INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR) BEVEZETÉSI PROJEKT SIKERTÉNYEZŐI

SZABÓ ZSOLT MIHÁLY, ÓBUDAI EGYETEM, BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA, BUDAPEST, MAGYARORSZÁG, SZABO.ZSOLTMIHALY@UNI-OBUDA.HU

ABSZTRAKT

Napjainkban a projektmenedzsment a fejlett vállalati kultúra elengedhetetlen kiemelt része. A szervezetek kezdik felismerni, hogy projektmenedzsment nélkül nem lehet modern és gazdaságos szervezetet fenntartani, működtetni. A folyamatok pontos tervezése, kivitelezése, ellenőrzése és felülvizsgálata nélkül nem lehet bírni a gazdasági versenyt, pontosabban a szervezetek túlélésének egyik alapja projektmenedzsment. Nemzetközi nagyvállalatoknál és szervezeteknél már régóta nagyon fontos szerepet kapott a projekttervezés folyamata és a projektmenedzsment, hazánkban pedig egyesek igen felismerték ennek jelentőségét, jellemzően multinacionális vállalatok.
A legtöbb szervezet információs rendszerekre építi kritikus üzleti folyamatait. Ez a függőség elektronikus biztonsági fenyegetések formájában a kockázat egy új formájának megjelenéséhez vezetett, mint például a hackelés, adatvesztés, a titkosság megsértése vagy akár a terrorizmus. Az egyre kifinomultabb támadások érkezhetnek magánszemélyektől, magánvállalkozásoktól, vagy akár titkos külföldi hírszerző ügynökségektől is. Az ilyen támadások, amikor információk vesznek el, bizalmas adatokat lopnak el vagy kritikus rendszerek és dokumentumok sérülnek meg, kockázatot jelentenek a szervezet pénzügyeire, jó hírnevére is.
Az Információbiztonsági Irányítási Rendszer (IBIR) a vállalatirányítási rendszer azon része, amely átfogja és szabályozza a teljes informatikai tevékenységet, kiemelten kezelve az adatbiztonsági és adatvédelmi területeket. Segítségével a vállalat működésének kockázatelemzésén és kockázatkezelésén keresztül kialakítható a magas szintű információvédelem. A rendszer magában foglalja a szervezeti felépítést, a biztonságos működtetéshez szükséges szabályzatokat, a tervezési tevékenységeket, a felelősségi köröket, a gyakorlatot, az eljárásokat, a folyamatokat és az erőforrásokat.
Az előadás és a hozzá kapcsolódó tanulmány is konkrét példákon keresztül mutatja be a projektmenedzsment feladatokat egy IBIR bevezetési projekten keresztül. A különféle részterületeiből választott példák mindegyikére jellemző a projekt alapú tervezés és bevezetés, továbbá jól szemléltetik a projektmenedzsment alapú gondolkodást, persze figyelembe véve a helyi elvárásokat és kivételeket.

KULCSSZAVAK: *projektmenedzsment, információbiztonság, Információbiztonsági Irányítási Rendszer (IBIR) informatikai biztonság, információbiztonsági képzés*

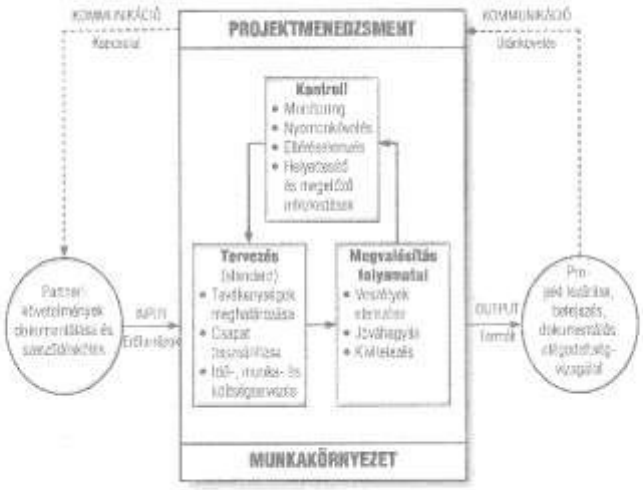
BEVEZETŐ

Informatikai (IT) projekt – eredményét tekintve – informatikai megoldások vagy információs rendszerek elemeinek kiválasztását, bevezetését vagy fejlesztését (esetleg továbbfejlesztését) valósítja meg a szervezet stratégiai céljainak megvalósítása érdekében (Michelberger, 2015).

1. A PROJEKTMENEDZSMENTRŐL ÁLTALÁBAN

1.1 Projekt

Egy projekt részfeladatok összességéből áll, egy folyamatot alkotva. A projekt olyan feladat, amelyhez világosan definiált cél, idő, költség és teljesítményértékek tartoznak. Az Nemzetközi Szabványügyi Szervezet (ISO) által kiadott szabványokban foglaltak alapján a projekt egy lehetséges definíciója: A projekt olyan egyedi folyamat, amely egyértelmű kezdési és befejezési dátumokkal megjelölt, specifikus követelményeknek – minőségi, erőforrás és költségkorlátoknak – megfelelő, egy adott célkitűzés érdekében vállalt, koordinált és kontrollált tevékenységek csoportja. Dolgozatomban a projekteket olyan időben behatárolt szervezeti feladatoknak tekintem, melyek méretük, bonyolultságuk, újdonságtartalmuk, vagy jelentőségük miatt a szervezet rutinszerű alaptevékenység ellátási megoldásaival valószínűleg nem oldhatóak meg hatékonyan. A fenti jellemzők arra késztetik a vezetőket, a feladatok keletkezése esetén ideiglenes szervezeti megoldással kezeljék a felmerülő problémákat, melyek kifejezetten a projekt sikeres végrehajtására koncentrálnak. Az 1. ábra alapján a projektmenedzsment a projekt tevékenységek vezetésével, szervezésével és irányításával foglalkozik.



1. ábra: A projekt rendszerösszetevői (Henczi-Murvai, 2012)

A projektmenedzsment az innovációs folyamat (maga a projekt) egészét átfogó és eredményességét segítő integrált vezetési irányítási rendszer, amely magában foglalja a projekt egész életciklusát, a problémafeltárástól a megvalósításig (Verzuh, 2006). A projektmenedzsment az erőforrások szervezésével és azok irányításával foglalkozó szakterület, melynek célja, hogy az erőforrások által végzett munka eredményeként egy adott idő- és költségkereten belül sikeresen teljesüljenek a projekt céljai (Lock, 2004). Napjainkban a projektmenedzsment egyéb szempontokat és feladatokat is figyelembe vesz pl. 10 PMI tudásterület, egyéb. Mivel a projektek nem ismétlődnek meg azonos feltételek között, így

megvalósításukra sem dolgozhatunk ki recepteket, csak eredménygyorsító hatékony technikákat. Ezek projekthez illesztése a projektmenedzsment kiemelten fontos feladata. A projektmenedzsment által átfogott projektek fontos ismérvei:

- a feladat egyszeri, nem ismétlődő (típusmegoldások nem alkalmazhatók)
- a feladat összetett, komplex (igényli az érintett szakterület munkájának összehangolását, koordinálását)
- a feladat egyértelműen azonosítható (célok, teljesítménykritériumok, idő, költség és erőforrásigények vonatkozásában)

1.2 Projekt szakaszai

A szervezetek számára a mindennapi működés mellett az egyik legnagyobb kihívás a projektek megfelelő előkészítése és lebonyolítása (Eszenyiné, 2014). Míg a normál üzleti folyamatok irányítását és végrehajtását hosszas gyakorlat során csiszolták, addig a projektek mindig egyediek, más és más célokkal, problémákkal, résztvevőkkel. Ennek megfelelően a projektek hatékony és sikeres lebonyolításához szilárd alapokon nyugvó és kipróbált módszertanra, valamint annak alkalmazásában jártas szakemberekre (projektvezetőre) van szükség (Verzuh, 2006). A projekteredmény a megvalósítási folyamat végterméke. A dolgozatomban a projekteket három szakaszra bontom.

1.2.1 Előkészítő (Tervezési) szakasz

Tervezés szakasz: célmeghatározás, helyzet és problémaelemzés, paraméterek felállítása (pénz, idő, személyi és tárgyi feltételek), a döntéshozatal módja és a szerepek meghatározása. Elsődleges célja a projekt időbeni megvalósulásának feltárása. Eredménye a megvalósítási ütemterv, amely alapvető funkcióit tekintve a megvalósításban résztvevő különféle közreműködők közötti kommunikációs és ösztönző eszköz, az ellenőrzés eszköze is, és mint ilyen alkalmasnak kell lennie a megvalósítás során bekövetkező változások kezelésére is. A projekttervezés módszertani vonatkozásainak legfontosabbika, hogy megtaláljuk a projekt karakteréhez leginkább illeszkedő (az optimális) tervezési formát.

2. ábra: Projekt szakaszok (Eszenyiné, 2014)

1.2.2 Kivitelezési (Végrehajtási) szakasz

A kivitelezés több mint felerészben az előkészítő munkán múlik. A kivitelezés akkor sikeres, ha a munkát az áttekinthetőség, a rugalmasság és a pontosság jellemzi. A projektmenedzser az

a személy, aki a projektet irányítja, annak teljesítéséért, de különösen a teljesítmény paraméterekért, a költségekért és a határidőkért egyszemélyi felelősséggel tartozik. A projektmenedzsment nem más, mint magának a projekt tevékenység megvalósítási folyamatának vezetése, irányítása, szervezése, az erőforrások, az információk, a rendelkezésre álló módszertani és technikai eszközök cél elérése érdekében történő összpontosítása. A projektmenedzsment feladatai lehetnek a cél folyamatos szem előtt tartása, a projekt dokumentálása, információgyűjtés és információadás, a munka koordinálása szervezése, a határidők és költségek folyamatos figyelemmel kísérése, engedélyek megszerzése, a döntés előkészítés és döntéshozatal biztosítása, a folyamat ellenőrzése, kapcsolattartás a partnerekkel, a team építése, a külső és belső visszajelzések figyelemmel kisérése, értékelése. A projektmenedzser döntési hatásköre minden esetben a vállalat felső vezetésétől származik. A projektmenedzser tényleges hatásköre nagymértékben függ a befolyásolási képességétől. Ezt a befolyásolási képességet több más tényező (szakmai képességek, helyzetfelismerés, tárgyalási készség) mellett jelentős mértékben alakítja a vezetői stílus. A vezetők a vezetői stílus alapján lehetnek feladat-orientáltak vagy humán-orientáltak. A projektmenedzsernek alkalmasnak kell lennie arra, hogy képes legyen egyensúlyt fenntartani a feladat orientáltság és a humán orientáltság között.

1.2.3 Lezáró (Értékelési) szakasz

A lezáró szakasz az utómunkálatok elvégzésén túl az értékelést jelenti. Ennek lényege az, hogy megtudjuk, hogy elértük-e a célunkat, mit gondolnak az elvégzett munkáról azok, akiknek szólt és azok, akik részt vettek benne. Az értékelésnél vizsgáljuk az elért eredményeket és az eléréséhez vezető folyamatot, olyan módon, hogy reális képet kapjunk az elvégzett munkáról, a sikerekről és a tévedésekről, annak érdekében, hogy levont a következtetéseket felhasználjuk következő munkánknál. A projekt kiértékelését és sikerét nem néhány specifikus mutatón keresztül, hanem folyamatában kell értelmeznünk és elvégeznünk. A projektmenedzsment a projekt sikerét három dimenzióban vizsgálja. Sikeres projekt az, amelyet: az eredeti ütemtervben, az eredeti költségvetésen belül, az eredeti szakmai követelményeknek megfelelő szinten valósítanak meg. Az utóelemzés célja annak megállapítása, hogy sikeres volt-e a projekt megvalósítása:

- a vevő számára akkor sikeres, ha projekt biztosítja számára a végső cél elérését;
- a vállalkozó számára a sikeres megvalósítás feltételei a teljesítési határidőben, költségeinek alakulásában, a műszaki és a teljesítményparaméterek elérésében keresendők.

Lényeges, hogy a sikeres megvalósítás általános feltételén túl a sikeresség konkrét kritériumai alapján is elemzésre kerüljön a folyamat.

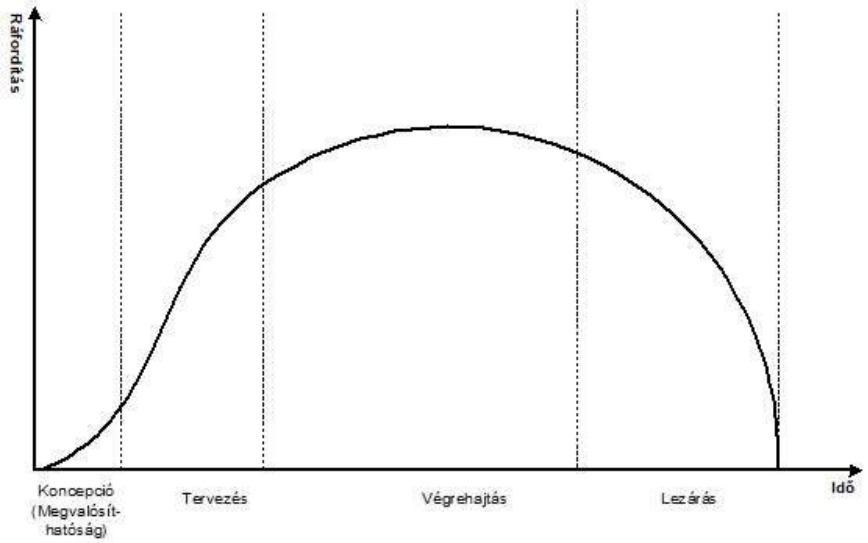
1.3 A projekt pénzügyi-gazdasági értékelése

Egy projekt megvalósítása többnyire jelentős mértékű tőkebefektetést igényel a vevő részéről és ez a befektetés csak később a projekt működése során térül meg. A vevő érdeke, hogy a projektbe invesztált tőkéje minél előbb megtérüljön, ezért olyan variációt választ, amelyik ennek az elvárásnak megfelel. A variációk közötti döntés, különböző pénzügyi-gazdasági technikákon is alapul (életciklus szerinti gazdasági elemzés, hatékonyságvizsgálatok, gazdasági elemzések, költség-hozam elemzése, költségeredményesség számítások, stb.). Mivel a projekt

többféle elvárásnak is eleget kell, hogy tegyen, magától érthető, hogy maga a választás többféle kritériumon alapszik.

1.3.1 Projekt életciklus szerinti elemzése

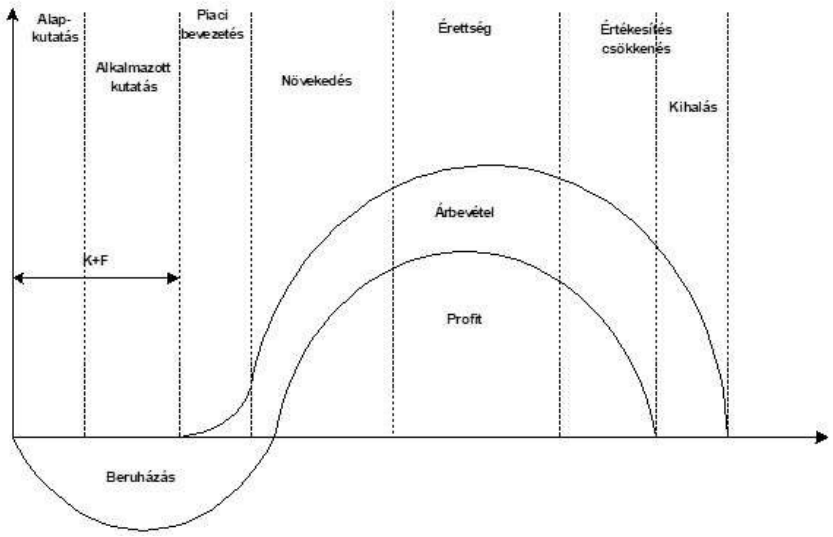
Általánosan a projekt kiindulópontja a koncepció, ötlet, amely egy megbízáshoz, vevői igény kielégítéséhez, esetleg önálló kezdeményezéshez fűződik. Zárópontja a széles körben értelmezett produktum, amely a projekt végrehajtása után létrejön, s mind a megbízó, mind a projektmenedzser számára gazdasági haszonnal jár. A legáltalánosabb projekt életciklus a termék életciklusához hasonlítható. Az 3. ábra vízszintes tengelyén a projekt időbeli lefutása, a fázisok láthatóak (idődimenzió). A függőleges tengely az egyes fázisok munkaráfordításával arányos (munkaóra, embernap, néha pénz), tehát a projektbe invesztált munka-mennyiséget mutatja.



3. ábra: A projektek életciklus fázisai (Daróczi, 2011)

1.3.2 Az életciklus elve szerinti gazdasági elemzések

A 4. ábra alapján a projektek elemzésének egyik fajtája a projekt végtermékének teljes életciklusára vonatkozik. Az elemzés alapfeltevése az, hogy a projekt végterméke a piacon értékesíthető, de elkészülte legalábbis számszerűsíthető eredményre vezet. A végrehajtás során jelentkező kiadásokat a piacon való értékesítés árbevétele ellensúlyozza. Ha a termék nem kerül értékesítésre, hanem pl. valamilyen megtakarítást lehetővé tévő technológiai fejlesztés, akkor a kiadásokkal szemben a megtakarított kiadások állnak. A gazdasági elemzés időtartama nem csak a projekt életciklusát, hanem a projekt végtermékének életciklusát is figyelembe veszi. A gazdasági elemzést tehát a projekt gyűrűződő hatásainak figyelembevételével végezzük.



4. ábra: Projekt életciklus elve szerinti gazdasági elemzése (Bucsy, 1976)

Az 4. ábrán jól látszik, hogyan viszonyul egymáshoz a projekt életciklus és a termékciklus. A nettó jelenérték mutató (NPV), a belső megtérülési ráta (IRR) vagy a jövedelmezőségi index segítségével történő gazdasági számítások a teljes termék-életciklusra végzendők (Csiszárik-Kocsir, 2018). Termékfejlesztési projektek esetében ezt az elvet kell követni. A nettó jelenérték megmutatja a projekt időtartama alatt keletkező pénzáramok (bevételek és kiadások, azaz hasznok és költségek) jelenre diszkontált értékét. Egy projektet gazdasági szempontból akkor érdemes megvalósítani, ha az NPV >0. Minél nagyobb az érték, annál kedvezőbb a projekt. A belső megtérülési ráta (IRR), az az r érték, ahol az NPV = 0. Az IRR megmutatja, hogy milyen belső megtérülése van egy projektnek, minél nagyobb ez az érték, annál kedvezőbb a projekt megítélése. Ez az érték közvetlenül összehasonlítható különböző méretű projektek esetén is, ahol a képződő NPV nagysága nem tükrözi az eredményességet. A jövedelmezőségi index a nettó jelenértéket veti össze a projektbe történt befektetések összegével. Egy projekt akkor javasolt megvalósításra, ha a jövedelmezőségi index nagyobb, mint 1. Egynél kisebb érték olyan projektnél adódik, amelynél a megtérülés kisebb, mint a befektetett összeg. Az elemzések másik fajta megközelítésében nem vesszük figyelembe a végtermék kihatásait, a teljes termék-életciklust, hanem az elemzést csak a projekt életciklusára végezzük el. Akkor végezzük el így az elemzést, ha a gyűrűző hatásokat nem tudjuk figyelembe venni. (Pl. szervezet-átalakítási projekt esetén)

Bizonyos esetekben nem kvantitatív, hanem kevésbé számszerűsíthető, kvalitatív megfontolások alapján kell dönteni. Ilyenkor olyan szempontokat is figyelembe kell venni, mint pl. stratégiai szempontok, jogi és adatvédelmi megfelelőség, biztonsági fejlesztések esetén a megtérülési számítások, vevőhöz való közelség, készség a vevővel való kommunikációra, reagálási sebesség stb. De a gazdasági elemzést ezen szempontok figyelembevétele mellett is el kell végezni (Csiszárik-Kocsir, 2018).

2. INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR)

Minden szervezet legalapvetőbb üzleti folyamatai az adatokra és az információra épülnek. Olyan kulcsfontosságú adatokról beszélhetünk, mint az ügyfelek és partnerek bizalmas adatai,

a különféle termékekkel, szolgáltatásokkal, megrendelésekkel és belső folyamatokkal, valamint számos egyéb, a cég know-how-jával összefüggő információk. Üzleti kockázatot jelent, ha bármilyen zavar keletkezik ezeknek az információknak a minőségével, mennyiségével, pontosságával vagy elérhetőségével kapcsolatban. A különböző fenyegetettségek származhatnak kívülről és a szervezeten belülről is, lehetnek véletlenszerűek vagy szándékosak. A védelmi rendszer hiányosságai révén az információ sérülhet, nyilvánosságra kerülhet, illetéktelenek férhetnek hozzá, vagy akár meg is semmisülhet. Mindezek alapján az adatok sértetlenségének, bizalmasságának és rendelkezésre állásának biztosítása, a sérülések és az adatvesztés elkerülése kritikus fontosságú feladat.

2.1 Szabályozott információbiztonság

Az Információbiztonsági Irányítási Rendszer (IBIR) az átfogó irányítási rendszernek (vállalatirányítási rendszernek) az a része, amely egy, a működési kockázatokat figyelembe vevő megközelítésen alapulva kialakítja, bevezeti, működteti, figyeli, átvizsgálja, fenntartja és fejleszti az információvédelmet. Az irányítási rendszer magában foglalja a szervezeti felépítést, a szabályzatot, a tervezési tevékenységeket, a felelősségi köröket, a gyakorlatot, az eljárásokat, a folyamatokat és az erőforrásokat. Napjainkban az információ biztonsága, a hivatalok, cégek és magánszemélyek adatainak védelme egyre inkább központi kérdéssé válik. Az adatok véletlen vagy szándékos kompromittálódása, sérülése, ellopása vagy rossz szándékú manipulálása komoly erkölcsi károkat okoz az érintett szereplőknek, elvesztik jó hírnevüket, megrendül a bizalom a szolgáltatásban. E mellett sokszor további, anyagi, kártérítési és büntetőjogi következményei is lehetnek az adatok helytelen kezelésének (pl. GDPR).
Az információbiztonsági rendszer lehetséges előnyei:

- az információ mindig rendelkezésre fog állni,
- az adatok sértetlenek maradnak,
- védett lesz a külső és belső fenyegetések ellen,
- a vezetőség tisztában lesz a kockázatokkal, és felkészült lesz az esetleges veszélyekre,
- a munkatársak elkötelezetté válnak az információbiztonság iránt és másként tekintenek majd a rendszer szerepére.

A bevezetett intézkedéseket általában két nagy területre lehet bontani:

- Adatvédelem: a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozásával, az érintett személyek védelmével foglalkozik. Ennek eszközei lehetnek jogi szabályok, eljárások, de akár technológiai eszközök is.
- Adatbiztonság: Az informatikai/információs rendszerek adataihoz való illetéktelen hozzáférést meggátló szabályozások, folyamatok és megoldások.

2.2 Szabályozott Információbiztonági Irányítási Rendszer (IBIR) tanúsítása

Az Információbiztonsági Irányítási Rendszer (IBIR) tanúsítható rendszer. A tanúsítás alapján az ISO/IEC EN 27001:2013 (magyar fordításban: MSZ ISO/IEC 27001:2014) szabvány alkotja. Az információbiztonsági irányítási rendszer szabványa hasonlóan a minőségirányítási rendszer szabványához az ISO/IEC EN 9001:2015 (magyar fordításban: MSZ ISO/IEC 9001:2015) egy szervezet vezetésének munkáját segítő menedzsment eszköz, és kockázat-értékelésen alapuló szabvány (Szádeczky, 2014). Megoldást mind az adott szervezet, mind

pedig partnereik szempontjából az információbiztonsággal kapcsolatos kockázatok és folyamatok hatékony menedzsmentje jelent. A cégek üzleti szempontból kritikus információi, informatikai rendszerei, valamint folyamatai biztonságának elősegítésére szolgál az ISO/IEC 27001 szabvány szerinti Információbiztonsági Irányítási Rendszer (IBIR) kiépítése és működtetése.

Az információbiztonsági irányítási rendszer alapja, hogy az információbiztonság szemszögéből a kockázatértékelésének módszerével felülvizsgálja a vállalat működési kockázatait, majd a számára túl nagy kockázatot jelentő területeken (megengedhető vagy elviselhető kockázati határ feletti) kockázatos esetén új biztonsági intézkedéseket vezet be. Végül mind a kockázatkezelés alkalmazását, mind a bevezetett védelmi intézkedéseket bevonja a vállalatirányítási rendszere működésébe, azaz menedzseli: működésüket megtervezi, ellenőrzötten működteti, folyamatosan figyeli eredményeiket és hatékonyságukat, majd dönt a javításról, fejlesztésről.

A kiindulási pont a vállalat tevékenységének, folyamatainak, kapcsolódó adatainak és adatbázisainak (információinak) átvilágítása során a védendő információk felmérése, majd azok alapján az ún. "információs vagyon" meghatározása. Az információs vagyon jelenti mind a védendő információkat, mind azokat az adathordozókat és eszközöket, ahol azok előfordulnak, illetve amelyeken keresztül azok hozzáférhetők. Ennek az információs vagyonnak a fenyegetettségeit méri fel a kockázatelemzés módszere, becsülve minden egyes lehetséges fenyegetettségre a bekövetkező kár nagyságát és annak bekövetkezési valószínűségét. Ily módon összevethető minden egyes fenyegetettség általi lehetséges káresemény információbiztonsági kockázata a vállalat működése számára. Ezek alapján - az elviselhető kockázati szint feletti kockázatok esetére - határoz meg a vállalat védelmi intézkedéseket. A kockázatkezelés alkalmazásának legfontosabb előnyei:

- A teljesség (minden "információs vagyontárgy") vizsgálata miatt nem maradhat ki gyengepont.
- Egyenszilárdságú védelem kialakítása.
- A védelmere fordított erőforrások leghatékonyabb felhasználása.

Az információbiztonsági irányítási rendszert kiépíteni szándékozó vállalatok nagy része nem rendelkezik a szükséges biztonsági elemekkel, illetve a meglévők nagyrészt alkalmatlanok a feladatuk ellátására. A kiépítendő rendszerelemek létrehozása - a rendszer összetettségénél fogva - egyszerre sok szakma ismeretét, tudását igényel(het)i (pl. őrzés védelem, személyi biztonság, informatikai védelem, folyamatok és eszközök védelme, katasztrófa-elhárítás, ...). Ezért is, valamint a kockázatelemzés szakszerű és érdemi lefolytatása miatt célszerű hozzáértő és (ezeken a területeken) tapasztalt tanácsadók segítségét igénybe venni. A rendszer kiépítésekor sokszor azok a tanácsadó vállalkozások tudnak érdemben és hatékonyan segíteni, amelyeknek az információbiztonság különböző területein már jelentős működtetési tapasztalataik vannak. Érdemes arra is odafigyelni, hogy - a minőségirányítási rendszerek felkészítésénél általánosan alkalmazott - "egy személy a felkészítő" modell itt általában nem hatékony, mert kevés az olyan tanácsadó, aki egyszemélyben mind az irányítási rendszerekhez, mind a bevezetendő eljárások mindegyik kapcsolódó szakmai területén egyidejűleg szakértő lenne.

3. AZ IBIR BEVEZETÉS PROJEKT SIKERTÉNYEZŐI

Az informatikai (IT) projekt végrehajtásához szükséges, de nem elégséges a hagyományos projekt eszközök és módszertanok használata pl. Projektmenedzsment útmutató (PMBOK® Guide). Sajátosságait többek között az ilyen típusú projektek összetettsége, bizonytalansága és sikertényezőinek nehéz mérhetősége adja. A Standish Group International Inc. vagy a Standish Group (http://standishgroup.com/) független, nemzetközi, 1985-ben alapított IT-tanácsadási cég, amely az információs rendszerek megvalósításának projektjeiről ismert a köz- és magánszektorban. A cég elsősorban a kritikus fontosságú szoftveralkalmazásokra összpontosít, különös tekintettel a hibákra és az IT-projektek lehetséges fejlesztéseire. A Standish Group 1994 óta méri az IT projektek sikerességét, ami számos témában íródott tanulmány, tankönyv, valamint módszertan ellenére sem változott meg jelentősen. Az előbb említett felmérés kritikával is illethető (Eveleens-Verhoef, 2010). Nem egyértelműen tisztázott, hogy mi tekinthető sikeres informatikai projektnek és a bekövetkező változások akár lehetnek előnyösek is. A nagyszámú globális megkérdezés alapján kapott, „sokkoló" adatokat azonban más globális felmérés hiányában nem lehet teljesen figyelmen kívül hagyni. Informatikai (IT) projekt - eredményét tekintve - informatikai megoldások vagy információs rendszerek elemeinek kiválasztását, bevezetését vagy fejlesztését (esetleg továbbfejlesztését) valósítja meg a szervezet stratégiai céljainak megvalósítása érdekében.
A projektháromszöget (ld. 6. sz. ábra) „vas háromszögnek” is szokták nevezni, illetve „hármas kötöttségnek” is. Lényege az, hogy nem lehet módosítani egy projekt költségvetését, ütemezését vagy hatókörét anélkül, hogy ez ne hatna legalább az egyikre a másik két rész közül.

MUNKAPROGRAM SZAKASZOK	HÓNAPOK											
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
1. Politika meghatározása	■											
2. Az információbiztonság irányítás területének és tárgyának meghatározása		■										
3. Kockázat felmérés			■									
4. Kockázat elemzés				■								
5. Kockázatok kezelése					■	■						
6. A szabályozási célok rögzítése és szabályozási dokumentumok (IBSZ) elkészítése és bevezetése							■	■	■			
7. Képzések és oktatások	■									■		
8. Rendszer próbaműködés										■	■	■
9. Audit, tanúsítás												→

5. ábra: IBIR kiépítésének lépései (KIB 25, 2008)

Az 5. ábra az Információbiztonsági Irányítási Rendszer (IBIR) kiépítésének a ptojekt szakaszait és lépéseit mutatja. A projekt során meg kell különböztetni bevezetési és fenntartási költségeket, mivel Információbiztonsági Irányítási Rendszer (IBIR) bevezetése után évenkénti felülvizsgálati tanúsítást kell kötelező jelleggel végeznie a szervezetnek, hasonlóan a bevezetés

során, melyek további ráfordítással jár. Jó esetben a bevezetési költségeknek csak töredéke a felülvizsgálati tanúsítások költségei, de mindenképpen tervezni szükséges velük.
A projekt mindig egyensúlyozás a projektháromszög csúcsai között. A három tényező az idő a költség és hatókör általában egymás ellen szoktak hatni. Minden projekt az idő, a pénz és a hatókör háromszögét igyekszik egyensúlyban tartani – nem lehet módosítani az egyiket anélkül, hogy legalább az egyiket ne kellene módosítani a másik kettő közül. A projektvezető dolga, hogy megóvja az egész háromszöget a széteséstől.

6. ábra: A projektháromszög (humansoft.hu, 2018)

A klasszikus projektmenedzsment a projektek sikerességét az ún. „vas háromszög" megvalósulásával méri (ráfordítás - átfutási idő – hatókör = „minőség"). IT projektek esetében azonban lényegesen több - többségében nehezen mérhető - sikertényezőt is figyelembe kell venni (Lock, 2004). A projektháromszög negyedik eleme a minőség: a középpontban van, a háromszög bármelyik oldalának módosítása befolyásolja. Egy nagyon fontos szempont: a minőségnek nincs egyetemes mércéje. A minőséget különböző szempont alapján pl. folyamati, stakeholderek, végtermék minősége, egyéb lehet meghatározni - minden projekt esetében magában a projektben kell meghatározni. Vannak vállalatok, ahol leginkább a költségkeret betartásával mérik a projekt minőségét. Mások számára fontosabb az időben való piacra hozatal. A projektvezetőnek tudnia kell, hogy mi minőség definíciója a szervezet és a konkrét projekt esetében.

7. ábra: A projekt sikertényezőinek kiterjesztett értelmezése (Deák, 2005)

A projektmenedzsment legfontosabb feladata, hogy a projektet sikerre vigye. Azonban a projektek menedzselése során sokszor a cég inkább a siker helyett a sikertelenséggel került szembe. Azonban manapság nem csupán a szokványostól eltérő projektekre jellemző a magas sikertelenségi arány. A projektsiker, mint fogalom elsődleges fontossággal bír a projektvezetés szempontjából, hiszen projektsiker nélkül a vállalatok nem tudják elérni stratégiai céljaikat vagy realizálni bevételeiket. Számos kutatás történt már a projektek sikerességét illetően, aminek során különböző megközelítések születtek. Kiemelendő, hogy a sikertelenség csak kevésbé magyarázható az erőforrások hiányával, hiszen manapság ezek már szinte korlátlanul elérhetőek a piacon . Sokkal fontosabb szerepet játszottak az olyan kvalitatívabb tényezők, mint például az elégtelen projektbehatárolás mértéke, vagy a projektvezetői tudás birtoklásának elégtelen volta (lásd pl. Standish Group jelentések). A projektmenedzsment hatékonysága részben azt mutatja meg, hogy a projekt mennyire érte el a kitűzött célokat, részben pedig azt, hogy mindezzel mennyiben járult hozzá a szervezet céljainak eléréséhez (Deák, 2005). Ahogy az 7. ábrán jól látható, a minőség - költség - idő háromszöggel a projekt eredményét vagyunk képesek mérni, ez azonban csak egy részét képezi a projekt siker értékelésének. Az átfogó méréshez ugyanis a stratégiával való összhang és az érdekcsoportok elégedettsége is hozzátartozik. A siker definiálása kapcsán a hármas peremfeltétel, avagy a projekt mágikus háromszöge a mai napig a legszélesebb körbe alkalmazott módszer a siker mérésére. De be kell látnunk, hogy a minőség fogalmának értelmezése sem egységes. A szakirodalom (Veress, 1999) szerint a minőség kapcsán két megközelítést különböztethetünk meg: az általános filozófiai értelmezést és az értékszemléletű filozófiai értelmezést. A pályázati projektek minőségi értelmezésének szempontjából szintén felfedezhető a definiált két kategória (Veress-Birher-Nyilas, 2005):

- egy projekt általános filozófiai értelmezéseként egy tevékenység vagy annak eredményei jól körülírhatók a különböző indikátorokkal és az adott programban előírt és elvárt, pályázat benyújtásakor tervezett outputokkal;
- az értékszemléletű filozófiai értelmezés alapján be kell látnunk, hogy a pályázati projektek elbírálására, éppen úgy, mint a végrehajtott projektek hasznosságának megítélésére, s ezért kaphat kiemelkedő szerepet valamennyi pályázati projekt kapcsán a különböző célcsoportok számára nyújtott hasznosság hangsúlyozása.

Az Információbiztonsági Irányítási Rendszer (IBIR) abban az esetben működik megfelelően, ha az abban foglaltakat sikeresen teljesíteni tudja, eléri kitűzött biztonsági célokat. Az Információbiztonsági Irányítási Rendszer (IBIR) és az információbiztonsági program elemeinek mérésére a leginkább a kritikus sikertényezők (CSF), a legfontosabb célmutató (KGI), és a kulcsfontosságú teljesítménymutatók (KPI) a legalkalmasabbak (Muha-Szádeczky, 2014). Ezek nyújtják a legpontosabb, és leginkább használható információkat a folyamat- és szolgáltatáscélok megvalósulásának nyomon követéséhez, illetve a kitűzött célok és mérföldkövek teljesítésének, elérésének ellenőrzéséhez. A megvalósítása során rendszeresen figyelemmel kell kísérni, monitorozni kell az Információbiztonsági Irányítási Rendszer (IBIR) működését és a célok megvalósulásának előrehaladását az előre definiált, szervezetre szabott mutatók segítségével. Az eredményeket riportok formájában rögzíteni kell, melyeket az érintett személyeknek kell eljuttatni, akik értékelik azok eredményét, összehasonlítják a tényértékeket az előre tervezett célértékekkel, és szükség esetén beavatkoznak az érintett folyamatokba annak biztosítása érdekében, hogy a célkitűzések teljesüljenek. Meg kell határozni azon

személyeknek, csoportoknak a körét, akik az érintett riport elkészítéséért felelősek, illetve akik a riportoláshoz adatot szolgáltatnak, valamint honnan, mely rendszerekből származnak a kinyert adatok.
A mérési adatok csak abban az esetben tekinthetőek eredetinek és hitelesnek, amennyiben az előre meghatározott forrásból, adatszolgáltatásért felelős személytől vagy szervezettől érkeznek. A riportok összeállításánál nagyon fontos annak ismerete, hogy az elkészített jelentést ki és hogyan fogja feldolgozni, mi a riportolás célja. Ennek érdekében meg kell határozni az egyes célcsoportokat, célközönséget, illetve azok információs igényét. Például az elmúlt hónap során bekövetkezett nem várt rendszer leállások teljes részletei, körülményei valószínűleg inkább csak az információbiztonsági vezető számára nyújtanak értékelhető és hasznos információkat, és a menedzsment számára mindebből inkább csak a költség vonzatú, üzleti folyamatokat érintő adatok lesznek relevánsak (Muha-Szádeczky, 2014). Azon túl, hogy meghatározásra kerül, hogy az egyes célcsoportok jelentései milyen információkat kell tartalmazzanak, ezek hatékony teljesítésének és megfelelőségének biztosításához ki kell jelölni, hogy az egyes célcsoportok részére ki készíti a riportokat. Ennek köszönhetően az előző példában az üzemeltetésről érkezett részletes riportokból az információbiztonsági vezető összeállíthat egy, a felső vezetés számára megfelelő és feldolgozható információtartalmú jelentést. A folyamatgazdák és erőforrásgazdák (üzemeltetők) számára szakterületi, információbiztonsági relevanciájú riportok, jelentések az általuk meghatározott tartalommal és formában saját munkatársaiktól kérhetőek. A felsővezetői döntéseket, meghatározott célokat az információbiztonsági vezető kommunikálja feléjük. A visszamérés, ellenőrzés célja, hogy a stratégiában foglaltak megvalósulásának státuszáról, illetve megfelelőségéről információt kapjunk.
A monitorozás során készült riportok, rendszeres jelentések, belső és külső auditok eredményei alapján lehet meghatározni, hogy a stratégiában foglalt célok és a mért értékek, megállapítások egyeznek-e, és amennyiben eltérés tapasztalható, mit és milyen irányban, mértékben kell fejleszteni, módosítani. Ezen információk képezik a felülvizsgálatok bemenő adatait, alapjait. Természetesen a visszamérés és monitorozás csak abban az esetben teljesíti a feladatát és éri el a célját, amennyiben az eredményei ténylegesen és megfelelően felhasználásra kerülnek, ezáltal valóban hozzájárul az információbiztonsági rendszer megfelelő működtetéséhez és hatékony megvalósításához.

ÖSSZEFOGLALÁS

A gazdasági és társadalmi élet egyik legfontosabb értéke az információ. Az információ a szervezetek számára erőforrás, hatékony működésük alapja, a szervezet vagyona és gyakran termék, áru is. Az információ biztonsága ritkán merül fel bennünk, mint probléma, pedig valójában mindennapjainkat behálózza az információk védelmében tett tevékenységek sorozata. Vannak folyamatok, amelyek kritikus helyzetbe hozhatják a szervezetet működését probléma esetén, ha nem megfelelően szabályozzuk azt, és nem készülünk fel hatékonyan egy esetleges katasztrófa elhárítására. Az informatikai biztonság átgondolt tervezése egyrészt meghatározza a rendelkezésre álló informatikai erőforrásokkal és befektetésekkel kapcsolatos főbb igényeket, másrészt megadja azt a keretet, amelyben a súlypontok és a megvalósításra vonatkozó felelősségek kijelölése, valamint az erőforrások kulcsterületekre való koncentrálása

történik. Kizárólag a részletes előzetes tervezés biztosítja, hogy az informatikában rejlő valamennyi lehetőséget kihasználhassuk a szervezet törekvéseinek és céljainak támogatására. A tervezés feladata biztosítani, hogy az alkalmazni kívánt megoldások az adott pénzügyi keretek közé illeszthetők, műszakilag megvalósíthatók, megfelelő kontroll alatt tarthatók és minden érintett számára értelmezhetők legyenek. Komplex informatikai biztonsági rendszer, mint az Információbiztonsági Irányítási Rendszer (IBIR) tervezésének és bevezetésének ma már elengedhetetlen feltétele a korszerű tervezési módszerek ismerete és alkalmazása. Mint a tanulmányból kiderül, nagyon sok szempontot kell figyelembe venni, hogy ezt a típusú munkát siker koronázza. Végezetül nem szabad elfelejteni, hogy az informatikai biztonság témájának nagysága és folyamatos fejlődése miatt, elengedhetetlen, hogy ismereteinket folyamatosan frissítsük és aktualizáljuk.

IRODALOMJEGYZÉK

Bucsy L. (1976): Az innovációk rendszere és a vállalati fejlődés. Közgazdasági és Jogi K Budapest, p31-41

Csiszárik-Kocsir Ágnes (2018): Vállalkozások pénzügyei, Óbudai Egyetem, Budapest, p1-192

Daróczi, M. (2011): Projektmenedzsment, Szent István Egyetem, p1-152

Deák, Cs. (2005): Projekt menedzsment képességek szervezeti szintű fejlesztése, ,,Tudásalapú társadalom Tudásteremtés - Tudástranszfer Értékrendváltás.” V. Nemzetközi konferencia, Miskolci Egyetem Gazdaságtudományi Kar. II. köt. Miskolc-Lillafüred 2005. május 11-12. p80-86

Eszenyiné Borbély Mária (2014): Projektmenedzsment a könyvtárban, Debreceni Egyetemi Kiadó, p1-95

Eveleens J. L., Verhoef, C. (2010): The Rise and Fall of the Chaos Report Figures. IEEE Software. Vol. 27. No.1, p30-36

Henczi, L., Murvai, L. (2012): Projekttervezés és projektmenedzsment, Saldo Kiadó, Budapest, p1-184

Lock, Dennis (2004): Projektmenedzsment, Panem Könyvkiadó Budapest, p1-236

Michelberger, P. (2015): Információtechnológiai projektek másképpen, HADMÉRNÖK 10:(1) p224-233

Muha L., Szádeczky, T. (2014): Irányítási rendszerek egyetemi jegyzet. Nemzeti Közszolgálati Egyetem, Budapest, p1-79

Szádeczky, T. (2014): Információbiztonsági szabványok egyetemi jegyzet. Nemzeti Közszolgálati Egyetem, Budapest, p1-50

Veress G. szerk. (1999): A minőségügy alapjai, Műszaki Könyvkiadó, Budapest. p1-281

Veress, G., Birher, N., Nyilas, M. (2005): A minőségbiztosítás filozófiája. JEL Könyvkiadó, Budapest, p1-281

Verzuh, E. (2006): Projektmenedzsment, HVG könyvek, Budapest, p1-424

Project Management Institute (2019): Project Management Institute. Projektmenedzsment útmutató 6. kiadás (PMBOK® Guide), Akadémia kiadó, Budapest, p1-678

KIB 25 (2008): KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR) 1.0 verzió 2008. június.

https://regi.ugyintezes.magyarorszag.hu/dokumentumok

(letöltés dátuma: 2020.11.08.)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

(letöltés dátuma: 2020.11.08.)

Standish Group International Inc. (1994): CHAOS MANIFESTO, p1-8

https://www.standishgroup.com/sample_research_files/chaos_report_1994.pdf

(letöltés dátuma: 2020.11.09.)

Standish Group International Inc. (2013): CHAOS MANIFESTO, p1-52

http://www.versionone.com/assets/img/files/CHAOSManifesto2013.pdf

(letöltés dátuma: 2020.11.10.)

Standish Group International Inc. (2014): CHAOS MANIFESTO, p1-16

https://www.projectsmart.co.uk/white-papers/chaos-report.pdf

(letöltés dátuma: 2020.11.11.)

CHAOS Report 2016: Outline. CHAOS Report 2016: The CHAOS Report: Decision Latency Theory: It's All About the Interval. (Note printed version in full color).
https://www.standishgroup.com/outline
(letöltés dátuma: 2020.11.12.)