képező BS7799 eredetileg a Brit Szabványügyi Hivatal (British Standard Institute, BSI) által kiadott brit szabvány. Ennek előzményei az 1987. májusában alapított brit DTI/CCSC (DTI/CCSC = Department of Trade and Industry's, Commercial Computer Security Centre - Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép Biztonsági Központ) tevékenységéhez nyúlnak vissza, amelynek feladata volt a nemzetközi szinten is elfogadható informatikai biztonság értékelési és tanúsítási kritériumok és mechanizmus kidolgozása.

A DTI/CCSC másik feladatában a brit számítógép felhasználók támogatását tűzte ki célul, amely 1989-ben „A Users Code of Practice” címen került kiadásra, mint az informatikai biztonság megteremtésére és fenntartására vonatkozó legjobb gyakorlatot leíró dokumentum. A brit Nemzeti Számítóközpont az ipari terület felhasználóiból szervezett konzorcium bevonásával ezt továbbfejlesztette. Az eredmény a PD 0003 jelű BSI ajánlás tervezet lett és „A Code of Practice for Information Security Management, Az információbiztonság menedzsmentjének gyakorlati kódexe” címmel jelent meg. A dokumentum IT szakemberek és felhasználók közös munkájával tovább fejlesztésre került, míg végül a BSI 1995-ben BS7799 szabványként adta ki. Később a szabványt az informatikai biztonság menedzsment résszel bővítették.

A BS7799 második része „Az információbiztonság menedzsment rendszerének specifikációja” (Specification for Information Security Management Systems) címmel került kiadásra 1998-ban, az első rész kiegészítéseként. A BS 7799 szabvány első felülvizsgálata 1999-ben történt meg, és az első részét nemzetközi szabványként (ISO) történő elfogadásra javasolta a BSI.

A Nemzetközi Szabványügyi Szervezet 2000. év augusztusában a BS 7799 1. részét változatlan szerkezetben, és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven. Az ISO/IEC 17799: 2005-ben egy nagy szabványszám- és jelzet váltás következményeképpen létrejött a ma ismert ISO/IEC 27000 szabványcsalád, ami a nemzetközi szabványosítás területén egy kiemelt, speciális témakörnek van fenntartva, az információbiztonság és annak menedzselése, amely tartalmazza a tervezésre, a kiépítésre, a fejlesztésre és fenntartásra valamint az ellenőrzésre vonatkozó nemzetközi ajánlásokat. Az ajánlásokból származtathatók a hazai és az Európai ajánlások, irányelvek, utasítások, előírások és törvények.[16]

Mindezen szabályozási törekvéseket az elmúlt években komolyabb európai, illetve ma már elmondható, hogy világszintű szabályozási rendszer követett, ami érinti elsősorban a közszolgálati információs rendszereket állami, valamint az ipari és a gazdasági rendszereket a nagyvállalati szférában. Az intézményeknek és szervezeteknek adaptálnia kell az elektronikus információkezeléssel összefüggő szabályozási rendszert a szervezet által megalkotott előírásokba és a gyakorlati alkalmazásokban egyaránt (elektronikus információ áramlása és védelme, GDPR). Az információbiztonsági szabványi (ISO/IEC 27001) ajánlás lényegében egy követelményrendszer az információbiztonsági irányítási rendszer kialakítására, bevezetésére, fenntartására illetve információbiztonsági tevékenység fejlesztésére.

Az ajánlás nemcsak azoknak szól, akik egy információbiztonsági irányítási rendszert szeretnének bevezetni, kialakítani, hanem útmutatóul szolgál az Európai Uniós (EU) és a magyar jogszabályok kialakításához is. A szabványi szakkifejezéseket átültették az EU-s irányelvekbe és a magyar jogszabályokba is.

4. Az információbiztonság, mint jogintézmény

Az információbiztonság napjaink egyik legösszetettebb és legfiatalabb jogintézménye, ókori eszmékkel a háttérben, modern információs technológiai és jogi vonatkozásokkal. Mint fogalom hosszú utat tett meg a mai formájáig és betöltött szerepéig. A jelenlegi előírásokat figyelembe véve az államigazgatási és közigazgatási szervek kötelezettek arra, hogy többek között az elektronikus információbiztonsági Ibtv. és az Infotv. előírásait együttesen alkalmazzák.

„A biztonság nem egy termék, hanem egy folyamat.” Sőt, a biztonság nem technológiai, hanem emberi és vezetési probléma. Az Ibtv. értelmében az elektronikus információs rendszer biztonsága az adott rendszer olyan állapota, amelyben a védelem zárt a rendszerben nyilvántartott és kezelt adatok, valamint a rendszerelemek bizalmasságára, sértetlenségére és rendelkezésre állására. A biztonságos rendszer minden elemével és információjával együttvéve a sértetlenség és a rendelkezésre állás szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. A rendszer zárt, amennyiben az elemzés során minden jelentős fenyegetést figyelembe vesz és kezel. Teljes körű, ha a rendszert alkotó összes elemére kiterjed és folyamatos, ha az időben változó körülmények ellenére is megszakítás nélkül működik és kiszolgálja a szükséges folyamatokat, kéréseket.

A rendszer kockázatarányos, amennyiben a feltehető kárérték és a kár valószínűségének szorzata nem haladhat meg egy előre megállapított és rögzített küszöbértéket. A küszöbérték minden esetben az üzleti döntés függvénye. A kockázatikezeléssel kapcsolatban nagyon fontos

tudatosítani, hogy nincs, és nem is létezik teljes mértékű biztonság, nemcsak az informatikában, de más területen sem, így a gazdaságban vagy az üzleti tevékenységben sem. A megállapított kockázati érték csak konvergál a teljes biztonsághoz, elérni sosem fogja, így a fennmaradó érték a maradványkockázat. A biztonsági szint növelhető a kockázatkezelés során meghozott szükséges intézkedések végrehajtásával. Az elért és az intézkedések végrehajtásával elérhető biztonsági szintet sok tényező befolyásol, de ezek közül is a legkiemelkedőbb az emberi tényező. Mint az élet más területein is általában, itt is a leggyengébb láncszem az ember.

Az információ ebben a kontextusban bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy új ismeret. Lényegét tekintve valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. Ez a fogalommeghatározás pontosítja és közelebb viszi az információs rendszerhez a latin eredetű meghatározást.

Az információbiztonsági szabványok és a vonatkozó rendelkezések szerint az elektronikus információs rendszert ért biztonsági esemény egy előre nem tervezett, nem kívánt olyan egyedi esemény vagy eseménysorozat, amely a rendszerben kedvezőtlen változást, kárt idéz elő, és amelynek hatására a rendszer által hordozott vagy nyilvántartott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása illetve rendelkezésre állása megsemmisül vagy sérül.

A biztonsági eseményt az adott katasztrófaelhárítási tervnek megfelelően kezelni kell, így szükséges az esemény dokumentálása, a következmények felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a jövőre vonatkozó hasonló események elkerülésének érdekében az intézkedések megfogalmazása és végrehajtása. További alkalmazandó meghatározások, jogintézmények a kibervédelem és a kiberbiztonság, amelyeket az adatvédelemhez és az adatbiztonsághoz megfelelő módon alkalmazhatunk.

A kiberbiztonság értelmében, a kibertérben, a kibernetikai virtuális térben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása,[17] amelyek a virtuális térben keletkező kockázatok elfogadható szintjét biztosítva a kiberteret elvárhatóan megbízható környezetté alakítják a társadalmi, gazdasági és kulturális folyamatok zavartalan működéséhez és üzemeltetéséhez. A kibervédelem az előbbi meghatározáshoz képest, a virtuális térből jelentkező fenyegetések elleni védelem, beleértve a saját kibertér képességeinek megőrzését is. Míg a kibervédelem a teljes információs rendszer védelmét érintheti, a logikai védelem az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított, programozott védelem. Az információbiztonsággal kapcsolatos legfőbb meghatározás itt is a bizalmasság, sértetlenség és a rendelkezésre állás.

Az információbiztonság a jelen kor egyik divatos kifejezése vagy jogintézménye, amelyet szokás összekötni az informatika világával, hiszen az információ az informatika egyik alapfogalma is. Ez a kényelmes megközelítés elfelejtteti velünk azt, hogy nemcsak az informatika szakterületén találkozhatunk információval. Attól függően, hogy milyen modellben, értelmezési szinten, valamint tudományágban használjuk, az információ más-más jelentéstartalommal bír, más-más aspektusa lehet releváns az adott kontextusban. Az információhoz társuló biztonság a dolgok olyan rendje, állapota, amelyben kellemetlen vagy negatív kimenetelű meglepetés szerű eseménynek, zavarnak, behatásnak, veszélynek nincs, vagy alig van bekövetkezési valószínűsége, lehetősége.

A jelen álláspontok értelmében az információ és a biztonság együttesen, az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai vagy más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Egy elektronikus információs rendszer biztonságán például olyan állapotot értünk, amelyben annak védelme a rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[18] Érdemes itt megjegyezni, hogy egy rendszer fogalmán szintén sokféle jelentést érthetünk, így lehet könyvek katalogizálása és elhelyezése a polcon, vagy tűzvédelmi rendszer, és nem minden esetben egy elektronikus információs rendszer.

A huszadik század második feléig az elektronikus rendszer fogalmának napi szintű használata nem létezett, de az információkutatás vagy információvédelem, különösen a katonai védelem területén igen. Az információbiztonság az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon

kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ebbe a témakörbe tartozhatnak. (MSZ ISO/IEC 27000:2014 szabványcsalád) Egy információbiztonsági rendszer kiépítése során ezen fogalmakra irányuló alapelvek teljesítése kötelező.

A bizalmasság alapelve, amely annak biztosítása, hogy az információ csak az arra felhatalmazottak számára legyen elérhető. Ha megfigyeljük akármelyik olyan történelmi momentumot, amely hadászati tartalommal rendelkezik, kiemelten fontos szerepet játszott a titkos információ eljuttatásának irányítása és legpontosabb végrehajtása, hiszen akár egy uralkodó státusza, vagy egy ország sorsa múlhatott ezen. A sértetlenség (integritás) alapelve, amely az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése. Téves információk téves döntéshez vezetnek, így a megoldások, a variációk halmaza is bővebb, ami zavart kelthet akármelyik rendszerben, legyen az stratégiai, gazdasági vagy katonai.

A rendelkezésre állás alapelve, amely annak biztosítása, hogy az érintett felek mindig hozzáférjenek az információkhoz és a kapcsolódó értékekhez akkor, és amikor az szükséges. Mindhárom alapelv elengedhetetlen tehát akár a napjaink információbiztonsági rendszerének kiépítéséhez.

Az alkalmazható intézkedéseket két nagy területre lehet bontani:

- Információvédelem (informatikai vonatkozásban): az informatikai, illetve az információs rendszerek adatvesztés elleni védelmét, az adatok folyamatos rendelkezésre állását biztosító szabályzatok, folyamatok és megoldások alkalmazásával.
- Információbiztonság: az informatikai, illetve információs rendszerek adataihoz való illetéktelen hozzáférést meggátló szabályozások, folyamatok és megoldások meghatározása és alkalmazása.

Az információbiztonsági intézkedések alatt adatok sérülése, megsemmisülése, jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttesét értjük. Információbiztonságot a gyakorlatban például a kontroll módszert alkalmazva, és egyes jelentős kérdések megválaszolásával lehet befolyásolni:

- Mit kell megvédeni?
- Mitől kell megvédeni?
- Hogyan kell megvédeni?

Amennyiben a fenti kérdésekre adott válasz ismert, a terület szabályozás alá vonható és megfelelő intézkedésekkel az adott terület információbiztonsági szintje erősíthető.

Összegzés

Az évszázadok során megszokott szabályok fejlesztéséhez ismerni és érteni kell történetüket, az elmúlt korok szokásait, szabályait és az információs társadalom új igényeit is. Az információtörténet kutatásának eredményei az információbiztonság szabályainak megalkotásához vagy igény szerinti megváltoztatásához elengedhetetlen. Az információ fogalma nagy utat tett meg az „ideák” világától az információelméletig, bár minden tudományágban jelen van, mégis legfőképp az információbiztonság, valamint az informatikai technológia bitorolja. Valószínű ennek oka, hogy az információelmélet[19] leginkább a számítástechnika, az informatikai hálózat tanulmányozásához kapcsolható.

Az információtörténet érdekessége, hogy az információ mai, informatikai vonatkozású fogalma igen fiatal, alig száz éves és a kapcsolódó információbiztonság jogintézménye is néhány évtizedes múltra tekinthet vissza. E tekintetben meglehetősen gyermekkorban lévő fogalommal és intézményrendszerrel találkozhatunk, szemben az ókori filozófiai, állam-, matematikai és orvostudomány elméletekkel szemben. Vajon a legifjabb tudományág meghatározásai felveszik a versenyt az őskövületi tudományágakkal? Véleményem szerint, mindenképp. Az a tény, hogy fiatalabb és kiforratlanabb, nem jelenti azt, hogy alkalmazásával hátráltatná vagy megakadályozná a többi tudományág fejlődését, épp ellenkezőleg. Fiatalságával és dinamikus fejlődésével pozitívan hat a többiekre, és a kommunikáció felgyorsításával, a biztonságosabb csatornák és információs rendszerek használatával biztos közeget teremthet a többi tudományág számára.

Irodalomjegyzék

[1] Shannon, C. E., A Mathematical Theory of Communication, The Bell System Technical Journal 379 – 423p, 1948, DOI: 10.1002/j.1538-7305.1948.tb01338.x, https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[2] Norbert Wiener: Cybernetics or Control and Communication in the Animal and the Machine, 1948

[3] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)

[4] Kiss Miklos, Muha, Lajos, The Cybersecurity Capability Aspects of Smart Government and Industry 4.0 Programmes, INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 1334-4684 1334-4676 16 (3) pp. 313-319 2018, DOI: 10.7906/indecs.16.3.2, https://doi.org/10.7906%2Findecs.16.3.2

[5] Xue-Shan Yan: Information Science: Its Past, Present and Future, Department of Information Management, Peking University, Beijing 100871, China, 2011, DOI:10.3390/info2030510, https://doi.org/10.3390/info2030510

[6] Manuel Castells: Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996, Az identitás hatalma, 1997, Az évezred vége, 1998

[7] Hendlein Teréz, Prazsák Gergő: A hálózati társadalom receptje, Gondolatok Manuel Castells „A hálózati társadalom kialakulása" című könyvéről, 2005.

[8] Daniel Bell: Az információs társadalom társas keretrendszere, Információ és távközlés a posztindusztriális társadalomban, Információs Társadalom, I. 3-33., Budapest, 2001. (fordította: Rédey Szilvia, Földvári Balázs)

[9] Daniel Bell: Az információs társadalom társas keretrendszere, Információ és távközlés a posztindusztriális társadalomban, Információs Társadalom, I. 16., Budapest, 2001. (fordította: Rédey Szilvia, Földvári Balázs)

[10] Manuel Castells: Az információ kora. Gazdaság, társadalom és kultúra, trilógia, A hálózati társadalom kialakulása, 1996, Az identitás hatalma, 1997, Az évezred vége, 1998

[11] International Telecommunication Union, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, letöltés: 2021. június 22.

[12] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve, Budapest, Verlag Dashöfer, 2000-2005.

[13] Gémes Csaba: Az információbiztonság alapkérdései, Hadmérnök (XII) IV, Budapest, 2017

[14] Herodotus, „The Histories", London, England: J.M. Dent & Sons, Ltd, 1992

[15] Muha Lajos: Informatikai biztonsági szabványok és irányelvek, GDF, Budapest, 2006.

[16] Muha Lajos – Szádeczky Tamás: Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014

[17] Tóth Georgina Nóra, Muha Lajos, Minőségirányítás és biztonság, FMTÜ XVII. Nemzetközi Tudományos Konferencia. (2012) pp. 339-342, DOI: 10.36243/fmtu-2012.087, https://doi.org/10.36243%2Ffmtu-2012.087

[18] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008 [In.: Bolyai Szemle, XVII. évf. 4. szám, p. 137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443]

[19] Shannon, C. E., Communication in the Presence of Noise, Proceedings of the IRE 10 - 21p, 1949, DOI: 10.1109/JRPROC.1949.232969], https://doi.org/10.1109/JRPROC.1949.232969