NEMZETI
KÖZSZOLGÁLATI EGYETEM
Doktori Tanács

Gerevich János

Agilis szoftverfejlesztési technikák alkalmazási lehetőségei a Magyar Honvédség számára

című doktori (PhD) értekezésének szerzői ismertetője

Budapest

2020

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI DOKTORI ISKOLA

Gerevich János

Agilis szoftverfejlesztési technikák alkalmazási lehetőségei a Magyar Honvédség számára

című doktori (PhD) értekezésének szerzői ismertetője

Témavezető: Dr. habil. Négyesi Imre alez. PhD

Budapest

2020

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Napjaink információs társadalmában a katonai célú informatikai rendszerek jelentősége folyamatosan növekedik. Ezen rendszerek a potenciális haderő növeléséhez és a védelmi képességek fenntartásához egyaránt hozzájárulnak. Magyarország védelméért az Alaptörvény alapján a Magyar Honvédség felel, a feladat ellátásához magas színvonalú informatika rendszerek alkalmazása szükséges mind a stacioner[1] és a tábori rendszerek területén. A honvédelem megfelelő szintű megszervezéséhez elengedhetetlen a magas szinten támogatott elektronikus ügyintézés és a zavartalan külső kapcsolattartás. Ebből a tekintetből a Magyar Honvédség a közigazgatási szervekéhez hasonló ügyviteli folyamatokat valósít meg – szem előtt tartva a hierarchikus szervezeti felépítést és katonai parancs elvű működést. Az imént említett ügyviteli és iratkezelési folyamatok képezik a hivatalos információáramlás alapját a védelmi szektor vérkeringésén belül és kimenő irányba is. A közigazgatási szervekkel, egyéb jogi személyekkel, természetes személyekkel történő elektronikus kapcsolattartás túlnyomórészt már informatikai rendszerekkel támogatva, elektronikusan valósul meg. Jelentős súllyal bírnak azok a módszerek és technológiák, amelyekkel a védelmi szektor infokommunikációs rendszereit kialakítják, mert a kialakított rendszerek biztonsági és megbízhatósági mutatói napi szinten hatással vannak a társadalom átfogó biztonságára is.

Az elmúlt két évtizedben tapasztalható felhő alapú megoldások elterjedéséből kifolyólag a disszertáció kizárólag virtuális közegben, a kibertérben értelmezett szoftvertechnológiai problémákat tárgyal. A fizikai mérőszámokat, a hálózati és hardver környezethez köthető kérdéseket csak érintőlegesen vizsgálja a dolgozat – mindig az adott szoftverfejlesztési probléma megértéséhez szükséges mértékben.

Az értekezés kiindulási pontjának számítástudományi oldalról az agilis szoftverfejlesztési módszertanokat tekintettem, amelyeket a kutatásom megkezdésekor világszerte a szoftverfejlesztési tevékenységet folytató cégek 53%-a használt már. [2] A 2019-es statisztikai adatok szerint ez a szám már 97%-ra volt tehető.[3] A friss felmérésekből az is kiderül, hogy a szoftverfejlesztési tevékenységet folytató cégek negyede már több mint öt éve alkalmazza a vizsgált módszereket. Úgy gondolom, hogy az elmúlt négy év statisztikai adatai alapján az agilis szoftverfejlesztési módszertanok kiindulási alapnak tekintése helyes döntés volt a kutatás megkezdésekor. Az értekezésben vizsgált konkrét problémák a következő felsorolásban szerepelnek:

[1] Stacioner informatikai rendszer – jelentése: állandó felhasználású informatikai rendszer
[2] Az agilis szoftverfejlesztés elterjedését vizsgáló 2016-os nemzetközi felmérés adatai alapján
[3] A StateOfAgile.com amerikai weboldal által megismételt 2019-es felmérés adatai alapján

- Alkalmazhatók-e az agilis szoftverfejlesztési módszertanok a Magyar Honvédség számára?
- Milyen folyamatok és dokumentum sablonok szükségesek egy agilis szoftverfejlesztési projekt szabályozott végrehajtásához?
- Miben lehet más egy katonai célra agilisan készített egyedi szoftver, mint egy civil alkalmazás?
- Milyen tervezési minták, szoftver architektúrák merülhetnek fel egy agilis szoftverfejlesztési módszertan katonai célú alkalmazása során?

KUTATÁSI CÉLOK

A kutatás célja az imént vázolt probléma feltárása szoftvertechnológiai és védelemi szempontok szerint, ezt követően olyan szoftverfejlesztési módszerek és tervezési minták kialakítása, amelyek hasznosíthatók védelmi és általános célú infokommunikációs rendszerek fejlesztése során is. Ezen belül alapvető kutatási célom egy olyan hibrid, ugyanakkor agilis módszertan kialakítása, amely alkalmazható egy katonai szervezet és egy szoftvergyártó cég közös projektmunkájára a legjobb minőségű végeredmény elérése érdekében. Ebbe beletartozik a megfelelő szerepkörök és feladatok azonosítása a tervezési, fejlesztési, tesztelési időszakokban. Érdekes kutatási lehetőség a projekt szakaszaihoz a szükséges dokumentációkra vonatkozó követelmények meghatározása, milyen táblázatokra, sablonokra van szükség az egyes feladatok elvégzéséhez. Célom olyan egyedi technikák és módszerek kialakítása, amelyek segítségével a speciális katonai követelmények (sérülékenységvizsgálat, hibatűrés, számítási kapacitás kiesés, sávszélesség csökkenés, algoritmusok közötti váltás, stb..) a kezdetektől fogva beépíthetők a kifejlesztendő szoftverbe és ez által egy folyamatosan katonai célra fejlesztett rendszer állítható elő már az első lépésektől.

A kutatás további célja a kialakított módszertan alkalmazásakor létrejövő architekturális és szoftvertervezési minták azonosítása és feltárása. Olyan katonai informatikai rendszereknél, ahol a hierarchikus szervezet is része a modellnek, komoly problémákkal találkozhatnak az informatikusok. Az egyes szervezeti elemek felszámolása, áthelyezése kihatással lehet az addig kiadott parancsokra, határidőkre, folyamatokra, felelősökre, hatáskörökre, jogosultságokra, ezekben az esetekben nagyon fontos a jogutódok kiszámítása, modellezése, hogy a folytonosság fenntartható legyen az adott információs rendszeren belül. A modern technológia és a speciális követelmények szintéziséből új tervezési minták, megoldások születhetnek, amelyeket fel lehet használni létező rendszerek modernizálásakor vagy új

rendszerek kifejlesztésekor. Az alkalmazott agilis módszerekhez tartozó folyamatok feltárása és megértése után elkészíthetők és kialakíthatók azok a speciális szoftverre vonatkozó közbeszerzési eljárások és belső szabályozók, amelyek alapján a Magyar Honvédség is megfelelő képességekkel rendelkezhet egy agilis szoftverfejlesztési pályázat kiírására és megvalósítására.

KUTATÁSI HIPOTÉZISEK

- Az agilis szoftverfejlesztési módszertanok alkalmazhatók katonai célra a különböző katonai szakterületek speciális követelményeinek figyelembe vételével.
- Katonai alkalmazás során is azonosíthatók az agilisan végrehajtott projekt fázisai, amelyekhez kidolgozhatók a megfelelő dokumentációs sablonok.
- Egy agilis szoftverfejlesztési módszertan alkalmazása során rugalmasabb és a valóságot jobban modellező katonai célú szoftverek fejleszthetők ki.
- Új szoftvertervezési minták azonosíthatók egy katonai célra agilisan fejlesztett szoftver előállítása során, amelyek a későbbiekben széleskörűen alkalmazhatók.

KUTATÁSI STRATÉGIA ÉS MÓDSZEREK

Az agilis szoftverfejlesztés és a védelmi informatika külföldi és hazai szakirodalmának együttes feldolgozásával, valamint a több mint 15 éves személyes szoftverfejlesztési és tervezési tapasztalataimra támaszkodva egy olyan követelményrendszer kidolgozása a célom, amelynek kielégítéséhez a tipikus tervezési, fejlesztési, tesztelési problémákat széleskörűen fel lehet tárni. Az kutatás során valós problémákból levezetett, az átfogó vizsgálat számára leegyszerűsített, ugyanakkor elégséges példákat fogok vizsgálni a védelmi szempontok és az agilis szoftverfejlesztési irányelvek szem előtt tartásával. A kiválasztott példák az elektronikus ügyintézésből, a katonai iratkezelésből és egyéb védelmi informatikához köthető területekből kerülnek levezetésre, amelyeket eddigi szakmai tevékenységem során már átfogóan volt szerencsém megismerni. A kutatás során kizárólag nyilvános és mindenki számára elérhető irodalom kerül felhasználásra, úgy gondolom, hogy publikus információk alapján is teljes mértékben vizsgálható a probléma.

Kutatói tevékenységem alatt szem előtt fogom tartani a védelmi informatikai elvárásokat és az agilis szoftverfejlesztési elveket egyaránt. Eleinte deduktív módszerrel fogom az általánosan ismert védelmi, biztonsági, informatikai követelmények felhasználásával és

szoftverfejlesztésben elfogadott módszerek alapján kialakítani az alap problémát általános és speciális kutatási követelmények formájában.

A követelményrendszer alapját az Európai Unió közleményei és irányelvei, a NATO projektmenedzsment szabványai, Magyarország különböző biztonsági stratégiái, illetve a kutatáshoz kapcsolódó hatályos jogszabályai és a Magyar Honvédség informatikai követelményeket tartalmazó dokumentumai adják. A kutatás által vizsgált irodalom feltárása során általános informatikai, projektmenedzsment, tervezési, szoftverfejlesztési, szolgáltatási, üzemeltetési, biztonsági, megbízhatósági (minőségi) követelmények azonosítása a cél.

A kialakított szempontrendszer segítségével, érintve a szoftvertechnológiát és a védelmi informatikát, induktív módszerekkel kerül kialakítása a feltárt speciális követelményeket kielégítő szoftverfejlesztési módszertan, a *Military Scrum*. A módszertan részeként előállnak a folyamatleírások, dokumentációs technikák és dokumentum sablonok is, valamint a módszertan által megkívánt szoftverfejlesztési eljárások és üzemeltetési ajánlások is.

A módszertan meghatározását követően az elektronikus ügyintézéshez és a hierarchikus szervezetek folyamataihoz köthető példák segítségével olyan tervezési minták kialakítása a cél, amelyek megfelelnek a kor követelményeinek, valamint üzembiztosan, megbízhatóan és biztonságosan működő szolgáltatások alakíthatók ki felhasználásukkal.

A deduktív szakasz során feltárt kutatási követelményeknek való megfelelés két fázisban történik. A speciális kutatási követelményeknek való megfelelés végeredményei egy katonai célú alkalmazást lehetővé tevő szoftverfejlesztési módszertan és a katonai szervezetek működését támogató szoftvertervezési minták. A két egzakt eredmény segítségével a kutatási hipotézisek igazolása várhatóan megvalósul.

A kutatás során feltárt általános követelmények kielégítése a kutatási eredmények felhasználásával valósulhat meg – a kutatási hipotézisek igazolásán túl –, az eredmények alkalmazási lehetőségeinek bemutatásával.

ELSŐ FEJEZET ÖSSZEFOGLALÁSA

Az 1. fejezet feltáró munkája során áttekintésre került az Európai Uniós és a magyar kritikus infrastruktúra védelemhez köthető szabályozási keretrendszer, amelynek eredményeként az általános azonosítási, kijelölési, felülvizsgálati és nyilvántartásba vételi folyamatok tárgyalása is megtörtént. Végezetül, a Magyar Honvédségre vonatkozó ágazatilag kezelt kritikus infrastruktúra védelem kérdésköre is említésre került – kapcsolódási pontra lelve a létfontosságú rendszerek és a védelmi szektor működése között.

Ezt követően a létfontosságú infokommunikációs rendszerekre vonatkozó speciális szabályozás tárgyalása valósult meg a hálózat- és információbiztonság szemszögéből, amelynek eredményeként nyolc általános információbiztonsági kutatási követelmény azonosítása történt meg a felhő alapú szolgáltatás típusok átfogó tárgyalása mellett.
A fejezet záró szakaszában Magyarország különböző biztonsági stratégiáinak kiberbiztonsághoz köthető aspektusait vizsgálva további speciális és általános kutatási követelmények azonosítása valósult meg.

MÁSODIK FEJEZET ÖSSZEFOGLALÁSA

Az értekezés 2. fejezetében a Magyar Honvédség hatályos informatikai dokumentumainak szoftvertechnológiai perspektívából történő áttekintése valósult meg. Az elemző munkával párhuzamosan, az infokommunikációt érintő stratégiai célkitűzések áttekintése is megtörtént.
Az elemzés során négy általános módszertani elvárás került azonosításra az MH Informatikai Szabályzata alapján, majd az MH HID-ben helyet foglaló – szoftvertechnológiai szempontból is értelmezhető – tizenkét speciális informatikai követelmény elemzése következett, egyaránt szem előtt tartva az infokommunikációs rendszerek és a fejlesztési folyamatok perspektíváját. Befejezésképpen, a szabályozó dokumentumok átfogó vizsgálata után, öt speciális követelményelemzési igény megfogalmazása is lehetővé vált.

HARMADIK FEJEZET ÖSSZEFOGLALÁSA

A kutatás deduktív szakaszának végszavaként elmondható, hogy a NATO katonai képességfejlesztési módszertana – az SLCM – lefedi a katonai rendszerek teljes élettartamát, ehhez megfelelő modellt és folyamatokat biztosít. Az elemzés során láthattuk a szakaszokra bontott életciklust, valamint az egyes szakaszok hatókörét és feladatrendszerét. A kutatási célokhoz igazodva azonosításra kerültek a szoftvertechnológiai aspektusból értelmezhető módszertani, technológiai és dokumentációs követelmények.
A NATO SLCM irányelv elemzése során hét szoftvertechnológiai és három módszertani követelményt meghatározása történt meg. Az életciklus modellt bemutató NATO AAP-20-ban tizenkettő módszertani és három szoftverfejlesztésre értelmezhető dokumentációs elvárás definiálása valósult meg. Végezetül, a folyamatok áttekintése során egy lényeges AQAP szabványnak való megfelelésre vonatkozó módszertani, ezen túl két szoftvertechnológiai és hét dokumentációs követelmény is megfogalmazódott.

NEGYEDIK FEJEZET ÖSSZEFOGLALÁSA

A 4. fejezetben megismerhettük a jelenlegi szoftvertechnológia adta lehetőségeket, áttekintettük az agilis szoftverfejlesztés és a Scrum szoftverfejlesztési módszertan alapvetéseit. Ezt követően a Scrum elhelyezésre került a projekt menedzsment háromszögben, majd láthattuk, hogy a módszertan által elfoglalt hely megfelelő a kormányzati és ezen belül a honvédelmi ágazaton belüli alkalmazásra is.

Ezután, a Military Scrum szoftverfejlesztési módszertan szisztematikus meghatározása valósult meg a NATO SLCM folyamatok és a Scrum módszertan figyelembe vételével, feltételezve, hogy a kialakított módszertan elsődleges felhasználási területe a szoftver alapú szolgáltatások fejlesztése és támogatása, a munkához hozzájárultak a 2. fejezetben feltárt követelményelemzési (R) elvárások is. A fejezet során a Military Scrum által használt életciklus szakaszok, szerepkörök, feladatok és dokumentációs sablonok definiálása is megtörtént – támogatandó az alábbi tevékenységeket:

1) Igények felmérése – koncepcionális előtervezés;
2) követelményhalmazok kialakítása – koncepcionális előtervezés;
3) követelmények meghatározása – koncepcióalkotás;
4) átadás-átvételi tesztelési forgatókönyvek elkészítése – fejlesztés;
5) hibajegyek rögzítése – támogatás;
6) változtatási igények gyűjtése – felhasználás.

A fejlesztési szakasz támogatásához kijelölésre kerültek azok az agilis szoftverfejlesztési technikák, amelyek lehetővé teszik a szoftver alapú szolgáltatások előállításához szükséges telepítőkészletek megfelelőségének garantálását módszertani és technológiai oldalról is egyaránt: TDD, DDD, CI, stb.. A fejlesztést követő szakaszok támogatásához meg lettek határozva az üzemeltetési környezettel szemben támasztott folyamat szintű követelmények, valamint az integrált üzemeltetési platform (IÜP) fogalma is, amelyek együtt lehetővé teszik a megfelelő szintű üzemeltetési mutatók elérését. A módszerek meghatározása során szem előtt volt tartva a biztonsági követelményeknek és a nyomon követési infrastruktúrának való megfelelés is.

ÖTÖDIK FEJEZET ÖSSZEFOGLALÁSA

Az 5. fejezetben bemutatásra került a GDPR [7] hatóköre és az általános adatkezelési tevékenységekhez köthető fogalmak meghatározása is: érintett, személyes adat, adatkezelés, adatkezelő, adatfeldolgozó. Megtudhattuk, hogy a tagállamok felmentést kaptak a védelmi

szektorban a GDPR végrehajtására vonatkozóan – abból a meggondolásból kiindulva, hogy ebben a szektorban legalább a rendeletben foglalt, vagy annál szigorúbb szabályozások érvényesek.

Ezt követően az érintettek személyes adatainak és a hozzájuk kapcsolódó adatkezelési tevékenységek primitív modelljének vizsgálata következett a CRUD műveletek szemszögéből, amely rávilágított a primitív modell hiányosságaira az adatmódosítás és a fizikai törlés kapcsán is. A hiányosságok kiküszöbölésére a Proxy és a Holder tervezési minták tulajdonságait ötvözve meghatározásra került az ÉrintettHolder tervezési minta, amely megfelelő viselkedést mutat az érintetteken végrehajtott CRUD műveletek esetében – a párhuzamosan végzett adatkezelési tevékenységek esetén is.

Ugyan a GDPR terminológiájában az érintett fogalma természetes személyeket takar, ezzel együtt az ÉrintettHolder tervezési minta kiterjeszthető hierarchikus szervezetek modellezésére is az ÉrintettHolder-ből származtatott FelelősHolder és ÜgyfélHolder tervezési minták segítségével.

A tervezési minták működésének meghatározása ügyviteli példák segítségével valósult meg, ám azok felhasználása tetszőleges katonai szakterület számára is alternatívát jelenthet a hierarchia modellezésére és a szakterület specifikus folyamatok megvalósítására.

Ezután, a Magyar Honvédség ügyviteli folyamatainak bemutatása mellett – a vonatkozó hatályos jogszabályi követelmények értelmezésével – további tervezési minták kidolgozása valósult meg az elektronikus ügyintézési folyamatok támogatásához: a *Küldemény* tervezési minta és a belőle származó *BejövőKüldemény* és *KimenőKüldemény* formájában.

A fejezet záró részében a meghatározott tervezési minták felhasználási lehetőségeinek bemutatása történt meg az iratkezelési szoftverek jogszabályi szinten meghatározott folyamatainak támogatásához – ezzel betekintést nyújtva a dolgozat során azonosított tervezési minták speciális szakterületi alkalmazási lehetőségeihez.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Kutatásom megkezdésekor négy hipotézist állítottam fel, amelyek igazolásához előbb szoftvertechnológiai aspektusból elemeztem az Európai Unió és Magyarország kiberbiztonságot érintő szabályozási keretrendszerét. Majd ezt követően feltártam a szoftver alapú szolgáltatások fejlesztésének és üzemeltetésének kérdéskörét a NATO katonai képességfejlesztési módszertanának, valamint a Magyar Honvédség informatikai elvárásainak tükrében. A feltáró munka során nyolcvannégy különböző kutatási követelményt

azonosítottam és rendszereztem. Az azonosított követelményeket kiberbiztonsági, módszertani, szoftvertechnológiai, információbiztonsági, minőségbiztosítási és dokumentációs kategóriákba, illetve speciális és általános szintekre soroltam be.

A kialakított követelményrendszer hatvan speciális elvárással tette lehetővé számomra a kutatásom induktív szakaszának megkezdését, amelynek elsődleges célja az agilis szoftverfejlesztési technikák és a szabványos katonai képességfejlesztési módszerek szintetizálása volt. Az első két hipotézisem igazolásához célszerűnek láttam egy katonai célú szoftverfejlesztési módszertan meghatározását, amely hibrid megoldásként ötvözi a NATO SLCM folyamatokat és a Scrum agilis szoftverfejlesztési módszertant [8], valamint kielégíti a rá vonatkozó speciális követelményeket, a módszertanok közötti lényeges különbségeket az 1. táblázat mutatja be.

	Scrum	**NATO SLCM**	**Military Scrum**
Szerepkörök	ScrumMaster, Terméktulajdonos, Fejlesztőcsapat	Pontosan nem definiált, az ISO 15288 szabvány szervezeti folyamatain alapszik	Megrendelő, Projektmenedzser, Terméktulajdonos, Fejlesztő, Üzemeltető, Minőségbiztosító
Felhasználási terület	Szoftverfejlesztés	Általános katonai képességfejlesztés	Szoftver alapú szolgáltatások fejlesztése
Szakaszok/ lépések	Sprint tervezés, fejlesztés	Koncepcionális előtervezés, koncepcióalkotás, fejlesztés, előállítás, felhasználás, támogatás, leszerelés	Koncepcionális előtervezés, koncepcióalkotás, fejlesztés, üzembe helyezés, felhasználás, támogatás
Iterációk kezelése	egy szintű: fejlesztési sprintek	egy szintű: módosítási és frissítési eljárás	kétszintű: Military Scrum fejlesztési menetek, illetve a fejlesztés szakaszában fejlesztési sprintek.
Dokumentáció	Termék feladatlista (Story), fejlesztési feladatlista (Task), egyéb fejlesztés során keletkező tervezési, tesztelési dokumentum	A D-1, D-2, D-3 speciális kutatási követelmények tartalmazzák a szoftverfejlesztés vonatkozásában értelmezhető dokumentumokat.	Igények, követelményhalmazok, termék feladatlista, sprint feladatlista, átvételi tesztforgatókönyv, hibajegyzék, változtatási igények.

1. táblázat A Scrum, NATO SLCM és a Military Scrum módszerek összevetése (saját szerkesztés)

A Military Scrum szoftverfejlesztési módszertan meghatározása sikerrel járt, az előírt dokumentációk számát sikerült csökkenteni a modern technológiák javára, oly módon, hogy a módszertant a képességei továbbra is alkalmassá teszik a katonai célú felhasználásra a NATO követelmények alapján – az egyes követelményeknek való megfelelést az értekezés 2. számú melléklete tartalmazza, többek között az SLCM által előírt dokumentációs elvárásoknak való megfelelést is a Military Scrum alkalmazásakor. Így a kialakított módszertan a Magyar Honvédség számára is alternatívát jelent a katonai célú szoftver alapú szolgáltatások kialakításához.

A fennmaradó két hipotézis igazolásához a Magyar Honvédség által végzett ügyviteli folyamatokat és az elektronikus ügyintézés kérdéskörét vizsgáltam az alapvető adatkezelési (CRUD[4]) műveletek végrehajtásának szemszögéből. A műveletek elvégzését a hierarchikus struktúrát alkotó szervezeti elemeken értelmeztem, feltételezve az általuk párhuzamosan folytatott adatkezelési tevékenységeket a GDPR alapelveinek szem előtt tartása mellett: *célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg*.

A kutatás eredményeként általános tervezési mintákat alakítottam ki, amelyek támogatják a párhuzamosan végzett, a GDPR alapelveknek megfelelő adatkezelési folyamatokat a hierarchikus felépítésű szervezetek számára, így azok különböző katonai szakterületek számára is alkalmazhatók.

KUTATÁSI HIPOTÉZISEK VIZSGÁLATA

A NATO életciklus menedzsment folyamatainak, a Magyar Honvédség informatikai kérdésekben mérvadó dokumentumainak, valamint a magyar és az EU-s kibervédelmi stratégia alkotóelemeinek feltáró elemzésével 58 darab olyan speciális kutatási követelményt azonosítottam, amelyek alapján lehetővé vált az 1. és 2. számú kutatási hipotézisek vizsgálata. A Honvédelmi Minisztériumra és a Magyar Honvédségre vonatkozó hatályos jogszabályok, valamint az általános adatbiztonságot előirányzó GDPR rendelet, illetve a NIS direktíva korábbi elemzése során kialakított követelmények alapján vált lehetővé a 3. és 4. számú kutatási hipotézisek vizsgálata. A 2. számú mellékletben található (I-9) és (I-10) speciális információbiztonsági követelmények kielégítését a Military Scrum és a Holder tervezési minták együttes alkalmazása teszi lehetővé.

1. hipotézis: Az agilis szoftverfejlesztési módszertanok alkalmazhatók katonai célra a különböző védelmi szakterületek speciális követelményeinek figyelembe vételével.

A kutatás induktív szakasza során meghatározott Military Scrum szoftverfejlesztési módszertan agilis módszereket és technikákat használ fel a szoftverek és a szoftver alapú szolgáltatások fejlesztésének támogatásához, egyúttal megfelel az azonosított NATO és MH katonai elvárásoknak, így katonai célra alkalmazható. A módszertan által adott konkrét válaszok a kutatási követelményrendszerre az értekezés 2. számú mellékletében találhatók.

A kutatási eredmények alapján igazoltnak tekintem az 1. hipotézist.

[4] CRUD – az angol **C**reate, **R**ead, **U**pdate, **D**elete szavak kezdőbetűiből alkotott rövidítés. Jelentése: létrehozás, olvasás, módosítás, törlés.

2. hipotézis: Katonai alkalmazás során is azonosíthatók az agilisan végrehajtott projekt fázisai, amelyekhez kidolgozhatók a megfelelő dokumentációs sablonok.

A Military Scrum hat szakaszból álló iterációt határoz meg a teljes szoftverfejlesztési folyamat számára: koncepcionális előtervezés, koncepcióalkotás, fejlesztés, üzembe helyezés, felhasználás, támogatás. A módszertan a szoftverfejlesztési projektfolyamatok támogatásához projekt menedzsment sablont biztosít, amely hozzárendeli az egyes szakaszokhoz a megfelelő táblázatokat: igények, követelményhalmazok, termék feladatlista, sprint feladatlista, átvételi tesztforgatókönyv, hibajegyzék, változtatási igények.

A kutatási eredmények alapján igazoltnak tekintem a 2. hipotézist.

3. hipotézis: Egy agilis szoftverfejlesztési módszertan alkalmazása során rugalmasabb és a valóságot jobban modellező katonai célú szoftverek fejleszthetők ki.

A hierarchikus katonai szervezetek ügyviteli folyamataira támaszkodva, a természetes személyek és a szervezeti elemek adatain párhuzamosan végrehajtott CRUD műveletek vizsgálatával, rugalmas és valóságot tükröző tervezési minták kerültek kialakításra. A kialakított tervezési minták támogatják a fizikai törlés műveletét, a múltbéli és a naprakész adatok szeparált kezelését. Egyaránt alkalmazhatók a természetes személyek adataira és a katonai hierarchia részét képező egyéb entitásokra – a katonai célú felhasználás lehetőségét a Military Scrum által előírt módszertani és technológiai elvárások teremtik meg.

A kutatási eredmények alapján igazoltnak tekintem a 3. hipotézist.

4. Új szoftvertervezési minták azonosíthatók egy katonai célra agilisan fejlesztett szoftver előállítása során, amelyek a későbbiekben széleskörűen alkalmazhatók

Az *ÉrintettHolder*, az *ÜgyfélHolder*, a *FelelősHolder* és a *Küldemény* tervezési minták azonosítása a természetes személyeken és a szervezeti elemeken végzett CRUD műveletek elemzésével valósult meg a használati esetek tükrében. Az eljárás a Military Scrum szoftverfejlesztési módszertan során előírt TDD és DDD módszerekkel mutat analógiát. A CRUD műveletek leírásai képezik a tesztforgatókönyveket, a tervezési minták pedig a kialakított fogalomteret. Az eredményként létrejött modell univerzális, megfelelő szoftvertechnológia háttér mellett a kormányzat és a magánszektor is alkalmazhatja ügyintézési, kapcsolattartási folyamatok megvalósításához.

A kutatási eredmények alapján igazoltnak tekintem a 4. hipotézist.

ÚJ TUDOMÁNYOS EREDMÉNYEK

- Elsőként dolgoztam ki a védelmi fejlesztések szempontrendszerét figyelembe vevő, az általános kiberbiztonság fokozását elősegítő, a gyakorlati felhasználhatóságra is hangsúlyt fektető huszonnégy kritériumot.
- Kidolgoztam egy speciális NATO SLCM kompatibilis követelményrendszert a katonai célra alkalmazható szoftverfejlesztési módszertanok kiegészítésére.
- Meghatároztam a Military Scrum szoftverfejlesztési módszertant, amely megfelel a kutatás során kialakított követelményrendszernek.
- A GDPR alapelveknek megfelelő modellbe helyeztem a hierarchikus szervezetekben megvalósuló párhuzamos adatkezelési folyamatokat, majd ez alapján kidolgoztam egy katonai ügyviteli folyamatokon alapuló feladatrendszert.
- Meghatároztam az *ÜgyfélHolder*, a *FelelősHolder* és a *Küldemény* tervezési mintákat, amelyek támogatják a párhuzamosan megvalósuló adatkezelési folyamatokat és alkalmazhatók hierarchikus struktúrában működő szervezetek számára.

GYAKORLATI FELHASZNÁLHATÓSÁG

Az értekezés első felében feltárt huszonnégy általános kutatási követelmény legalább ugyanennyi gyakorlati felhasználási lehetőséget rejt magában. A továbbiakban a különböző kutatási területekről azonosított általános követelmények és a kutatás tudományos eredményeinek gyakorlati felhasználási lehetőségei következnek.

1. A különböző biztonsági komplexumhoz köthető információs rendszerek kialakítása során egyaránt törekedni kell a biztonságra, különös tekintettel a katonai biztonságra. A kutatási hipotézisek igazolása során kialakított Military Scrum szoftverfejlesztési módszertan segítségével olyan szoftver alapú szolgáltatások kialakítása válik lehetővé, amelyek teljes élettartamuk alatt egyenletes biztonsági és megbízhatósági mutatókkal rendelkeznek. A módszertan alkalmazható a katonai biztonsági komplexum információs rendszereinek kialakításához, hisz a szoftver alapú szolgáltatások fejlesztési folyamatainak NATO SLCM-ben való értelmezésével került kialakításra. A biztonsági elvárások már a koncepcionális előtervezés szakaszától integrálhatók a módszertannal megvalósított projektek követelményrendszerébe. A Military Scrum fejlesztést és üzemeltetés támogató eljárásai garantálják a biztonsági követelmények megvalósulását és azok későbbi fenntartását a rendszerek teljes élettartama alatt. Az eljárások alkalmazása nem csak a katonai biztonsági

komplexumon belül lehetséges, gazdasági és állami szereplők is egyaránt választhatják a szoftverfejlesztési projektjeik megvalósítása során.

2. Olyan infokommunikációs technológiák és módszerek kialakítása szükséges, amelyek biztosítják a megfelelő védekezési és reagálási képességeket. Ezen a területen a Military Scrum technológiát és módszereket ad a szolgáltatások tárgyát képező fejlesztett szoftverek tervezéséhez, fejlesztéséhez, üzemeltetéséhez, felhasználásához és támogatásához, értelmezve a biztonsági követelmények fogalmát is. A módszertan segítségével fejlesztett szoftverek a biztonsági követelmények integrált kezelésének köszönhetően a kezdetektől védekezési és reagálási képességekkel alakíthatók ki.

3. A számítógépes hálózatokat és a kapcsolódó információs rendszereket fel kell készíteni az összehangolt támadásokkal szemben. A felhőalapú szolgáltatási modell tetején elhelyezkedő szoftver alapú szolgáltatások esetében a Military Scrum alkalmazásával a biztonsági követelmények meghatározásától kezdve a fejlesztés, az üzembe helyezés és a támogatás részeként az automatizált rendszerfelügyelet képessége kialakítható a SaaS rétegben. Amennyiben különböző információs rendszereken belül azonos jellegű incidensek tapasztalhatók az automatizált rendszerfelügyelet által, akkor feltételezhető, hogy összehangolt támadásról van szó és életbe lehet léptetni az egységes kibervédelmi protokollokat.

4. Szoros együttműködést, hatékony információcserét biztosító infokommunikációs rendszerek kialakítása szükséges a védelmi ágazat szereplői számára. A FelelősHolder és a Küldemény szoftvertervezési minták alkalmazásával a hierarchikus felépítésű szervezeteken belül és a külső információcsere során a GDPR követelményeit kielégítő ügyintézési folyamatok és kétirányú kapcsolattartás valósítható meg. A kutatás során kialakított szoftverfejlesztési folyamatok és az azok alkalmazásán alapuló tervezési minták alternatívaként szolgálnak a jövőben a védelmi ágazat infokommunikációs rendszereinek kifejlesztéséhez és egymáshoz illesztéséhez.

5. Az informatikai rendszereknek olyan felügyeleti eszközökkel kell rendelkezniük, amelyek lehetővé teszik az észlelési, feldolgozási, és felderítési tevékenységek támogatását. A Military Scrum az első fejlesztési menetben előállított prototípusok esetében már lehetőséget biztosít arra, hogy az észlelési, feldolgozási és felderítési tevékenységek követelményei elvárásként

jelenjenek meg a fejlesztett szoftverrel szemben alap szinten. Ezt követően az integráltan végrehajtott fejlesztési, üzemeltetési és felhasználási szakaszokban a képességek fenntartása és növelése lehetséges. Az üzemeltetési környezet kritériumait folyamatosan figyelembe vevő fejlesztés lehetővé teszi, hogy a szoftver alapú szolgáltatás olyan információkat osszon meg az üzemeltetési környezet rendszerfelügyeleti szoftvereivel, amelyek alapján észlelhetők a szokatlan tevékenységek, azok technikai információi kinyerhetők és feldolgozhatók. Az okok, a külső és belső eredetű tényezők felderítése a feldolgozott információk alapján elvégezhetővé válnak.

6. Az ágazaton belül és ágazatok között is megfelelő módszerekkel kell támogatni a kockázatok kezelését. A kiberbiztonsági fenyegetések minden ágazatot érintő időközönként megismételt átfogó kockázatelemzésének támogatására alternatíva lehet a Military Scrum biztonsági követelményhalmazok finomítására szolgáló technikája. A technika alkalmazásakor a kockázatelemzési folyamat végére előállnak a minden ágazatot érintő kockázatkezelési elvárások – a létrejövő dokumentum egy biztonsági termék feladatlista. Az egyes ágazatokon belüli speciális kockázatkezelési eljárások kidolgozásához ez a dokumentum szolgálhat kiindulási alapként, amelynek finomításával az ágazatokon belüli speciális kockázatok feltárása és kezelése is megvalósulhat a technika újbóli alkalmazásával. Az eredmények együttes feldolgozásával ágazatokon átívelő integrált kockázatkezelési koncepció alakítható ki.

7. A kiberfenyegetésekre történő megfelelő reagálási eljárások kialakításához és támogatásához a kockázatelemzés és a kockázatkezelés számára megfelelő eszközrendszer biztosítása szükséges. Amennyiben a kiberfenyegetésekre történő reagálás informatikai rendszerek – szoftver alapú szolgáltatások – segítségével valósul meg, akkor a kockázatelemzés támogatásán túl a kockázatok kezelését megvalósító informatikai rendszerek előállítása is megvalósítható a Military Scrum szoftverfejlesztési módszertan segítségével. Ebben az esetben a módszertan képezi az eszközrendszert, amely segítségével a kockázatelemzéstől a működő reagálási eljárásokig el lehet jutni.

8. Gyors helyzetfelismerést, értékelést és kockázatelemzést támogató módszerek kialakítása szükséges. A szándékosan szoftver alapú szolgáltatásokkal szemben indított kibertámadások esetében, amikor nem az infrastruktúra működésképtelenné tétele a cél, nagy jelentőségűvé válik az adott informatikai rendszer önálló védekező képessége. A Military Scrum a

biztonsági követelményrendszer értelmezésével, a speciális biztonsági funkciók meghatározásával, majd azok beépítésével a fejlesztetett szoftverbe lehetővé teszi működő infrastruktúra esetén a kibertámadások gyors felismerését, azok jelzését. Amennyiben már rendelkezésre áll a felismert incidensek kezelésének módja, azok rendszeren belül, automatizáltan elvégezhetők. A tapasztalatok beépítését a biztonsági követelményrendszerbe a későbbi kockázatelemzések során a módszertan lehetővé teszi.

9. A megbízhatóságra tervezési és fejlesztési oldalról is törekedni kell. A Military Scrum módszertannal megvalósított szoftverfejlesztési projektek koncepcionális előkészítésekor a kiemelt megbízhatósági követelmények a megrendelő és a terméktulajdonos által beépíthetők a különböző követelményhalmazokba. Azok megvalósulásáról a módszertan további szakaszai gondoskodnak. Lényeges továbbá, hogy a módszertan által biztosított követelményelemzési technikák harmadik lépésében, a sprint tervezések során a termék feladatlista elemeinek elemzése és megvalósíthatóságra alkalmas feladatokká történő szétbontása zajlik. A folyamat során a követelmény jelentésével tisztában lévő – akár keletkezésének történetét is ismerő – szakértő (terméktulajdonos) beszélget egy megfelelő szaktudással rendelkező fejlesztőcsapattal, így a tervezés első lépése indukálja a funkcionális megbízhatóságot.

10. Felhő alapú üzemeltetési környezetben is megfelelő megbízhatósági és biztonsági paraméterekkel rendelkező szolgáltatásokat kell kialakítani. A felhőalapú üzemeltetési környezet feltételezi, hogy az adott szoftver alapú szolgáltatás infrastrukturális üzemeltetése harmadik fél által valósul meg. Olyan fejlesztési módszertanra van szükség, ahol a fejlesztett szoftver képességeit egyértelműen el lehet különíteni az üzemeltetési környezettől. Így lehetővé válik az üzemeltetési környezettel és a fejlesztett szoftverrel szemben támasztott megbízhatósági és biztonsági paraméterek szeparált kezelése. A Military Scrum szoftverfejlesztési módszertan elkülöníti a fejlesztési és üzembe helyezési szakaszokat, így lehetővé válik a fejlesztett szoftverrel szemben támasztott megbízhatósági és biztonsági követelmények ellenőrzése az üzembe helyezés előtt. Ha az üzembe helyezés egy felhőszolgáltatásba történő telepítést jelent, akkor az előfeltételek ellenőrzése és a tesztelés ezt követően megvalósítható az üzemeltetési környezet biztonságát és megbízhatóságát illetően.

11. Magas szintű biztonságot és megbízhatóságot garantáló szabványok kialakítása és alkalmazása a cél. Szoftvertechnológiai oldalról a Military Scrum lehetővé teszi a szoftverek,

különös tekintettel a szoftver alapú szolgáltatások magas szintű biztonságot és megbízhatóságot garantáló előállítását. A módszertan alapját képezheti a követelményben szereplő szoftvertechnológiai szabványok kialakításának.

12. A biztonsági események detektálása, a logikai hibák feltárása, javítása szabványos eljárásokkal és módszerekkel történjen. A Military Scrum alkalmazásával saját vagy harmadik fél által biztosított üzemeltetési környezetben is egyaránt kialakíthatók azok az automatizált rendszerfelügyeleti megoldások, amelyek képesek detektálni a szoftver alapú szolgáltatás vonatkozásában a már ismert, releváns biztonsági eseményeket. A szolgáltatás működésében tapasztalható hibák monitorozása az eljárás segítségével ugyancsak megvalósítható. A begyűjtött információk alapján a következő fejlesztési menetben az igazolt logikai hibák javítása és az azonosított biztonsági események kezelésének képessége szabályozott eljárásokkal megvalósítható a fejlesztett szoftveren belül.

13. Szabályozott módszerek és folyamatok segítségével történjen a biztonsági tervek előállítása. A Military Scrum fejlesztési meneteiben az első két szakaszban a külön kezelhető a biztonsági követelményrendszer és az azokból levezethető biztonsági feladatok.

1. kockázatelemzés → biztonsági követelményhalmazok meghatározása
2. kockázatkezelés → biztonsági követelmények és reagálás meghatározása (a termék feladatlista részét is képezheti)
3. eszközrendszer → automatizált tesztelés, szakterület specifikus eszközök (a fejlesztett szoftvert érintő incidenskezelési képességek kialakítása)

14. Megfelelő tájékoztatás mellett kezelhetők, detektálhatók, bejelenthetők legyenek a biztonsági események. Amennyiben széles körben kerülne felhasználásra a Military Scrum szoftverfejlesztési módszertan és az üzemeltetési környezetekkel szemben támasztott követelmények szabványként lennének előírva, akkor kialakítható lenne a következő bejelentési modell. Az egyes incidens típusokhoz tartozó megfelelő egyezményes incidenskódok kialakításával – hasonlóan a HTTP hibakódokhoz –a létfontosságú rendszerek esetében lehetővé válna a központi incidensgyűjtés. Így az alapvető szoftver alapú szolgáltatásokat érintő kibertámadások központi kezelése és bejelentése is lehetségessé válna.

15. Biztonsági szempontok kezelésére alkalmas, folyamatos működést garantáló tervezési módszerekre van szükség. A Military Scrum fejlesztési meneteiben lehetőség van a

biztonsági szempontok felülvizsgálatára és azok kiegészítésére a kiberbiztonsági tapasztalatok alapján. Amennyiben egy újabb fenyegetés jelenik meg a kibertérben, akkor a koncepcionális szakaszokban kielemezhető annak szoftveres szinten történő kezelése. Amennyiben a felmerült fenyegetések ellen kialakíthatók a fejlesztett szoftveren belüli reagálási eljárások, akkor azok fejlesztése megvalósítható a fejlesztési szakaszon belül, így garantálva az ismert kockázatok tükrében a folyamatos működési képességet.

16. A megfelelő reagálási képesség elősegítéséhez olyan rendszerfelügyeleti megoldások kialakítása szükséges, amelyek azonnal jelzik az alapvető szolgáltatásokban bekövetkező változásokat, figyelmeztetnek a potenciális biztonsági eseményekre. A digitális infrastruktúra felügyelete, a különböző kibertámadások elleni védekezés Európai Uniós és kormányzati szinten is megvalósul. Ha egy Military Scrum módszertan segítségével fejlesztett szoftver alapvető szolgáltatásként kerülne besorolásra, akkor az üzemeltetési környezettel és a fejlesztett szoftverrel szemben támasztott rendszerfelügyeleti követelmények integrált kezelése biztosított lenne. A módszertan lehetővé teszi a fejlesztett szoftveren belüli megbízható reagálási képességek kialakítását az evolúciós szoftverfejlesztési technika segítségével. A fejlesztett szoftver által jelzett incidensek becsatornázhatók az üzemeltetési környezet rendszerfelügyeleti szoftverébe, így a szoftveres szinten detektált incidensek is láthatóvá válhatnak az infrastrukturális és hálózati biztonsági események mellett.

17. Elengedhetetlen a gyors változáskezelési képesség megléte az informatikai rendszerek teljes életciklusa alatt. Egy változtatási igényről a megfelelő szintű szakértői támogatás segítségével gyorsan eldönthető, hogy a megvalósításához elegendő-e az aktuális rendszerkoncepció vagy esetleg annak bővítése, módosítása szükséges. Utóbbi eset ritkának számít egy üzembe helyezett szoftver alapú szolgáltatás esetén. A Military Scrum helyes alkalmazásakor megvalósul az evolúciós szoftverfejlesztés technikája, így a követelmények változtatásának hatásait a tesztfuttató infrastruktúra rövid időn belül képes visszajelezni. Ezt követően már csak a rendszer konzisztenciájának visszaállítása a feladat az új követelmények tükrében. A változtatások kiadhatók a soron következő szoftvertelepítő csomag előállításakor, majd üzembe helyezhetők a Military Scrum által meghatározott automatizált üzembe helyezési eljárásokkal.

18. Az új rendszerek fejlesztése során fenntartható, folyamatosan frissíthető műszaki alapok kialakítása szükséges. A Military Scrum helyes alkalmazása a fejlesztett szoftver esetében azt

jelenti, hogy a rendszer működése automatizált tesztek formájában is dokumentált. Ez a megközelítés lehetővé teszi, hogy amennyiben a szoftver alapú szolgáltatás valamelyik komponense frissítésre szorul, akkor a frissítés kis kockázattal elvégezhető, mert az evolúciós szoftverfejlesztés technikája lehetővé teszi az új komponens és a rendszer konzisztenciájának kiértékelését. A módszertan által meghatározott üzembe helyezési folyamatok visszajelzést adnak a komponens működéséről az éles üzembe helyezés előtt, de már az üzemeltetési környezeten belül.

19. Az újonnan kialakított informatikai rendszerek esetén a biztonsági követelmények folyamatos ellenőrzése képezze részét a fejlesztési folyamatnak. Az evolúciós szoftverfejlesztés technikája nem tesz különbséget a műszaki, a funkcionális és a biztonsági követelmények között. Ha Military Scrum követelményhalmazai megfelelően tartalmazzák a fejlesztett szoftverrel szemben támasztott biztonsági elvárásokat, akkor azok kiértékelése folyamatos a rendszer teljes élettartama alatt a fejlesztési szakaszokban.

20. Kritikus rendszerek esetében a biztonsági követelmények ellenőrzése, a sérülékenységvizsgálat szektor függetlenül képezze részét a rendszerfejlesztéseknek. A követelmény megvalósításához természetesen törvényi szabályozás is szükséges. A Military Scrum lehetőséget biztosít a sérülékenységvizsgálat automatizált beépítésére az evolúciós szoftverfejlesztési technika alkalmazása során. Az üzembe helyezés átadási fázisában a migrációs környezetre történő telepítéskor a tesztek ismételt elvégzésével az üzemeltetési környezetben is meg lehet győződni a helyes konfigurációról és működésről a sérülékenységek vonatkozásában. Így kettős védelemmel rendelkezhetnek a módszertannal fejlesztett szoftver alapú szolgáltatások.

21. A szolgáltatások minimális erőforrás és idő ráfordításával legyenek átalakíthatók, adaptálhatók a változó felhasználói igényeknek és alkalmazási körülményeknek megfelelően. A módszertani követelmény teljesítése akkor lehetséges, ha az adott szoftver alapú szolgáltatás számára szükséges működést lehetővé tévő rendszerek érettségi szintje eléri a megfelelő szintet – a NATO SLCM Rendszer Koncepciójához igazodva. A megfelelően alkalmazott Military Scrum biztosítja a hatékony feladatvégzést és a gyors átfutási időt a felhasználói igények megvalósításakor. Az üzemeltetési környezetben bekövetkező változásokra való felkészülés gyorsan és hatékonyan valósítható meg a módszertan fejlesztési és üzembe helyezési szakaszai során.

22. Az infokommunikációs szolgáltatások fejlesztése és biztosítása az alkalmazó szervezetek műveleti követelményei, az infokommunikációért felelős szervezetek szakmai követelményei, a beszerzés műszaki követelményei, a kialakításra kerülő rendszer rendszerterve, az alkalmazó szervezet alkalmazási terve, valamint a tevékenységet szabályozó jogszabályok, okmányok intézkedések alapján valósuljon meg. A Military Scrum követelményrendszer meghatározási módszerei lehetővé teszik a felsorolásban szereplő igények összegyűjtését és felelősökhöz rendelését. Ezt követően a követelményelemzési eljárás első két lépésében a követelményhalmazok és a termék feladatlista előállítása során a különböző szintű szervezeti elemek elvárásai beilleszthetők a követelményrendszerbe. Az iteratív finomítás folyamat segítségével a követelményrendszerben mutatkozó anomáliák feloldhatók. Az átadás előtti fejlesztési sprintek során a funkcionális követelményrendszer, a fejlesztett szoftver dokumentációja és az alkalmazási terv finomíthatók.

23. Az infokommunikációs szolgáltatások biztosítását, tervezését, fejlesztését, felügyeletét támogató, a szolgáltatás teljes életciklusára értelmezhető szoftverfejlesztési módszertan kialakítása a cél. A NATO SLCM-re épülő szoftver alapú szolgáltatások tervezését, fejlesztését, üzemeltetését támogató Military Scrum módszertan megfelel a kutatási követelménynek.

24. A fejlesztési javaslatok elemzését, majd szabályozott módon történő változtatási igények meghatározását támogató módszertan kialakítása szükséges. A Military Scrum módszertan minden fejlesztési menet során előírja a változtatási igények elemzését a koncepcionális előtervezés és a koncepcióalkotás szakaszában is. A folyamat szabályozott módon történik az 1. fejlesztési menetben, az átadási előtti időszakban és az átadott rendszer esetében is.

AJÁNLÁSOK

1. Javasolom a Military Scrum szoftverfejlesztési módszertan beépítését a magyar védelmi ágazat informatikai fejlesztéseket szabályozó dokumentumaiba és folyamataiba, ezzel átláthatóságot és átjárhatóságot teremtve a megrendelői és beszállítói folyamatok között.
2. A Military Scrum által meghatározott fejlesztési és üzemeltetési előírások bevezetését javasolom a létfontosságú infokommunikációs rendszerek szoftvereket érintő fejlesztési és üzemeltetési folyamataiba.

3. További kutatásra ajánlom a speciális szoftvertechnológiai (S) követelmények (hatékonyság, rugalmasság, telepíthetőség, stb.) mérési eljárásainak integrálási lehetőségeit a Military Scrum által alkalmazott evolúciós szoftverfejlesztési környezetbe.
4. Ajánlom minden hierarchikus szervezeti felépítést modellező, párhuzamosan végrehajtott adatkezelési folyamatokat megvalósító informatikai rendszerben az *ÜgyfélHolder*, a *FelelősHolder* és a *Küldemény* tervezési minták alkalmazását, beleértve a kormányzati és nagyvállalati felhasználást is.
5. Szorgalmazom az iratkezelési szoftverek fejlesztésével foglalkozó szakemberek számára, hogy a jogszabályi követelményekben meghatározott fogalmak modellezésekor alkalmazzák az értekezésben meghatározott tervezési mintákat.

A DOKTORJELÖLT TÉMÁVAL KAPCSOLATOS PUBLIKÁCIÓS JEGYZÉKE

[1] GEREVICH J.: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. In: Hadmérnök XII. 1. (2017) 170-181. o.

[2] GEREVICH J.: Híradó-Informatikai fejlesztést támogató agilis dokumentációs módszerek. In: Hadmérnök XII. 3. (2017) 210-222. o.

[3] GEREVICH J., NÉGYESI I.: Híradó-Informatikai fejlesztést támogató agilis dokumentációs módszerek - 2. rész. In: Hadmérnök XIII. 1. (2018) 230-244. o.

[4] GEREVICH J., NÉGYESI I.: A Military Scrum követelményelemző módszerének alkalmazása létfontosságú rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 3. (2018) 293-304. o.

[5] GEREVICH J., NÉGYESI I.: A Military Scrum szoftverfejlesztési módszertan alkalmazása létfontosságú infokommunikációs rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 4. (2018) 72-82. o.

[6] GEREVICH J., NÉGYESI I.: A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere - 1. rész In: Hadmérnök XIV. 2. (2019) 281-292. o.

[7] GEREVICH J.: Software Technological Interpretation of the NATO Military Capability Improvement Process. In: AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT IV. Évfolyam 3. szám (2019) 28-35. o.

[8] GEREVICH J., NÉGYESI I.: A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere - 2. rész In: Hadmérnök XIV. 4. (2019) 75-89. o.

[9] GEREVICH J., NÉGYESI I.: Network and Information Security of Cloud Computing Services. In: Hadtudományi Szemle XIII. 1. (2020)

A DOKTORJELÖLT SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Név: Gerevich János

Születési idő: 1984. 05. 07.

E-mail cím: gerevich.janos@agilexpert.hu

Munkahelyek

Évszám	Beosztás	Munkahely
2013–	ügyvezető	AgileXpert Szoftverfejlesztő és Tanácsadó Kft.
2016 2015	IT tanácsadó vezető szoftverfejlesztő	HM EI Zrt. Informatikai Igazgatóság
2012–2013 2010–2011 2009–2010	fejlesztési vezető vezető szoftverfejlesztő szoftverfejlesztő	Synergon Rendszerintegrátor Kft.
2008-2009 2007	junior szoftverfejlesztő gyakornok	Synergon Informatika Nyrt.

Egyetemi tanulmányok

Évszám	Kutatási terület / Szak	Intézmény
2016–	védelmi informatika és kommunikáció elmélete (PhD)	NKE HDI
2002–2008	programtervező matematikus (MSc)	ELTE TTK, IK

Tudományos és oktatói tevékenység

Évszám	Tevékenység	Intézmény / Helyszín
2018	Előadás: Emeltszintű informatikai szolgáltatások a kibertérben	Kommunikáció 2018 Tudományos Konferencia
2017	Előadás: Agilis szoftverfejlesztési módszerek és alkalmazásuk a robottechnikában.	Robothadviselés 2017 Tudományos Konferencia
2016–	11 publikáció, elérés az MTMT felületéről: https://m2.mtmt.hu/gui2/?type=authors&mode=browse&sel=10073524	NKE HDI
2014–2015	Programozási tantárgyak oktatása megbízott külső előadóként.	NKE HHK Informatikai Tanszék

Idegennyelv-ismeret

Angol: középfok (C), BME Nyelvvizsgaközpont (2016)

Ukrán: felsőfok (C), Külföldön szerzett érettségi bizonyítvány (2002)