

futurIT
Integrated Security
Research & Development Centre



2007

Éves jelentés
2007 futurIT



Pázmány Péter program



Nemzeti Kutatási és Technológiai Hivatal

A projekt a Nemzeti Kutatási és Technológiai Hivatal támogatásával valósult meg.

futurIT
„Informatikai Biztonsági
Kutató-Fejlesztő Központ”



Tartalomjegyzék

Vezetői összefoglaló	1	III. Informatikai biztonsági minősítés és eszközfejlesztés	29
Küldetésnyilatkozat	3	1. Informatikai megoldások biztonsági minősítése	30
Szervezeti felépítés	4	2. Informatikai biztonsági eszközök fejlesztése	31
Menedzsment működés	5	IV. Informatikai biztonsági képzési rendszer kiépítése	32
Konzorcium bemutatása	6	1. Informatikai biztonsági doktori képzés és kutatás	33
Tevékenységünk	8	2. Informatikai biztonságtechnikai képzés	
Kutatási programjaink	11	beindítása mérnöki mesterszak (MSc) keretében	34
Nemzeti és iparági információbiztonsági rendszerek kidolgozása	12	3. Az informatikai biztonság fontosságának kommunikációja és társadalmi tudatosítása, hazai szakmai színvonalának emelése	36
Szervezeti és humán biztonsági kutatások	13	Indikátorok	37
Adatmentés-technológia kutatás	14	PhD disszertációk	38
Tudásmenedzsment program	15	PhD, posztdoktori, egyetemi kutatói állások	39
Eredményeink	17	Hallgatói együttműködés program	40
Beszámolási időszak feladatai	18	A futurIT által támogatott	
Eredményeink összefoglalása	19	24 órás programozási verseny	41
I. Projekt előkészítés	20	Felnőttképzés	42
1. Infrastruktúra előkészítése	21	Technológiai transzfer	43
2. Kutatás-fejlesztéshez szükséges eszközök beszerzése	22	Konferenciák	44
3. Szervezet kialakítása	23	Erőforrások időráfordítása	46
4. Pénzügyi rendszer kialakítása	23	Teljesítmény indikátorok	47
II. Informatikai biztonsági megoldások	24	Média szereplések	48
1. Informatikai megoldások biztonsági tervezési és minősítési módszertanának kialakítása	25	Szakmai rendezvények	52
2. Nemzeti informatikai biztonsági szabályozási rendszer kidolgozása	27	Finanszírozás, összesített pénzügyi mutatók	53
3. Informatikai fenyegetettség és kockázatok felmérése, elemzése és kezelése	28	Monitoring adatszolgáltatás	55
		Elérhetőségek	56
		Ilyenek vagyunk	56

Vezetői összefoglaló



Értékvédő módszereket, eszközöket kutatunk, fejlesztünk, oktatunk információs értékeink megóvása érdekében.

A Pannon Egyetem informatikai biztonság témakörben két területen

nyert támogatást a Nemzeti Kutatási és Technológiai Hivaltól 2006-ban. A futurIT Informatikai Biztonsági Tudásközpont vezetője Kürti Tamás.

Az ÖkoRET Környezetbiztonsági Informatika Tudásközpont alapítója Prof. Dr. Rédey Ákos, vezetője Prof. Dr. Marton Gyula.

A Tudásközpont igazgatója Prof. Dr. Friedler Ferenc a Pannon Egyetem Műszaki Informatikai Karának alapítója és dékánja. Jelen beszámoló a futurIT munkáját mutatja be. A konzorcium tagjai az Albacomp Zrt. a KÜRT Zrt. és a Pannon Egyetem.

A konzorcium tagjai közös értékek, célok mentén hozták létre együttműködésüket. Céljuk, hogy meghatározóak legyenek saját területükön, legyen szó tudományról, üzletről vagy innovációról.

Mindhárom partner felelősségteljes, tudatos és szakmailag kiemelkedő munkatársakat alkalmaz a projekt feladataiban, akik proaktívan képesek a csapatmunkára.

Együttműködésük már a futurIT megalapítása előtt kezdődött, több sikeres projektet teljesítettek, stratégiai partnernek tekintik egymást. A tudásközpontban megkövetelt szoros együttműködéshez több szervezeti-kulturális kihívásnak kellett megfelelni, mint

például az eltérő probléma-megoldási folyamatok és munkajelleg összehangolása, valamint a bizalom kiépítése minden szervezeti szinten és közreműködőben az öt körülvevők iránt. Éppen ezért az első munkaszakasz egyik legfontosabb eredménye, hogy olyan menedzsment modellt építettünk, amely segítségével hosszútávra megalapoztuk a szervezet hatékony munkavégzését.

A konzorcium az operatív munkát a Kutatási Munkabizottság irányításával végzi. Feladata a munkafolyamatok, időközi eredmények egyeztetése, a szakmai tájékoztatás, illetve a szakszerű és tudományos munka elősegítése. A Kutatási Munkabizottság tagjai szükség szerint, de legalább kéthetente üléseznek.

A tudásközpont operatív céljainak és stratégiájának teljesülését a konzorciumi tagok képviselőiből álló Projekt Bizottság felügyeli, mely jogosult a munkák eredményeinek értékelésére és hasznosításáról szóló döntések meghozatalára is. A szakmai munka a kutatási témák szerinti témalaboratóriumokban történik. A Projekt Bizottság az alábbi laboratóriumok elindítását hagyta eddig jóvá:

1.) Nemzeti és iparági információbiztonsági rendszerek kidolgozása

Kutatás-fejlesztési programunk célja, hogy a tudományterület és az iparág legújabb elméleti eredményeinek és gyakorlati tapasztalatainak felhasználásával a különböző specifikus szakterületekre, iparágakra vonatkozó, testre szabott információbiztonsági eljárásokat, módszertanokat és eszközöket dolgozzunk ki, illetve gyakorlati hasznosításuk megvalósítását támogassuk.



2.) Szervezeti és humán biztonsági kutatások

Programunk célja, hogy módszertant fejlesszen ki a humán (és szervezeti) erőforrások informatika, információ kezelési kockázatainak elemzésére, a fenti tényezőkből származó kockázatok értékelésére, valamint hogy ezek rendszerbe foglalásával megbízható, automatizált előrejelzési, illetve riasztási lehetőségeket dolgozzon ki.

3.) Adattárolás-adatmentés

Az adathordozók és adattárolási logikák exponenciális ütemű fejlődése nagy mértékben növeli az adatvesztések kockázatát. Programunk e kockázatok csökkentése érdekében kiemelt partnerként dolgozik együtt a hazai adatmentési iparág létrehozójával, a KÜRT-tel.

A program célja nem csak az, hogy a meglévő eszközök mentési problémáit oldja meg, a jövő adathordozóiban rejlő adattárolási kockázatokat is kutatja.

4.) Tudásmenedzsment

A Tudásmenedzsment program a futurIT horizontális tevékenysége, amely a projektek keretében megvalósított kutatási programok szakmai eredményeinek összefogását és a létrehozott „best practice” ismeretek publikálását végzi. A Tudásmenedzsment program erősíti a futurIT szakmai megalapozottságát és elismertségét az akadémiai és üzleti életben, ezzel járul hozzá a projekt alapvető céljainak eléréséhez.

Ha további információra van szüksége munkánkkal kapcsolatban örömmel állunk rendelkezésre.

Veszprém, 2007. szeptember 30.

Prof. Dr. Friedler Ferenc

igazgató

Pannon Regionális

Tudásközpont

Kürti Tamás

vezető

futurIT Informatikai

Biztonsági Tudásközpont

küldetés

Küldetésnyilatkozat

A futurIT Informatikai Biztonsági Kutató-Fejlesztő Központ (a továbbiakban: futurIT) a tudományterület vezető elméleti és gyakorlati szakembereinek kiemelkedő szintű képzésével, szakmai tapasztalataik hasznosításával a Közép-Dunántúli Régió, Magyarország, és Közép-Európa vezető informatikai biztonsági kutató- és képzési központjává kíván válni. Fejlesztéseinek végtermékei világszínvonalú informatikai biztonsági eljárások, módszertanok és eszközök.

A Pannon Egyetem (a továbbiakban: PE) Műszaki Informatikai Kara (MIK), valamint a KÜRT Zrt. (KÜRT) és az ALBACOMP Zrt. (ALBACOMP) által közösen létrehozott futurIT Regionális Tudásközponttá válásával a közép-európai régióban egyedülálló módon elismert, színvonalában a világ élvonalába tartozó felsőfokú képzést nyújt magyarországi és külföldi informatikai biztonsági szakemberek számára, ugyanakkor a legújabb technikai és társadalmi változásokat szorosan követve folytat informatikai biztonsági kutatásokat, fejlesztéseket.

A futurIT szoros kapcsolatban áll a fejlesztésekben, illetve a kutatási eredmények hasznosításában együttműködő régióbeli vállalkozásokkal, valamint a kutatási és felsőfokú képzési programban nemzetközi partnerként résztvevő oktatási intézményekkel.

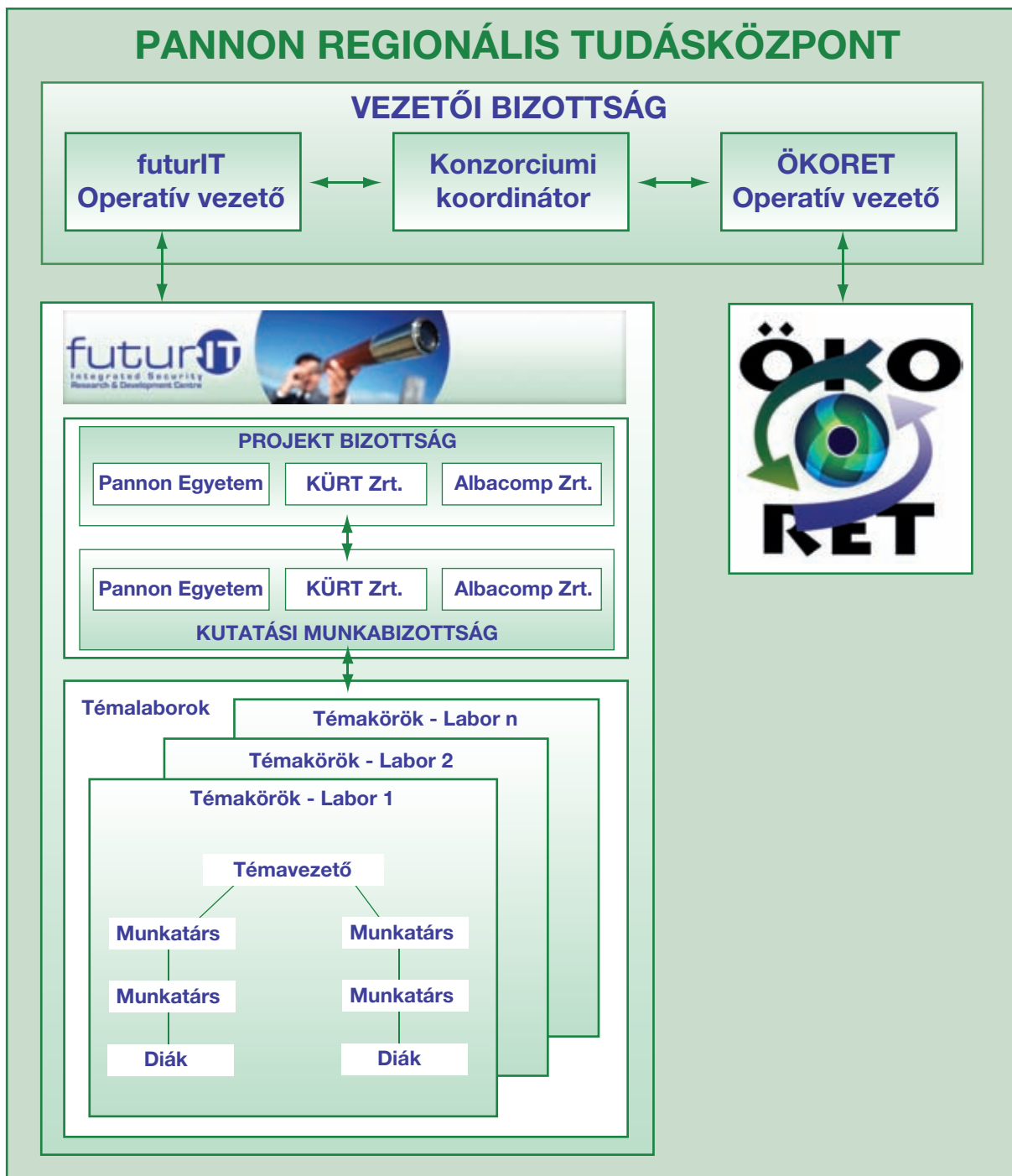
A futurIT tevékenysége az alapkutatástól egészen a spin-off cégekben realizált termékértékesítésig terjed. Mindezek mellett az informatikai biztonság nemzetközi tudásbázisa és konferenciaközpontja.

A futurIT hozzájárul a régió belüli innováció, kutatás-fejlesztési kapacitás növeléséhez, a szakképzésen keresztül helyi tudásintenzív kis- és középvállalatok számára teremt munkaerőt, illetve spin-off vállalkozások és a konzorciumi tagok saját K+F tevékenysége révén a képzett munkaerő számára megfelelő munkalehetőséget.

A futurIT oktatási és képzési programja lehetővé teszi a Pannon Egyetem Műszaki Informatika szakos hallgatóinak a műszaki informatika tartósan fontos területén élvonalbeli ismeretek megszerzését, valamint kutatási témát biztosít PhD hallgatók számára. Az alap- és alkalmazott kutatások eredményeit nemzetközi tudományos szakmai publikációk és konferenciák mellett a termékeik és a külföldi hallgatók képzésén keresztül valósítja meg.

futurIT
„Informatikai Biztonsági
Kutató-Fejlesztő Központ”

Szervezeti felépítés



Menedzsment működés



A futuriT Kutató-Fejlesztő Központ a Pannon Egyetem Műszaki Informatikai Karának elkülönített gazdálkodású, rész-jogkörrel rendelkező költségvetési egységeként működik.

A futuriT legfőbb döntéshozó szerve a Projekt Bizottság (PB), amely a projektben részt vevő tagok összességéből áll. A PB feladata a futuriT működési feltételeinek megteremtése, a szükséges infrastruktúra és a szervezet kialakítása a projekt-feladatok ütemezésének megfelelően. A PB végzi a költségterv és a határidők betartásának ellenőrzését, a beszerzéseknek a vonatkozó jogszabályokhoz való megfelelésének biztosítását, valamint az ezekhez kapcsolódó változtatások végrehajtását, illetve engedélyezését. A PB a futuriT vezetői számára rendszeresen készít jelentéseket a szervezet és a projekt belső működéséről, a belső szabályozásoknak való megfelelés ellenőrzéséről, valamint a feltárt működési illetve irányítási problémákról. Nagy hangsúlyt helyezünk rá, hogy a PB ne csak feltárja a működéssel, irányítással kapcsolatos hiányosságokat, hanem megfelelő megoldási javaslatokat is dolgozzon ki azok megszüntetésére.

A futuriT operatív irányító szerve a Kutatási Munkabizottság (KMB), amelyet a tagok által delegált képviselők alkotnak. A KMB feladata a futuriT kutatói laboratóriumaiban zajló alap- és alkalmazott kutatásokhoz kapcsolódó szakmai feladatok végrehajtásának irányítása, a kutatási és fejlesztési célok megvalósítása,



a munkafolyamatok megvitatása, az eredmények egyeztetése, a szakszerű tudományos munka elősegítése, illetve a futuriT keretében működő képzési programok kidolgozásának, működésének felügyelete.

A futuriT Operatív vezetőjének feladata a Projekt Bizottság által kijelölt stratégiai célok és kutatás-fejlesztési programok végrehajtása a rendelkezésre álló erőforrások felhasználásával. Az Operatív vezető egy személyben fogja össze a futuriT napi szintű tevékenységeit, feladatait. Ő felel továbbá a kutatási és fejlesztési programok eredményeinek gyakorlati hasznosításáért, és a hasznosítással kapcsolatos együttműködések kialakításáért, felügyeletéért.

A futuriT vezetői a stratégiai döntések megvitatása és a szakmai irányvonalak kijelölése kapcsán - elsősorban konzultatív jelleggel - rendszeresen egyeztetnek az informatikai biztonság területén elismert magyar és nemzetközi szaktekinetékkel, egyetemi oktatókkal és hasonló területen működő vállalkozások képviselőivel, akik szakmai állásfoglalásokkal, tanácsokkal, elemzésekkel segítik a döntések előkészítését, megalapozását.

Konzorcium bemutatása



Pannon Egyetem Műszaki Informatikai Kar

A Műszaki Informatika Szak 1991-ben indult először a Veszprémi Egyetemen, akkor még a Mérnöki Karon. 2003-tól a Műszaki Informatikai Karon folyik a képzés. A kar rugalmas "Department" rendszerben működik, ahol a kutatás a tanszékektől

függetlenül, nemzetközi elismerést szerzett professorok irányításával létrejött nyitott tudományos műhelyekben zajlik. A kutató laboratóriumok és a DSc minősítésű professorok tizenkilenc fős kara két doktori iskola megalapítását is lehetővé tette, például a PE MIK professzori laboratóriumai a Bio-Nanorendszerek Laboratórium, a Hálózatoptimalizálási Laboratórium, a CNN Alkalmazásai Laboratórium, a Nanoszenzorika és a Távközlési Laboratórium. Az oktatásszervezési feladatok ellátásáért a tanszékek felelősek. A kar a mérnök informatikus képzésnek valamennyi felsőfokú formáját biztosítja. A hallgatói létszám a 2006/2007-es tanévben meghaladta a kétezer főt. A kar a professzionális fejlesztési tevékenység végrehajtására külön szervezeti egységeket hozott létre, mint például az Informatikai Biztonsági - és az Orvosi Informatikai Kutató-Fejlesztő Központ. A kar szoros kapcsolatban áll számos ipari partnerrel, kutatói pedig tudományos tevékenységet végeznek az MTA Veszprémi Területi Bizottsága munkabizottságaiban.

KÜRT Zrt.

A KÜRT 1989-ben alakult. Magyar tulajdonban lévő vállalkozásból mára nemzetközi vállalatcsoporttá vált. A múlt tapasztalatai, valamint az innovatív szemléletű, kimagasló tudású szakembergárda munkája eredményeként a KÜRT komoly elismertségre tett



szert az információbiztonság területének vezető szakértője, az adatvédelem és adatbiztonság teljes palettáját átfogó, a nemzetközi és hazai szabványoknak megfelelő módszertana és auditorai révén. Európa egyik vezető adatmentő cége világviszonylatban is elismert adatmentési technológiával.

A megelőzésre kidolgozott, Információmenedzsment rendszerünk ma már több mint 40 önállóan is alkalmazható termékünk gyűjtőfogalma.

A KÜRT megalakulása óta nyereségesen működő vállalkozás, alaptőkéje 20 M Ft, alaptőkén felüli vagyona 800 M Ft.

A KÜRT első külföldi leányvállalatát, a KUERT Datenrettung Deutschland GmbH, 2003-ban alapította Németországban, 2004-ben pedig a KUERT Information Management GmbH lépett piacra ausztriai székhellyel. A 2007-ben a KÜRT megalapította leányvállalatát Dubai-ban, (KÜRT Information Security LLC), valamint az USA-ban (KURT Security, LLC) is.

A KÜRT tevékenységeit 1997. óta ISO 9002, 2002. óta ISO 9001-2000 tanúsítvány birtokában végzi. ISO 27001-es tanúsítvánnyal és NATO beszállítói minősítéssel is rendelkezik.

Albacomp Zrt.

Az Albacomp Zrt. a magyarországi informatikai piac egyik legnagyobb múltra visszatekintő vállalata, a hazai iparág meghatározó szereplője.

A 440 főt foglalkoztató székesfehérvári vállalat 2006-ban 15.5 milliárd forint árbevételt ért el. A cég összeszerelő részlegében 2006-ban 37.300 PC-t gyártottak, melyből 4.000 készült exportra.

A számítógépek összeszerelése mellett az Albacomp nevét több nagy, hálózati és rendszerintegrációs projekt is fémjelzi. A társaság aktív



résztevője több, kormányzati támogatással megvalósult informatikai programnak, valamint a munkaügyi, az informatikai és az oktatási tárca által meghirdetett Sulinet Expressz Programnak.

Az Albacomp Zrt. integrált informatikai megoldásszállítóként támogatja az önkormányzatokat a helyi e-közigazgatás kiépítésében.

Az Albacomp Zrt. egyik legfőbb célja, hogy mint Magyarország egyik informatikai tudásbázisa, helyt adjon a kreativitásnak, lehetőséget és szakmai támogatást biztosítson tehetséges szakembereknek új termékek kifejlesztésére. Az 1990-es évek elején létrejött Albacomp K+F csapat nevéhez immár több, egyedülálló termék megalkotása fűződik. Ilyen például az Elnfopont érintőképernyős terminál vagy a Personal Monitor.

A fentiek mellett számos szoftver alkalmazás, egyedi megoldás fűződik az Albacomp K+F csapatának nevéhez.

A vállalat teljes tevékenységére megszerezte az ISO 14001:2004 környezetirányítási tanúsítványt, valamint megújította ISO 9001:2000 minőségbiztosítási tanúsítványát, melyre alapozva a cég megszerezte a "NATO elfogadott szállítója" minősítést.

A konzorciumi tagok korábbi együttműködése

- A KÜRT vezetői és szakértői a MIK tanszékei által oktatott tantárgyak előadásain 2000-től kezdve rendszeresen vesznek részt előadóként. Az előadások során a KÜRT képviselői a tananyaghoz szervesen kapcsolódó gyakorlati információtechnológiai ismereteket adnak át a hallgatók számára.
- A MIK - valamint a jövőben a futurIT - keretében megvalósuló

PhD kutatási témákat a MIK oktatói és a KÜRT információtechnológiai szakértői közösen irányítják, így garantálva, hogy a témák a szakterület aktuális problémáit fedjék le.

- A KÜRT és a PE korábban a Széchenyi pályázat keretében már közös NKFP projektben vett részt és sikeresen teljesítette azt.
- A KÜRT vezető munkatársai a PE oktatóival a témavezetésben együttműködve több PhD képzésben vettek részt a Pannon Egyetemen, illetve számos sikeres diplomamunka elkészítésének irányítása fűződik nevükhöz.
- A KÜRT és a PE MIK 2005-ben a Jedlik Ányos program keretében a közös előkészítést követően a KÜRT, mint konzorciumvezető irányításával három évre szóló pályázati támogatást kaptak a humán, a logikai és a fizikai biztonságot egyesítő integrált informatikai biztonsági megoldások módszertanának, illetve kapcsolódó szoftverek és szenzorok kifejlesztésének támogatására.
- A KÜRT és az ALBACOMP együttműködését főként informatikai illetve rendszer- és hálózatépítési projektek jellemzik. Közösen végezték számos magyarországi nagyvállalat és állami intézmény informatikai kockázatainak felmérését, illetve az informatikai biztonsági rendszerek kialakítását, telepítését.
- 2000/2001-es tanévtől Székesfehérváron a Pannon Egyetem Kihelyezett Képzési Helyeként műszaki informatikai mérnök-asszisztens iskolai rendszerű felsőfokú képzés indult. A PE a SZÜV Területi Igazgatóságán működteti a képzéseket, itt a 2002/2003-as tanévben további számviteli szakügyintéző, pénzügyi szakügyintéző, logisztikai műszaki menedzser asszisztens, gépipari mérnökasszisztens és idegenforgalmi szakmenedzser AIFSZ szakokat indított. Az ALBACOMP a SZÜV 100%-os tulajdonosa.

tevékenységünk

Tevékenységünk

Az utóbbi évtizedek során alapvetően változott meg a biztonsággal kapcsolatos vélekedés. Ma már természetes, hogy a legkülönbözőbb élethelyzetekben merül fel a biztonság és a kockázatarányos védelem kérdése a közlekedéstől a személyes adatok védelméig keresztül egészen a banki adatkezelésig. A szervezeteknek ma már nem termékekre van szükségük, hanem az általuk elvárt biztonsági szint folyamatos fenntartására. Nem biztonsági eszközöket akarnak, hanem biztonságos működést, nem riasztókat, hanem betörésmentes infrastruktúrát, nem vírusirtót, hanem vírusmentes működést. Ezt az állapotot elérni és fenntartani csak átfogó és rendszerbe illeszkedő biztonsági megoldások alkalmazásával lehet.



A technikai fejlődéssel párhuzamosan az intézmények, gazdasági szervezetek életében egyre fontosabb szerepet tölt be, egyúttal növekvő értéket képvisel a tárolt adatok, dokumentumok formájában megjelenő, tárgyalások, telefonos megbeszélések során elhangzó, vagy konkrét termékekben, prototípusokban

megtestesülő információ. Az információ egy vagyonelem, és ugyanúgy, mint más vagyonelemek, jelentős - gyakran pótolhatatlan illetve felbecsülhetetlen - értéket képvisel a tulajdonosai, illetve a felhasználói számára.

A számítástechnikai rendszerekben tárolt és kezelt információk értéke évről évre nagyságrendekkel növekszik. Az információ minden formája hordozhat értéket, amelyet védeni kell az illetéktelen kezekbe kerüléstől vagy az elvesztéstől, esetleg használhatatlanná válástól - legyen ennek oka akár szándékos károkozás vagy valamilyen véletlen esemény. (Elég, ha csak egy kórház betegeinek előírt gyógyszeradagolását tartalmazó adatbázisra, egy könyvelőcég ügyféladatait tartalmazó adathordozóra, vagy egy katonai parancsnok bizalmas információit tartalmazó notebookra gondolunk.)

A rendszerekben tárolt, illetve az azokon keresztül elérhető információk bizalmassága, sértetlensége és rendelkezésre állása alapvető fontosságú a versenyképesség, a jövedelmezőség és a fejlesztési tervek fenntarthatóságában. A számítógépek megjelenésével nemcsak az információ védelme fejlődött, hanem maga a védendő információ is óriási változásokon ment keresztül. A számítógépes hálózati rendszerek kialakulása és fejlődése gyökeresen alakította át az információ gyűjtését, feldolgozását, kezelését, tárolását. Az információ az innováció egyik legfontosabb forrásává vált, értéke jelentősen megnőtt. A szervezetek információs rendszerei és hálózatai egyre inkább szembesülnek a biztonságukat fenyegető veszélyek széles skálájával, beleértve a számítógépes csalásokat, a kémkedést, a szabotázszt vagy a szándékos visszaéléseket, illetve a különböző környezeti fenyegetettségeket. A sérülések (mint például a számítógépes vírusok, a számítógépes betörések, illetve nem szándékos meghibásodások hatásai) egyre

gyakoribbá, súlyosabbá válnak. A működést érintő biztonsági incidensek mintegy 80%-a informatikai jellegű, ezen belül több mint 70% emberi mulasztásra vezethető vissza.

Az informatikai biztonság mai helyzetét nagyjából úgy jellemezhetnénk, hogy az intézmények, vállalkozások és magánszemélyek felbecsülhetetlen értékű adatokkal, adatbázisokkal rendelkeznek, és igen nagy részük használ is különféle eszközöket, megoldásokat adatvédelmi, megelőzési céllal. Viszont lényegesen kevesebb azoknak a száma, akik ezeket rendszerbe foglalva, és annak megfelelően a működést, illetve működtetést szabályozva alkalmazzák.

Az informatikai biztonság optimális szintjének elérését szolgáló rendszerek építéséhez építőelemként felhasználható eszközök tárháza széles, és folyamatosan bővül. Terjednek azok a szabványok és eljárások is, amelyekkel a kiépített rendszerek minősíthetők. Olyan szisztematikus tervezési módszertanok viszont nem állnak rendelkezésre, amelyek az elérhető eszközök felhasználásával garantált minőségű informatikai biztonságot eredményeznének. Ilyen módszertanok kidolgozása a szakterület alapvető igénye. A Magyarországon is rohamosan fejlődő informatikai rendszerek és eszközök, a keletkező információk növekvő tömege és koncentrációja új biztonsági kihívásokat jelentenek. A futurIT ezért legfontosabb feladatának egyrészt az információk kezelésének biztonságossá tételét, védelmét célzó módszerek, eszközök kialakítását, másrészt az elvárható előnyök és a vállalt biztonsági kockázatok mértékének meghatározását tekinti.

A futurIT célja, hogy a tudományterület vezető elméleti és gyakorlati szakembereinek kiemelkedő szintű képzésével, szakmai tapasztalataik hasznosításával, valamint - a legújabb

technikai és társadalmi változásokat szorosan követve - világszínvonalú informatikai biztonsági eljárások, módszertanok és eszközök fejlesztésével a Közép-Dunántúli Régió, Magyarország és Közép-Európa vezető informatikai biztonsági kutató- és képzési központjává váljon.

A veszteségek csökkentésének leghatékonyabb eszköze a képzés, oktatás, illetve megfelelő szabályozások, informatikai biztonsági módszertanok és eszközök kialakítása és elterjesztése. A Regionális Informatikai Biztonsági Tudásközpont kutatás-fejlesztési, illetve képzési programjai az informatikai biztonság területére koncentrálnak, és a programok kialakításakor alapvető szempontnak tekintettük, hogy a futurIT által megvalósítandó kutatás-fejlesztési projektek, képzések szorosan kapcsolódjanak az informatikai biztonság és az információvédelem témaköréhez, valamint a szakterület nemzetközi tudományos és piaci trendjeihez. Az elindított képzési programok keretében megszerezhető információbiztonsági ismeretek naprakész, elismert és piacképes szaktudást testesítenek meg, ezáltal az itt koncentrált, innen kikerülő szaktudás jótékony hatással van a régió gazdasági életére is. A biztonsági rendszerek jellegükből adódóan folyamatos fejlesztésre szorulnak, annak érdekében, hogy ellenálljanak a folyamatosan fejlődő támadási módszereknek, megfeleljenek az újabb és újabb kihívásoknak. Egy rendszer biztonságát alapvetően meghatározza az újonnan felmerülő kihívásokra adott válaszok gyorsasága. Ezért tűzte ki célul a futurIT, hogy kutatási tevékenysége eredményeként olyan megoldásokat nyújtson az informatikai biztonság fejlesztéséhez, amelyek hosszú távon is képesek hatékonyan fenntartani a kockázatarányos biztonság szintjét.

A futurIT kutatás-fejlesztési programjai az informatikai biztonság szempontjából alapvetően háromféle feladat megoldására koncentrálnak:

- az információ elvesztésének (megsemmisülésének) megakadályozására,
- az információ illetéktelen kézbe kerülésének megakadályozására,
- az üzletmenet-folytonosság biztosítására.

Az informatikai biztonság, mint állapot elérését és folyamatos fenntartását a futurIT a következő tevékenységeivel támogatja:

- Informatikai biztonsági szabványok és módszertanok kidolgozása
- Informatikai biztonsági tudásbázis kialakítása
- Informatikai biztonsági szabványok, módszertanok és eszközök használatának oktatása, népszerűsítése
- Informatikai biztonsági eszközök fejlesztése
- Informatikai rendszerek tervezése, működtetése és minősítése

A futurIT kutatás-fejlesztési tevékenységei egy úgynevezett kockázat-orientált spirális életciklus modellen keresztül valósulnak meg. A modell alkalmazásának előnye, hogy rendkívül világos a tevékenységek struktúrája, egyszerű a megvalósítás, és biztos alapot nyújt a tervezési fázisok feladatainak egységes szemléletű végrehajtásához. A koncepciókészítésnél az a cél, hogy a fejlesztési munkát az elképzeléseinkre alapozhatjuk, a tervezés fázisában pedig arra törekszünk, hogy az általunk elképzelt rendszer megvalósítható legyen, és a felhasználók igényeit a megoldások

maradéktalanul kielégítsék. A spirális életciklus modell lényeges sajátossága, hogy a kidolgozandó megoldások, valamint a fejlesztéseket támogató módszerek és eszközök kiválasztásának kritériuma a funkció rizikófaktoron alapuló hasznossága.

A spirálmodell szerinti megközelítésmód esetében a kiindulási pont a követelmények meghatározása és a kockázatok specifikálása. Ezt követi a fejlesztések tervének kidolgozása, a költségek becslése és a megvalósíthatósági alternatívák elkészítése. Az első körben kidolgozott tervek alapul szolgálnak a felhasználói oldal által is minősíthető prototípusok fejlesztéséhez, majd a kivitelezési és tesztelési munkák elvégzéséhez. A prototípuskészítés elvének alkalmazása nagymértékben csökkenti a kutatás-fejlesztési tevékenységek bizonytalanságát, hiszen olyan folyamatok végrehajtására kerül sor, amelyekben a nagyvonalú felhasználói elképzelések és a rendszerről feltárt ismeretek alapján kidolgozhatók a kívánt modellek.

A futurIT szoros kapcsolatban áll a fejlesztésekben, illetve a kutatási eredmények hasznosításában együttműködő régióbeli vállalkozásokkal, valamint a kutatási és felsőfokú képzési programban nemzetközi partnerként résztvevő oktatási intézményekkel. Létrehozásával olyan szaktudás koncentrálására nyílt lehetőség, amely - az informatikai és információbiztonság témakörében - egyedülálló nemcsak a régióban és Magyarországon, de a környező országok tekintetében is. Így nagymértékben emeli az itt folyó szakképzés vonzerejét, illetve a kutatás-fejlesztési eredmények egyedisége miatt növeli a régió vállalkozásain keresztül érvényesülő gazdasági hatásokat, a helyi vállalkozások know-how-jának értékét.

KUTATÁSI PROGRAMJAINK



információbiztonság

Nemzeti és iparági információbiztonsági rendszerek kidolgozása



Az információk, a megszerzésükre, tárolásukra és kezelésükre vonatkozó eljárások, illetve az informatikai rendszerek és hálózatok fontos üzleti értéket képviselnek.

A Magyarországon is rohamosan fejlődő informatikai rendszerek és eszközök, a keletkező információk növekvő tömege és koncentrációja új biztonsági kihívásokat jelentenek. Ezért kutatás-fejlesztési programunk célja, hogy a tudományterület és az iparág legújabb elméleti eredményeinek és gyakorlati tapasztalatainak felhasználásával a különböző specifikus szakterületekre, iparágakra vonatkozó, testre szabott információbiztonsági eljárásokat, módszertanokat és eszközöket dolgozzunk ki, illetve gyakorlati hasznosításuk megvalósítását támogassuk.

A program eredményeként a gyakorlatban is használható, testre szabott biztonsági kritériumrendszerek, módszertanok, eszközök és szabályozások jönnek létre az információbiztonsággal összefüggő veszélyek, kockázatok feltérképezésére, értékelésére és kezelésére. Elsősorban azokon a területeken, ahol a várható veszteségek nagysága vagy a veszteségek bekövetkezésének nagy valószínűsége miatt erre a leginkább szükség van (pl.: egészségügy, közigazgatás, oktatás, kritikus infrastruktúrák, belbiztonság, nemzetbiztonság, honvédelem). A kutatások egyrészt a hiányos vagy hibás információkezelésből és információvédelemből eredő veszteségek megelőzését, másrészt azok minimalizálását és kezelését célozzák.

Ez a szakterület, illetve a hozzá kapcsolódó kutatás-fejlesztési feladatok speciális szakértelmet igényelnek. Hasonló területen működő, hasonló iparág specifikus információbiztonsági megoldások kidolgozására törekvő, egyetemi és ipari kötődésű kutatási program jelenleg nem működik Magyarországon. A hazai és a nemzetközi trendeket is figyelembe véve megállapítható, hogy hasonló, specifikus szabályozásra törekvő koncepciók elvételre ugyan előfordulnak, de a futurIT kutatási programja által megcélzott teljes körű, specifikus információbiztonsági módszertanok jelenleg még nem állnak rendelkezésre.

A kutatási programunk továbbá feladatának tekinti a jelenleg heterogén hazai információbiztonsági szabályozási rendszer konszolidálását, és a szabályozók számára olyan ajánlások kidolgozását, amelyek figyelembe veszik az informatikai rendszerek fejlődését és a legújabb eredményeket, valamint alkalmasak az információbiztonsági kérdések teljes körű és átfogó kezelésére.



humán biztonság

Szervezeti és humán biztonsági kutatások



A szervezeti és humán biztonsághoz kapcsolódó kutatási témánk abból a megállapításból indul ki, hogy a működési kockázatok témaköre kiemelten kezeli ugyan a szervezeti és humán kockázatokat, azok szerepét

az üzleti folyamatokban, a lehetséges károkozások tekintetében, de nem tud megfelelő módszertani javaslatokat adni ezen kockázatok rendszerszintű kezelésére. A témában elvégzett piackutatásunk eredményei is alátámasztják, hogy a kiélesedett versenyben az emberi erőforrás kiemelkedő jelentőségűvé vált, miközben ezzel egyenes arányban nő az ebből eredő kockázatok jelentősége is.

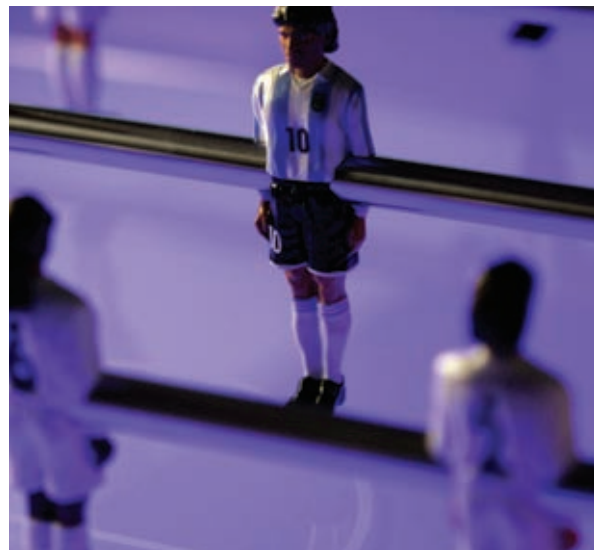
Az ANIMA Polygraph Pszichológiai Tanácsadó Kft.-vel közösen elindított kutatás-fejlesztési programunk célja, hogy módszertant fejlesszen ki a humán (és szervezeti) erőforrások kockázatainak elemzésére, a fenti tényezőkből származó kockázatok szerepének értékelésére a szervezeti működés folyamataiban, valamint hogy ezek rendszerbe foglalásával megbízható, automatizált előrejelzési, illetve riasztási lehetőségeket dolgozzon ki.

A jelenleg elérhető humán biztonsági megoldások nem rendszer-szemléletűek, sőt gyakran szubjektívek, és a folyamatok átfogó vizsgálata nélkül szemlélik a humán biztonsági kockázatokat. Magyarországon a futurIT kezdeményezte először a humán biztonsági kockázatok objektív módszertan alapján történő elemzését, az üzleti és működési folyamatokba való beillesztését, valamint ezek átfogó biztonsági rendszerbe történő foglalását. Kutatás-

fejlesztési tevékenységünk eredményeként elérhetővé válik a szervezeti folyamatokban rejlő biztonsági rések és a humán erőforrás kockázatait tekintve a kognitív, affektív és viselkedési megnyilvánulások integrált kezelése, preventív hasznosítása és az automatikus biztonsági riasztások megvalósítása.

Kutatóink, Méri László professzor vezetésével, egyrészt a kommunikációs folyamatok átfogó elemzése kapcsán a megjósolhatóságra, másrészt a humán biztonsági kockázatok fennmaradásával kapcsolatban a valószínűsíthető károkozás számszerűsítésére törekednek.

A program keretében megvalósítandó kutatási témák a szervezeti folyamatok biztonsági kockázatainak feltárására; a kockázatkereső és/vagy -kerülő magatartás humán erőforrás biztonsági hatásainak vizsgálatára; továbbá a félrevezető kommunikáció és manipuláció viselkedési megnyilvánulásainak érzékelésére, azonosítására és a beavatkozások módszertanának kidolgozására irányulnak.



Adatmentés - technológia kutatás



Az adattárolók forradalmát éljük. A hagyományos mágneses alapú adattárolás kezd elérni technológiai korlátait, melyet már csak különböző trükkökkel fessegetnek, a flash alapú tárolók pedig egyre nagyobb teret hódítanak.

Jelenleg azonban az tűnik valószínűnek, hogy mégsem a flash lesz a jövő adattárolási technológiája. Egy biztos: egyre több adatot szeretne az emberiség tárolni, és ezekből az adatokból mindig fog elveszni, mindig lesz mit megmenteni.

A KÜRT adatmentése folyamatosan változó, fejlődő adattároló eszközökkel, technológiákkal foglalkozik, így természetesen állandó fejlesztésre van szüksége a mentési feladatok professzionális ellátásához. Ennek ellenére a jelenlegi technológiáknak is vannak olyan területei, melyekkel a KÜRT adatmentés még nem tudja kezelni idő- vagy kompetenciahiány miatt. Az adatmentés-adattárolás témalaborban részt vevő hallgatók elsőként egy, a KÜRT Adatmentés Know How(tm) elméleti oktatásának megfelelő képzést kaptak hogy ezen keresztül megismerjék a KÜRT jelenlegi technológiai képességeit és főbb fejlesztési irányait. Ezután vontuk be őket a konkrét kutatási feladatokba.

Kutatási területek:

- A Novell Netware által használt legújabb NSS fájlrendszer-logikai felépítése, a mentés módszerei. A piacon léteznek részleges szoftveres adatmentési megoldások, azonban ezek távolról sem nyújtanak olyan tág lehetőségeket, amelyekkel a bonyolultabb esetek is megoldhatók lennének.

- „Storage” elmélet - A „storage” rendszerű adattárolás összetett struktúráiról, kockázatairól, módszertanairól szól a kutatás. Hogyan kell felépíteni egy storage-ot, hogy arról könnyű legyen adatot menteni? Hogyan kell visszafejteni egy sérült storage struktúráját?
- Flash adattárolók visszafejtési megoldásai. A flash adattárolóknak nem szabványos az adattárolási struktúrája, ahány típus, annyiféle megoldást használnak a gyártók. A meghibásodott adattárolóról sokszor nem derül ki, hogy az adott struktúra hogyan épül fel, így típusazonos eszközt használva kell a tárolási struktúrát visszafejteni. Ez egy igen bonyolult, sok emberi erőforrást foglaló matematikai/technológiai feladat, melynek automatizálása, szoftveres vagy bármilyen más módon való támogatása a cél
- JPG fájlok belső struktúrájának visszafejtése - A digitális fotótechnika elterjedésével napi problémává vált a hibás jpeg fájlok javítása, javítási algoritmusainak kidolgozása. Ez a magas tömörítési ráta miatt komoly matematikai, logikai probléma már akár néhány bajtnyi hibás adat esetén is.



tudásmenedzsment

Tudásmenedzsment program



A futurIT program keretein belül folyó szakmai tevékenységek támogatását oldja meg a Tudásmenedzsment program. Ennek legfontosabb célkitűzései és feladatai a következők:

- Az egyes kutatási programokban összegyűjtött információ és szaktudás megosztása az egyes kutatási témák között.
- Az egyes kutatási programokban létrehozott eredmények központi értékelése és tárolása.
- A kutatási programokban alkalmazni kívánt emberi erőforrások felkutatása és rendelkezésre bocsátása.
- A program keretein belül tevékenykedő kutatók és szakemberek szakmai fejlődésének gondozása és karriermenedzsmentje.
- A létrehozott eredmények minél hatékonyabb kommunikációja a tudományos és üzleti szektor irányába.
- Kapcsolattartás más kutatóhelyekkel és szakmai szervezetekkel.

A Tudásmenedzsment program erősíti a futurIT szakmai megalapozottságát és elismertségét az akadémiai és üzleti életben, ezzel járul hozzá a projekt alapvető céljainak eléréséhez.

Részfeladatok

1. Infrastruktúra kialakítása, amely a működéshez szükséges fizikai környezetet jelenti, biztosítja az internetes megjelenést, az ügyfelekkel, tudományos partnerekkel és a látogatókkal történő kommunikációt.
2. Szervezetfejlesztés, amelyben az infrastruktúra kialakítása

után az egyes tevékenységeket végző szervezeti egységeket is létrehoztuk.

3. A napi operatív működési folyamatok kialakítása, amelyek biztosítják, hogy a kutatási programok és a belső és külső szakemberek kapcsolódhassanak a tudásbázis elemeihez és a kialakított technikai infrastruktúrához.

Jelenleg a kiszolgálói infrastruktúra kialakításán dolgozunk, elindultak a kiszolgálói folyamatok, folyamatosan töltjük a rendszerbe a készülő szakmai anyagokat.

A futurIT Tudásmenedzsment legfontosabb területei

A Tudásmenedzsment program a futurIT horizontális tevékenysége, amely az egész projekt keretében megvalósított kutatási programok szakmai eredményeinek összesítését és publikálását végzi.

A legfontosabb területek a következők:

- futurIT portál
- biztonsági fórum
- folyóirat, tematikus és időszaki kiadványok
- tudományos cikkek
- szakmai, illetve ismeretterjesztő cikkek
- tanulmányok és elemzések
- konferencia előadások
- pályázati bírálatok
- pályázatok anyagai
- szervezeti tagságok
- futurIT tehetséggondozási program (összhangban a Pannon Egyetem MIK tehetséggondozási programjával)

futurIT
„Informatikai Biztonsági
Kutató-Fejlesztő Központ”



EREDMÉNYEINK



Beszámolási időszak feladatai

RET - 1. szakasz beszámoló anyagai						
Feladatok		Eredménytermékek (tanulmányok / beszerzett eszközök)				
Feladat	Részfeladat	Szakmai tartalom	Átadandó termék	Felelős	Határidő	
II. Az informatikai biztonsági megoldások egységes módszertani háttérnek megteremtése	1. részfeladat: Informatikai megoldások biztonsági tervezési és minősítési módszertanának kialakítása	Informatikai biztonsági minősítési eljárások kidolgozása	Dokumentált tervezési és minősítési módszertan	KÜRT	-	OKT. 15.
	2. részfeladat: Nemzetközi informatikai biztonsági szabályozási rendszer kidolgozása	Nemzeti szintű információbiztonsági Tudásbázis összeállítása és folyamatos aktualizálása	Átfogó információ-biztonsági ajánlás rendszer	KÜRT	-	OKT. 15.
	3. részfeladat: Informatikai fenyegetettség és kockázatok felmérése, elemzése és kezelése	Kockázatelemzési módszertan és szakterület specifikus kockázatelemzési módszertanok kidolgozása Informatikai ill. információ biztonsági ajánlások összeállítása (parágákra, eszközökre, fenyegetettségekre) Információbiztonsági fenyegetettség térképek összeállítása	Dokumentált kockázatelemzési módszertanok és fenyegetettség térképek	KÜRT	-	OKT. 15.
III. Az informatikai biztonsági minősítés és eszközfejlesztés	2. részfeladat: Informatikai biztonsági eszközök fejlesztése	Információbiztonsági fenyegetettség térképek összeállítása	Biztonságos informatikai rendszerek tervezési módszertana	KÜRT	-	OKT. 15.
IV. Az informatikai biztonsági képzési rendszer kiépítése	2. részfeladat: Informatikai biztonságtechnikai képzés beindítása mérnöki mesterszak (MSc) keretében	Az MSc képzés rendszerének kidolgozása, tanmenet összeállítása, tananyagok összeállítása, informatikai biztonsági MSc képzés elindítása, szigorlatok, szakdolgozatok	Hallgatói Együttműködés Program dokumentációja	KÜRT	PE MIK	OKT. 15.
	2. részfeladat: Nemzetközi informatikai biztonsági szabályozási rendszer kidolgozása	Információbiztonsági internetes portál létrehozása, menedzselése, folyamatos aktualizálása és fejlesztése (3 évfolyam) Hazai és nemzetközi informatikai biztonsági konferenciák szervezése és menedzselése Lektorált tartalmú tudományos szakfolyóirat elindítása, menedzselése és promotálása (1 évfolyam) Szakmai tréningek, felnőttképzési programok és társadalmi események szervezése, menedzselése és lebonyolítása	Aktualizált fűtűT honlap, a portál szolgáltatások leírása Konferenciák dokumentációja A fűtűT portálon a szakmai folyóirat 1. számának megjelenése PDF formátumban Felnőttképzési tananyagok és szakmai továbbképzési anyagok	KÜRT	PE MIK	OKT. 15. NOV. 5. NOV. 5. OKT. 15. OKT. 15.

eredményeink

Eredményeink összefoglalása

A futurIT, mint Regionális Tudásközpont, elmélyült tudományos és intenzív szakmai, üzleti együttműködés keretében egyesíti a partnerek szaktudását, kutató, oktató és fejlesztő kapacitásait, valamint nemzetközi kapcsolatait és tapasztalatait. A projekt első munkaszakaszában elért eredmények hozzájárulnak az informatikai biztonság témakörén belül az innovációs, illetve kutatás-fejlesztési kapacitások növeléséhez. Eközben a szakképzésen keresztül helyi tudásintenzív kis- és középvállalkozások számára teremtenek munkaerőt, illetve - a konzorciumi tagok saját K+F tevékenysége révén - a képzett munkaerő számára megfelelő munkalehetőséget. Az alap- illetve alkalmazott kutatási munkák segítségével az együttműködő partneregek és a régióban működő vállalkozások értékesíthető termékekhez, szolgáltatásokhoz és új munkahelyekhez jutnak.

Az elért eredmények nemzetközi bemutatása tudományos szakmai publikációkon és konferenciákon keresztül történik. Ezekon keresztül - neves oktatási intézmények, illetve nemzetközi szakmai egyesületek, szakhatóságok, vállalkozások részvételével - egy olyan nemzetközi kapcsolati háló jön létre, amelynek segítségével a futurIT szakmai színvonala, elismertsége és innovációs képessége még tovább növelhető, a kutatás-fejlesztési tevékenységek kibővíthetők, és az eredmények gyakorlati hasznosítása a régió, illetve az országhatárokon kívül is lehetővé válik.

A futurIT kutatás-fejlesztési és képzési programjai - az informatikai biztonság szempontjából - alapvetően háromféle feladat megoldására koncentrálnak:

- Az információ elvesztésének (megsemmisülésének) megakadályozása.
- Az információ illetéktelen kézbe kerülésének megakadályozása.
- Az üzlet illetve a működés folytonosságának biztosítása.

A feladatok és az elért eredmények egyfelől a megelőzésre, másfelől - a káresemény bekövetkezése után - akár csökkentésre irányulnak. A fentiekkel összhangban az informatikai biztonság, mint állapot elérését és folyamatos fenntartását a futurIT a következő feladatok megvalósításával támogatja:

- Informatikai biztonsági tudásbázis kialakítása.
- Informatikai biztonsági szabványok . és módszertanok kidolgozása
- Informatikai biztonsági eszközök fejlesztése.
- Informatikai rendszerek tervezése, működtetése és minősítése.
- Informatikai biztonsági szabványok, módszertanok és eszközök használatának oktatása, népszerűsítése.
- Az informatikai biztonság hazai szakmai színvonalának emelése és társadalmi tudatosítása, kommunikációja.

projekt

I. Projekt előkészítés

infrastruktúra

1. Infrastruktúra előkészítése



A Regionális Informatikai Biztonsági Tudásközpont megcélzott kutatás-fejlesztési tevékenységek beindítása egy sor olyan eszköz és erőforrás meglétét feltételezte, amelyek korábban nem álltak rendelkezésre a konzorcium résztvevőinél.

Így a szükséges infrastruktúra kezdeti megteremtése olyan biztos alap kialakítására nyújtott lehetőséget, amely a későbbi munkaszakaszok eredményes kidolgozásának alapját jelenti.

A beruházási elképzelések középpontjában a Jedlik Ányos program keretében 2005-ben indított „Módszertan kidolgozása logikai, fizikai és humán biztonsági technológiák integrálására intelligens ágenseken alapuló eszközök alkalmazásával” kutatási-fejlesztési projekt infrastruktúra fejlesztési irányvonalának követése állt. Elérendő célunk egy nemzetközi szintű, tudományos körökben is elfogadott kutatói munkakörnyezet megteremtése. Ennek megfelelően a Központnak otthont adó helyiségek fejlesztése, a berendezések és eszközpark bővítése, korszerűsítése jelenleg is folyamatban van.

A futurIT számára új ingatlan beszerzésére nem került sor, a szükséges helyiségeket a Pannon Egyetem bocsátotta rendelkezésre az egyetem domináns, frekvenciált helyen fekvő „I” épületében. A helyiségek műszaki állapota, illetve a jelenlegi műszaki felszereltség hiányosságai miatt - a megfelelő munkavégzési feltételek biztosítása érdekében - a futurIT saját

költségvetéséből a számára rendelkezésre bocsátott egyetemi helyiségeket felújítja, illetve ezzel párhuzamosan kialakítja a szükséges technikai feltételeket és műszaki infrastruktúrát. A szükséges munkálatok elvégzésére, a kivitelezők kiválasztására közbeszerzési eljárás keretében kerül sor.



2. Kutatás-fejlesztéshez szükséges eszközök beszerzése



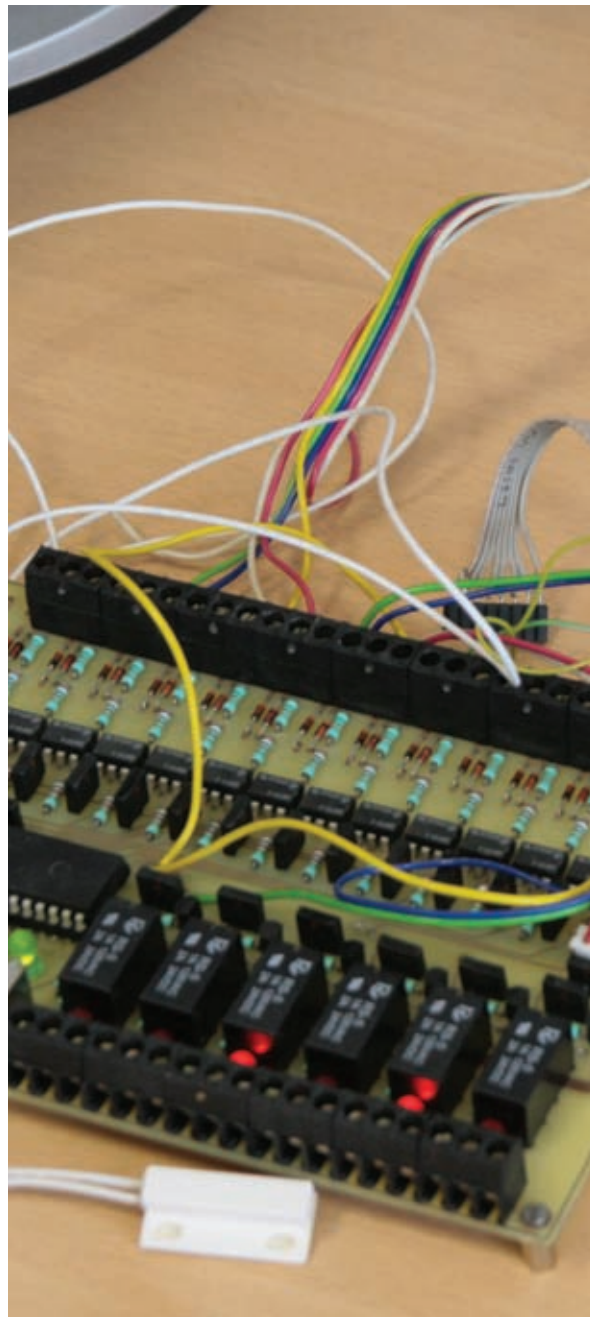
A projektben megfogalmazott cél egy nemzetközi szintű, tudományos körökben is elfogadott kutatói munkakörnyezet megteremtése, amelyben a feladatok végrehajtásához és a biztonságos környezet kialakításához, valamint a kialakított informatikai és információbiztonsági megoldások elemzéséhez szükséges számítástechnikai és egyéb eszközök rendelkezésre állnak.

Ennek megfelelően a Központnak otthont adó helyiségek fejlesztése, a berendezések és eszközpark bővítése, korszerűsítése jelenleg is folyamatban van.

A szükséges és még jelenleg hiányzó eszközök beszerzése a futurIT projektben közbeszerzési eljárás keretében megindult.

A beszerzés az első fázisban a következő eszköztípusokat jelenti:

- Számítógépek (munkahelyek és adatmentési eszközök)
- Fájl szerverek
- Hálózati nyomtató eszközök
- Számítógépes hálózat kialakításához szükséges eszközök
- Fizikai védelmi eszközök (beléptető, mozgásérzékelő, video megfigyelő eszközök)
- Szoftvereszközök (az első fázisban elsősorban a munkacsoport tevékenységet és oktatást támogató szoftverek)
- Irodai és oktatási szoftvercsomagok
- Kockázatelemzést támogató szoftverek



3. Szervezet kialakítása

A futurIT kutatás-fejlesztési szervezetével szemben támasztott elvárásokat egyrészt a futurIT hosszú távú stratégiájából következő célok, másrészt az egyes kutatási programok, illetve részfeladatok jellegzetességeinek megfelelően előálló elvárások határozzák meg. A szakmai munkavégzés a Karon hosszabb ideje sikerrel működő department rendszernek megfelelően szerveződik. Az egyes szakterületek szakértői, illetve a kutatási alprogramok végrehajtói úgynevezett „kutatói laboratóriumokba” szerveződve hajtják végre a feladataikat. A kutatói laboratóriumok egy-egy jól meghatározott szakterület, illetve tudományos kérdéscsoport mentén szerveződnek. Szakterületükhöz kapcsolódóan alap- és alkalmazott kutatásokat egyaránt folytatnak.

A laboratóriumok vezetői az adott tudományterület elismert akadémiai szakemberei, akik laboratóriumonként általában 4-10 fős - kutatókból és PhD hallgatókból álló - szakembergárdát irányítanak, és az egyes alprogramok feladatainak megvalósításához jól meghatározott célokkal és erőforrásokkal rendelkeznek.

Az egyes kutatási programok, és az ezek alapján meghatározott projektek, végrehajtásában két vagy több laboratórium is együttműködhet. Egy laboratórium, amennyiben szükséges, egyszerre több K+F projektben is részt vehet, hasonlóan a kutatókhoz, illetve a PhD hallgatókhoz. A laboratóriumok munkájában az Egyetem, a KÜRT és az Albacomp munkatársai mellett külső - meghívott - szakértők, egyetemi oktatók, kutatók is részt vesznek.

4. Pénzügyi rendszer kialakítása

A futurIT pénzügyi tevékenységeinek (tervezés, elszámolás, kontrolling) szabályozásához a Pannon Egyetem aktuális Gazdálkodási Szabályzata jelentette az alapot, mivel a futurIT az egyetem elkülönítetten gazdálkodó, részjogkörrel rendelkező költségvetési egységeként funkcionál.

A futurIT pénzügyi teljesítményének nyomon követése, ellenőrzése és értékelése egy egymással összefüggésben álló mutatókból felépülő, háromszintű Balanced ScoreCard mutatószámrendszer alkalmazásával történik: stratégiai szintű mérőszámok az átfogó teljesítmény-értékeléshez a hosszú távú stratégiai célok elérésének

függvényében; projektszintű mérőszámok a kutatás-fejlesztési programok megvalósításának értékelésére; valamint egyéni teljesítmény-értékelés a futurIT tevékenységében résztvevő személyek teljesítményének értékelésére.

A kidolgozott pénzügyi rendszer segítségével egységes kontrolling keretbe foglalható a kitűzött stratégiai, működési és irányítási célok elérésének mérése. A rendszer további előnye, hogy a mutatószámok aktuális értékei alapján megítélhető, hogy szükség van-e, és ha igen milyen mértékben, a teljes projekt, a programok illetve az operatív működés megváltoztatására.



it biztonság

II. Informatikai biztonsági megoldások



módszertan

1. Informatikai megoldások biztonsági tervezési és minősítési módszertanának kialakítása



A rendszer- és szoftverfejlesztés témakörét Magyarországon napjainkban kiemelten kezelik, ennek oka az informatika kiemelt szerepe a gazdaságban és az irányítási tevékenységekben. A versenyképes rendszer- és szoftverfejlesztő ipar kialakítása és működtetése elengedhetetlenül fontos ahhoz, hogy a magyar vállalkozások eredményesen bekapcsolódhassanak a nemzetközi munkamegosztásba.

A biztonsági problémák kezelése kilépett abból a korszakból, amikor pusztán IT technológiai kérdésként volt kezelendő. Az IT eszközök alkalmazása ma már szervesen illeszkedik az ügyviteli folyamatokba, ezért a technológiai védelem mellett az információ kezelési folyamatok védelme is elengedhetetlen.



Jellemző a mai helyzetre a biztonsági megoldások költségként való felfogása is, az újabb kutatások azonban rámutatnak arra, hogy a biztonság elsősorban befektetés.

A biztonság-tudatos fejlesztési, üzemeltetési módszerek fokozatos megjelenése és használatuk általánossá válása elősegíti a proaktív (és nem reaktív) védekezési módok előtérbe kerülését. Ma már számos olyan módszertan létezik, amely lehetővé teszi, hogy az eszközök, alkalmazások és rendszerek tervezése során megfelelő figyelmet fordítsanak a felmerülő biztonsági problémák kezelésére. Ezek piaci elterjedése az előrejelzések szerint 2010 -re várható; ennél fogva törekvéseinkkel ilyen eszközök kialakítására a legjobb időben vagyunk.

Az elkövetkező 5-10 év során kialakulnak és elterjednek azok a szoftverfejlesztési módszertanok, architekturális megoldások, és üzemeltetési gyakorlatok, amelyek lehetővé teszik az informatikai eszközök és rendszerek biztonságosabb használatát. Az általános biztonsági szint növekedésére különösen nagy hatása lesz a biztonságosabb szoftverfejlesztést lehetővé tevő módszertanok megjelenése. A biztonsági problémák többsége a szoftverfejlesztés problémáira vezethető vissza.

Jelenleg nem állnak rendelkezésre olyan módszertanok és eszközök, amelyek lehetővé tennék, hogy a piac által megkövetelt gyorsaság mellett is biztosítható legyen a biztonságos szoftverfejlesztés. Fontos látni, hogy a megfelelő funkcionalitással működő szoftver még nem feltétlenül biztonságos. A minőségi szoftver-

fejlesztés segíti ugyan a biztonsági problémák kiküszöbölését, ugyanakkor a biztonságos szoftver előállítására mindig többlet költséggel jár.

Szükség van a projekt és támogatási környezetek szigorú ellenőrzésére; az alkalmazói rendszerekért felelős vezetőknek vállalniuk kell a felelősséget a projekt és a támogatás környezetének biztonságáért. Gondoskodniuk kell arról, hogy megvizsgálják a rendszerben javasolt összes változtatást és megállapítsák, mennyiben befolyásolják ezek a rendszer vagy működési környezete biztonságát. Szükséges megfelelő fejlesztési szabályok kialakítása is.

Mivel az informatikai eszközök és rendszerek biztonsága jelentősen függ az üzemeltetők és felhasználók felkészültségétől is, ezért az előfeltételek közé kell sorolnunk a biztonsági kockázatok csökkentését elősegítő felhasználói és üzemeltetői ismereteket kialakulását is. A biztonság-tudatos felhasználói és üzemeltetői magatartás megteremtése elsősorban oktatás kérdése.

A projektben áttekintettük a legfontosabb használatos rendszerfejlesztési módszertanokat és szoftvertechnológiai megoldásokat, amelyek alapul szolgálhatnak a biztonság-tudatos fejlesztési tevékenységeknek. A projektben használt rendszerfejlesztési módszertan használja a vizsgált alapvető rendszerfejlesztési módszertanok (SSADM, RUP, MSF, SPICE, CMMI -Safety Extension) legfontosabb elemeit, mérőszámait, dokumentumait, ezeket egy célorientált megoldássá integrálja.



szabályozás

2. Nemzeti informatikai biztonsági szabályozási rendszer kidolgozása



A számítógépek megjelenésével nemcsak az információ védelme iránti igény nőtt, hanem maga a védendő információ is óriási változásokon ment keresztül.

A számítógépes hálózati rendszerek kialakulása és fejlődése

gyökeresen alakította át az információ gyűjtését, feldolgozását, kezelését, tárolását. A különböző szervezetek azzal a problémával találják szembe magukat, hogy tárolt információik olyan fenyegetettségeknek vannak kitéve, mint például az adatlopás, a számítógépes csalások, a kémkedés, a szabotázs, illetve az olyan környezeti fenyegetettségek, mint a tüzesetek, az árvíz.

A biztonsági fenyegetettségek sokrétűsége számos különböző védelmi mechanizmus egyidejű működését kívánja meg, ugyanakkor a hatékony védelem szükségessé teszi ezen mechanizmusok együttműködését és integrálását is. Kizárólag műszaki eszközökkel azonban csak korlátozott biztonság érhető el, éppen ezért szükséges azt megfelelő szabályozási és ellenőrzési módszerekkel támogatni.

A futurIT keretében megvalósítandó fejlesztési tevékenységünk során arra törekszünk, hogy a jelenleg heterogén hazai informatikai biztonsági és információbiztonsági szabályozási rendszer konszolidálása érdekében a szabályozók számára olyan ajánlásokat dolgozzunk ki, amelyek figyelembe veszik a technikai, technológiai fejlődés, illetve a legújabb kutatások eredményeit,

ezáltal alkalmasak az informatikai biztonsági kérdések átfogó szabályozására.

A nemzeti informatikai biztonsági szabályozási rendszer kidolgozásának célja egy olyan átfogó és homogén felmérési, elemzési, szabályozási, tesztelési, minősítési és tanúsítási módszertan kidolgozása, amely alapján az informatikai és információszolgáltatási rendszerek működése biztonságosabbá, megbízhatóbbá, átláthatóbbá, egyszerűbbé és hatékonyabbá tehető.

Az elkészült szabályozási rendszer a jövőben ajánlasként szolgálhat az információbiztonság komplex, szervezeti szintű kezeléséhez. Segítségével az információbiztonság megteremtése kapcsán lehetővé válik az egységes elveken nyugvó, a nemzetközi szabványokhoz és ajánlásokhoz igazodó, hazai előírások biztosítása.

Az egységes szabályozási rendszer továbbá átfogó tájékoztatást ad a szervezetek vezetésének és szakembereinek az információbiztonsággal kapcsolatos elvárásokról és követelményekről, illetve segítséget nyújt az informatikai fejlesztések valamennyi szakaszában a biztonság megtervezéséhez, megvalósításához, értékeléséhez és fenntartásához.

kockázatok

3. Informatikai fenyegetettségek és kockázatok felmérése, elemzése és kezelése



A vállalatok, szervezetek működési folyamataira ható kockázati tényezők bekövetkezési valószínűsége és kárpotenciálja változó.

A szervezetek informatikai függősége Magyarországon és a közép-kelet-európai régióban

is egyre nő, ami felveti a biztonságos informatikai rendszerek megteremtésének kérdését. Ennek egyik legfontosabb területe az informatikai fenyegetettségek és kockázatok felmérése, elemzése és kezelése. A szervezeteknek saját biztonságuk érdekében tisztában kell lenniük informatikai rendszereik gyenge pontjaival, kockázataival, valamint azzal, hogy miként, és milyen biztonsági intézkedésekkel tudják mérsékelni ezeket.

Elemzéseink azt mutatják, hogy egy szervezet biztonságának erősítése, fejlesztése kapcsán jelentkező új típusú kihívások és fenyegetettségek meghaladják a rendelkezésre álló lokális, illetve szakterület specifikus megoldásokat, intézkedéseket. Gyakran előforduló probléma, hogy ami kritikus helyi szinten egy-egy szervezeti egység vagy szakterület számára, az nem biztos, hogy kritikus a teljes szervezet számára is. Ráadásul minderről gyakran még pontos információkkal sem rendelkezik a szervezet, hiszen nagyon ritkák a szakszerű, tudományosan megalapozott és teljes körű fenyegetettség-elemzések és kockázatértékelések.

Kutatásaink megállapították, hogy az informatikai rendszerek biztonsága ellen ható veszélyek mára annyira összetettekké váltak,

hogy a kockázatelemzés formális módszerének az informatikai kockázatok elemzésére történő általános alkalmazása több komoly nehézségbe ütközik. Nem tudja megoldani a biztonság fokozását, és különösen az új fenyegetettségek elleni védelem problematikáját. Az informatikai kockázatok elemzése azonban elvégezhető a közvetlenül az informatikai védelmi intézkedésekre fókuszáló direkt módszerrel is, amelynek segítségével jóval kisebb ráfordítással könnyebben értelmezhető eredményt lehet elérni.

Eredményeink azt mutatják, hogy az eredményes megvalósításhoz a kockázatelemzési folyamatok olyan perspektívájára van szükség, amely képes - akár rövid távon is - objektíven átirányítani a rendelkezésre álló erőforrásokat oda, ahol az a leghatékonyabban képes a biztonsági kockázatokat mérsékelni. Ezért a futurIT keretében olyan átfogó és homogén módszertanok kidolgozására törekszünk, amelyek alapján az informatikai fenyegetettségek és kockázatok felmérése, elemzése és kezelése hatékonyan és eredményesen megvalósítható.





it biztonság

III. Informatikai biztonsági minősítés és eszköze fejlesztés



minősítés

1. Informatikai megoldások biztonsági minősítése



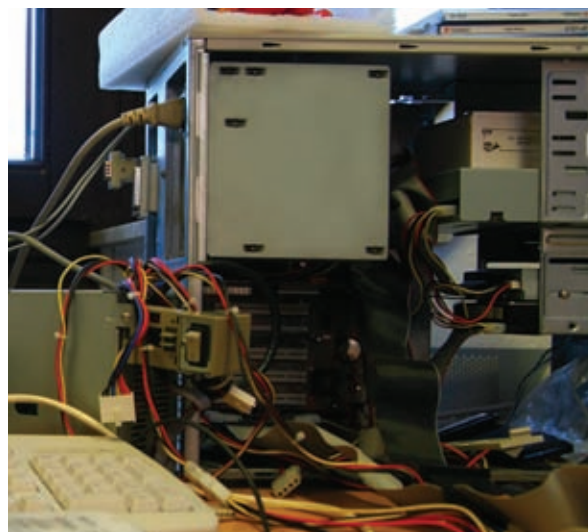
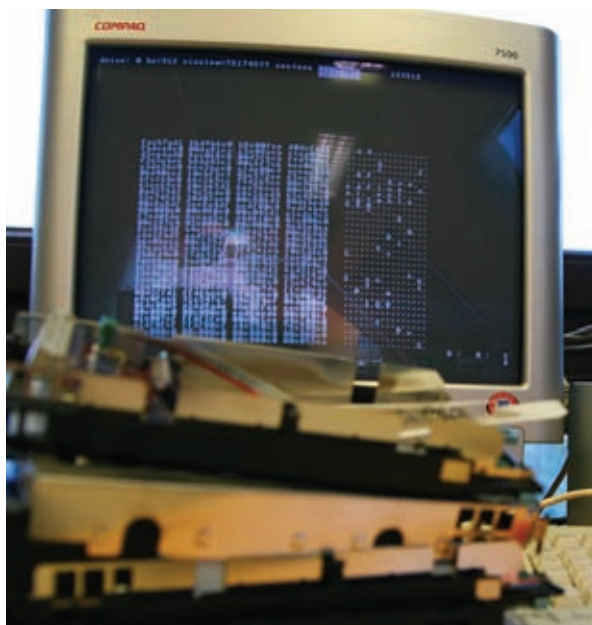
Világszerte nemzetközi szakmai és szabványügyi szervezetekben illetve a megfelelő nemzeti szinteken is folyamatosan fejlesztik és bővítik az információra, annak kezelésére, az információbiztonságra, a hozzá kapcsolódó eljárásokra, eszközökre vonatkozó szabványokat és irányelveket.

Ebben a témakörben kiemelt fontosságú, hogy el tudjunk igazodni a szabványok, szabványos eljárások, irányelvek, mérési, audit eljárások szövevényes hálózatában. Alapvető elvárás a témakör szakemberei felé, hogy minden területhez, feladathoz az arra leginkább megfelelő eljárást használják. Más az informatikai, a biztonsági és az informatikai biztonsági szabványok felhasználhatósága, mások az informatika üzemeltetését, az informatikai biz-

tonság technológiai kérdéseit szabályozó és az informatikai biztonsági rendszerek irányításával és ellenőrzésével kapcsolatos eljárások.

Az értelmezést és a kezelést megkönnyítő módon elemezzük a következő fontos szabványok és ajánlások legfontosabb elemeit és megállapításait:

- ITIL (IT Infrastructure Library)
- COBIT (Control Objectives for Information and Related Technology)
- ISO/IEC 15408 (CC-Common Criteria)
- BS7799 - ISO/IEC 17799:2005
- ISO/IEC TR 13335
- ISO/IEC 27001:2005
- NIST SP 800 (National Institute of Standards and Technology, Computer Security Resource Center)
- MEH ITB 8. sz. és 12. sz. ajánlása
- MIBÉTS irányelvek
- MIBIK irányelvek



fejlesztés

2. Informatikai biztonsági eszközök fejlesztése

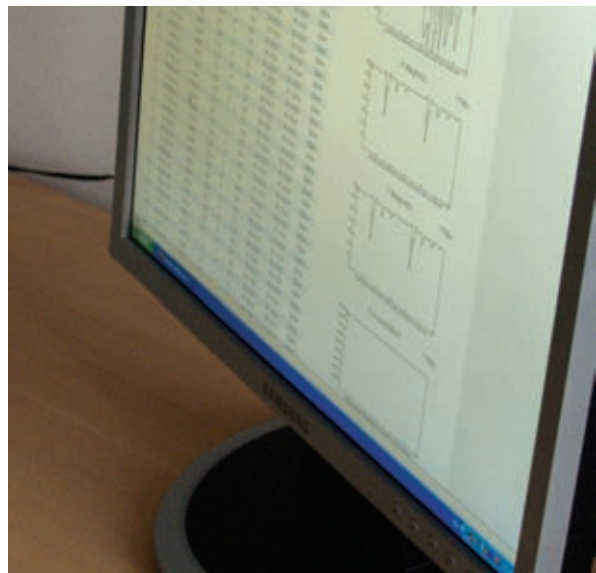


A projektben alkalmazott módszertani elvek alapján elmondható, hogy az elkövetkező 5-10 év során kialakulnak és elterjednek azok a szoftverfejlesztési módszertanok, architekturális megoldások, és üzemeltetési gyakorlatok, amelyek lehetővé teszik az informatikai eszközök és rendszerek biztonságosabb használatát.

Vizsgálatainkban megállapítottuk, hogy a biztonsági problémák többsége a szoftverfejlesztés problémáira vezethető vissza. Jelenleg nem állnak teljes körűen rendelkezésre olyan módszertanok és eszközök, amelyek lehetővé tennék, hogy a piac által megkövetelt gyorsaság mellett is biztosítható legyen a biztonságos szoftver fejlesztése. Fontos az a megfigyelés, hogy a megfelelő funkcionalitással működő szoftver még nem feltétlenül biztonságos. A minőségi

szoftverfejlesztés segíti ugyan a biztonsági problémák kiküszöbölését, ugyanakkor biztonságos szoftver előállítására mindig többletköltséggel jár. Szükség van a projekt és a támogatási környezetek szigorú ellenőrzésére. Az anyagban alkalmazott és elemzett szabványok alapján (különösen a CMMI - Safety Extension alapján) a felelős vezetőknek gondoskodniuk kell arról, hogy megvizsgálják a rendszerben javasolt összes változtatást és megállapítsák, mennyiben befolyásolják ezek a rendszer vagy működési környezete biztonságát. Szükséges megfelelő fejlesztési szabályok kialakítása is.

Mivel az informatikai eszközök és rendszerek biztonsága jelentősen függ az üzemeltetők és felhasználók felkészültségétől is, ezért az előfeltételek közé kell sorolnunk a biztonsági kockázatok csökkentését elősegítő felhasználói és üzemeltetői ismereteket kialakulását is. A biztonság-tudatos felhasználói és üzemeltetői magatartás megteremtése elsősorban oktatás kérdése.





képzés

IV. Informatikai biztonsági képzési rendszer kiépítése



PhD

1. Informatikai biztonsági doktori képzés és kutatás



A futurIT kutatás-fejlesztési tevékenységébe aktívan bevonja a Pannon Egyetem Informatika Tudományok Doktori Iskolájának hallgatóit.

A képzés célja a kiemelkedő tehetségű hallgatók számára olyan gyakorlati képzési lehetőség biztosítása, ahol az informatikai biztonság területén az élvonalba tartozó kutatásokban vehetnek részt, illetve olyan átfogó szakképzést kaphatnak, amelyen keresztül az informatikai biztonság és adatvédelem területén kiemelkedő elméleti tudású szakemberekké válhatnak.

A tudásközpontozó kapcsolódó témákban az „Integrált biztonsági rendszerek szintézise” témakör került meghirdetésre, erre jelentkezhetnek a legkiemelkedőbb képességekkel és tanulmányi eredményekkel rendelkező hallgatók.

A most lezárult időszakban három PhD hallgató diplomavédése történt meg az információbiztonsághoz kapcsolódó témákban (adataik az indikátor táblázatban szerepelnek). Jelenleg négy hallgató végez tanulmányokat egyéni tématerv alapján, de a futurIT kutatás-fejlesztési tevékenységével és céljaival szoros összefüggésben.

A PhD képzés hosszabb távon a hasonló területen tevékenykedő más EU-beli egyetemi központokon keresztül - kooperáció keretében - külföldre is ki fog terjedni.



mesterszak

2. Informatikai biztonságtechnikai képzés beindítása mérnöki mesterszak (MSc) keretében



A futurIT által elindított képzési és oktatási programok szervesen kapcsolódnak a Tudásközpont kutatás-fejlesztési programjaihoz.

A kutatás-fejlesztési eredmények beépülnek az oktatási anyagokba, így is biztosítva az oktatás

naprakészségét. A PhD hallgatók bevonása a kutatás-fejlesztésbe pedig az elméleti tudás mellett a szükséges akadémiai és gyakorlati tapasztalat megszerzését is biztosítja számukra. A képzési programok a kutatás-fejlesztési programokkal kapcsolatos know-how tudásbázisára is építenek.

A Központ oktatási és képzési programja az alábbi képzéstípusokat foglalja magában:

PhD (hazai és nemzetközi posztgraduális képzés)

A képzés célja a kiemelkedő tehetségű hallgatók számára olyan továbbképzési lehetőség biztosítása, ahol az informatikai biztonság területén az élvonalba tartozó kutatásokban vehetnek részt, illetve olyan átfogó szakképesítést kapnak, amelyen keresztül az informatikai biztonság és adatvédelem területén kiemelkedő elméleti tudású szakértőkké válhatnak. A PhD képzés hosszabb távon a hasonló területen tevékenykedő más EU-beli egyetemi központokon keresztül - kooperáció keretében - külföldre is kiterjed. A PhD képzésben az első hallgatók már eredményesen dolgoznak, a korábbi eredményekre alapozva 3 diplomavédés is történt ebben az időszakban.

Iskolarendszerű, felsőfokú informatikai biztonsági szakemberképzés alapképzésben (BSc) és mesterfokú (MSc) képzésben egyaránt

Az informatikai biztonság hangsúlyának növekedése, illetve ezzel párhuzamosan a megfelelően képzett szakemberek iránti növekvő igény indokolja az - iskolarendszerbe illeszkedő - kétszintű felsőfokú képzések elindítását. A Központban zajló tudományos tevékenységek, illetve ezek eredményei is garanciát jelentenek a magas színvonalú szakemberképzésre. Jelenleg ezekből a képzésekből egy informatikai biztonsággal foglalkozó BSc szak indult el, az MSc szak tantervei és előadásai is elkészültek, ez a képzési rész a MAB akkreditációjára vár. A tantervekben a témakör legkorszerűbb ismereteit oktatjuk, különös tekintettel a nemzetközi szinten is releváns információkra, elméleti és gyakorlati eredményekre.



Szakmai tréningek, felnőttképzés

A szervezetek számára nemcsak az informatikai biztonsági szakemberek szaktudása fontos, hanem az informatikai biztonság általános tudatosítása is kiemelt cél. Ennek megfelelően kerülnek kialakításra - rendszeres, illetve igény szerint eseti jelleggel - a szakmai tréningek, felnőttképzési programok. Az elkészített anyagok nagyban építenek a Központ kutatás-fejlesztési eredményeire és a résztvevő konzorciumi partnerek, az egyetem és az ipari partnerek felnőttképzési tapasztalataira.

A Központ az oktatási, képzési programhoz szorosan kapcsolódva a következő tevékenységeket folytatja:

- Az informatikai biztonság társadalmi tudatosítása, kommunikációja



A futurIT a technikai fejlődéssel együtt növekvő informatikai biztonsági kockázatokkal kapcsolatos ismereteket, védekezési technikákat, javaslatokat a tudományos eredmények publikációjával, bemutatók szervezésével kommunikálja abból a célból, hogy a társadalomban tudatosítsa a lehetséges veszélyeket.

- Konferenciák szervezése

A tudományos eredmények jobb kihasználása, hasznosítása céljából, illetve a társadalmi tudatosítás előmozdítására a Központ rendszeresen szervez a terület vezető hazai és külföldi elméleti és gyakorlati szakértőinek részvételével konferenciákat.

tudatosítás

3. Az informatikai biztonság fontosságának kommunikációja és társadalmi tudatosítása, hazai szakmai színvonalának emelése

A futurIT projekt célja az, hogy a tudományterület és az iparág vezető elméleti és gyakorlati szakembereinek kiemelkedő szintűképzésével világszínvonalú informatikai biztonsági eljárások, módszertanok és eszközök kidolgozásával, illetve gyakorlati hasznosításuk támogatásával a Közép-Dunántúli Régió, Magyarország és Közép-Európa vezető informatikai biztonsági kutató, fejlesztő és képzési központjává váljon. Tevékenysége az alapkutatástól egészen a spin-off cégekben realizált termékértékesítésig terjed. Ellett az informatikai biztonság nemzetközi tudásbázisává és konferenciaközpontjává kíván válni. A futurIT hozzájárul a hazai innováció és K+F kapacitás növeléséhez, a szakképzésen keresztül tudásintenzív kis- és középvállalatok számára teremt munkaerőt. A spin-off vállalkozások és a konzorciumi tagok saját K+F tevékenysége révén a képzett munkaerő számára pedig megfelelő munkalehetőséget biztosít.

A futurIT oktatási és képzési programmal a Pannon Egyetem Műszaki Informatika Kara a műszaki informatika hosszú távon is fontos területein élvonalbeli ismeretek megszerzését teszi lehetővé hallgatóinak, és csúcstechnológiai kutatási témát biztosít a PhD hallgatók számára. A Központ alap- és alkalmazott kutatási munkák segítségével az együttműködő partnereket, a régió vállalkozásait juttatja értékesíthető termékekhez, szolgáltatásokhoz, ezzel új munkahelyek teremtését is segíti. A Tudásközpont az elért eredményeket tudományos szakmai publikációk és konferenciák mellett a termékein és a külföldi hallgatókon keresztül mutatja be hazai és nemzetközi viszonylatban egyaránt. Szakmai konferenciák mellett hazai és nemzetközi workshopokat is rendez, valamint megjelentet egy,

a témakör aktuális eredményeit bemutató szakmai folyóiratot is.

A futurIT kutatás-fejlesztési és képzési programjai az informatikai biztonság szempontjából alapvetően háromféle feladat megoldására koncentrálnak: az információ elvesztésének (megsemmisülésének) megakadályozására, az információ illetéktelen kézbe kerülésének megakadályozására, illetve az üzletmenet-folytonosság biztosítására. A futurIT amellet, hogy törekszik az egyediségből adódó előnyök kiaknázására, hosszabb távon neves hazai és külföldi oktatási intézmények, illetve nemzetközi szakmai egyesületek, szakhatóságok, vállalkozások részvételével egy olyan nemzetközi kapcsolati hálót alakít ki maga körül, melynek segítségével a képzési program minősége, elismertsége és hozzáférhetősége tovább növelhető, a K+F tevékenységek kibővíthetők, és az eredmények gyakorlati hasznosítása a régió illetve az országhatárokon kívül is lehetővé válik.

A Tudásközpont tevékenysége az informatikai biztonsági módszertanok kidolgozásával, eszközök kifejlesztésével, a tudásintenzív iparágak fejlődésének segítségével, a K+F kapacitások koncentráálásával, ezen keresztül a versenyképesség növelésével az Európai Unió jelenlegi kutatási keretprogramjához (EU FP 7) is illeszkedik.

Különösen az alábbi, napjainkban világszerte és az EU-ban is kiemelten kezelt biztonsági témakörökben számítunk neves nemzetközi partnerekre:

- Infrastruktúrák és szolgáltatások védelme
- A biztonság és a működés helyreállítása vészhelyzetben
- Biztonsági rendszerek integrációja és interoperabilitása
- Biztonság és társadalom
- Biztonsági kutatások koordinációja és strukturálása

INDIKÁTOROK



disszertáció

PhD disszertációk

2007-ben 3 hallgató Ph.D. disszertációja készült el, doktori tevékenységük legfontosabb adatait a következő táblázat tartalmazza:

Név	Témakör	Intézmény	Témavezető	Védés időpontja
Ludik Péter	A virtuális tanulási környezet kialakításának és bevezetésének módszertani és technikai lehetőségei	Eötvös Lóránt Tudományegyetem Informatikai Kar Információs Rendszerek Tanszék	Remzsó Tibor Pannon Egyetem	2007 május
Major Andrea	Information Visualization	Eötvös Lóránt Tudományegyetem Informatikai Kar Információs Rendszerek Tanszék	Remzsó Tibor Pannon Egyetem	2007 június
Heckl István	Szétválasztási hálózatok szintézise: különböző tulajdonságokon alapuló szétválasztási módszerek egyidejű alkalmazása	Pannon MIK Számítástudomány Alkalmazása Tanszék	Friedler Ferenc Pannon Egyetem	2007 június

Eredményeik várhatóan alkalmazásra kerülnek a projekt különböző fázisaiban. A virtuális tanulási környezet témakör (Ludik Péter) elektronikus oktatási rendszereink kialakításában, valamint a felnőttoktatási anyagok terjesztésében használható. Hasonlóan az információk megjelenítésével kapcsolatos eredmények (Major

Andrea) az oktatási alkalmazások elkészítésében és az elkészített anyagok terjesztésében alkalmazhatók. Heckl István eredményei az oktatási tevékenységben és optimális hálózati (pl. információbiztonsági) alkalmazások kialakításában használhatók.

egyetemi kutatók

PhD, posztdoktori, egyetemi kutatói állások

A Pannon Egyetem Informatikai Tudományok Doktori Iskolájában 2006-os tanévtől szerepel a meghirdetett PhD témák között az informatikai biztonság. A téma tartalma biztonsági rendszerek matematikai leírására, szintézisére, minősítésére és továbbfejlesztésére szolgáló módszertan megalkotása. A Pannon Egyetemen jelenleg két ösztöndíjas PhD hallgató és két abszolutóriummal már rendelkező PhD jelölt dolgozik e témán. Munkájuk része az üzleti folyamatok és azokat támogató információs rendszerek formális leírása, modellezése; meglévő információbiztonsági minősítő eljárások és a folyamattervezési eljárások kapcsolatának meghatározása; algoritmikus módszer kidolgozása üzleti folyamatok

információbiztonsági szempontból optimális szintézisére; a kidolgozott szintézis eljárás és a meglévő biztonsági minősítő eljárások eredményeinek összevetése.

A biztonsági rendszerek elméleti háttérének kidolgozásán részmunkaidőben több matematikai modellezésben jártas kutató dolgozik. Maros István az operációkutatás nemzetközi híró professzora - aki az Imperial College Londonból tért vissza Magyarországra - tudásával szintén a futurIT kutatásait támogatja. Maros Istvánt egy Jedlik pályázat megvalósításának részeként tudtuk visszahozni Magyarországra, 2006 szeptemberétől a Pannon Egyetem Műszaki Informatikai Karán professzor.



hallgatók

Hallgatói együttműködés program



A hallgatói együttműködés program célja, hogy bevonja a legrátermettebb egyetemi hallgatókat a kutatás-fejlesztési tevékenységekbe. Ez lehetőséget nyújt számukra, hogy megismerkedjenek a futurIT-ban folyó világszínvonalú fejlesztési tevékenységekkel, illetve, hogy alkalmassá válhassanak arra, hogy az egyetem elvégzése után magas szintű szakmai tevékenységet végezzenek. A program egy szigorú kiválasztási procedúrával indul, amely alkalmas arra, hogy felmérhessük a jelentkező hallgatók elkötelezettségét a kutatás-fejlesztési tevékenységek iránt, megismerhessük személyes képességeiket, szorgalmukat, munkabírásukat, pontosságukat, a projekt tevékenységekbe való bekapcsolódásuk lehetséges

színvonalát. Természetesen a programba bekapcsolódó hallgatóktól magas szintű egyetemi tanulmányi eredményeket és biztos angol nyelvtudást is várunk, valamint szakmai elkötelezettséget az információbiztonsági témakörök iránt. Mindezek szükségesek ahhoz, hogy képesek legyenek megfelelni a projekt magas szakmai színvonalának és célkitűzéseinek. A hallgatói együttműködés program az abban részt vevő hallgatók számára a szakterületen úttörőnek számító kutatási lehetőségeket teremt, ugyanakkor az innen kikerülő publikációkon, kommunikáción keresztül kiemelt hangsúlyt helyez az informatikai biztonság és a kapcsolódó kérdések társadalmi tudatosítására is. A program szervesen kapcsolódik a Pannon Egyetem MIK egyedülálló tehetséggondozási rendszeréhez is. A két kutatási programban - Adatmentés Technológiai és Integrált Biztonsági termékcsalád fejlesztése - résztvevő kiválasztott 11 hallgató ez év elején kezdte meg a közös munkát.



verseny

A futurIT által támogatott 24 órás programozási verseny

(Pannon Egyetem Műszaki Informatikai Kar, 2007. március 27-28)

A Pannon Egyetem Műszaki Informatikai Kara hagyományosan arra törekszik, hogy miközben nagy számban képez jó informatikai szakembereket, a kiválóknak kiemelkedési lehetőséget is biztosít. Ennek egyik eszközét jelentik a különböző szakmai versenyek. Az ilyen alkalmak lehetőséget biztosítanak arra, hogy a résztvevők a tanórától eltérő körülmények között bizonyítsák szakmai hozzáértésüket és rátermettségüket rövid határidejű, komplex gyakorlati feladatok megoldásával.



Az idei versenyfeladat fókuszában az állt, hogy szembesítse a hallgatókat egy napjainkban egyre aktuálisabb, gyakorlati, informatikai biztonsági kérdéssel: mennyi idő szükséges ahhoz, hogy információt lopjunk egy olyan számítógépről, amelynek egyetlen kommunikációs csatornája a monitor, és egy vele szemközt lévő kamera.

A hallgatóknak huszonnégy óra alatt kellett a kihívást megoldaniuk, amelyhez a hardveres eszköztár rendelkezésre állt, de a szoftvert magát a versenyzőknek kellett megírniuk, vagy az internetről ösz-

szegyűjteniük. A kérdés megválaszolásához valós tesztkörnyezet optimális kialakítását is el kellett végeznie a versenyre összeállt hallgatói csapatoknak. Az összevetés során a résztvevőknek öt-öt perces elméleti, illetve megoldásaiknak éles, működés közbeni bemutatóját kellett megtartaniuk. A győztes csapatok tagjai közül jónéhányan azóta a futurIT keretein belül kutatási és fejlesztési feladatok megoldásán is dolgoznak.



A versenyt támogatta a Pannon Egyetem, a KÜRT Zrt., a futurIT, az Oktatási Minisztérium, a Siccontact Kft és a Continental Teves Magyarország Kft.

További információk: <http://www.irt.vein.hu/verseny/>

Felnőttképzés



A felnőttképzési program keretében, 2006. októberében és decemberében, a KÜRT 3 napos gyakorlati informatikai kockázatmenedzsment képzéseket szervezett az IQSOFT John Bryce

Oktatóközponttal karöltve. A képzésen részt vevő, elméleti tudással rendelkező szakemberek tucatnyi kockázatkezelési projekt gyakorlati tapasztalataival ismerkedhettek meg. A képzés fókuszában az elméleti háttér áttekintése, a kockázatmenedzsment megvalósítása, a lehetséges hibák és elkerülésük definiálása, a nehézségek és áthidalási módjuk elemzése, valamint gyakorlati esettanulmányok feldolgozása és megoldása álltak.

A képzés célja az volt, hogy bemutassa a kockázatmenedzsment gyakorlati alkalmazását az elméleti ismeretekkel rendelkező szakemberek és döntéshozók számára. A foglalkozások során elsősorban nem az elméleti ismeretek, hanem a nehézségek és azok lehetséges megoldásai kerültek kiemelésre, ugyanakkor a kapcsolódó szabályozási tevékenységgel együtt járó ún. „papírmunka” elvégzésének jelentősége is értelmet nyert.

A képzés során a kockázatmenedzsment megvalósításához kapcsolódó munkaanyagok összeállításának és használatának begyakorlására is lehetőség volt.

A képzés előadói a KÜRT évtizedes gyakorlati tapasztalatokkal rendelkező vezető szakemberei (Oroszi Norbert, Papp Attila és Frész Ferenc) voltak.

A megvalósított képzés az alábbi tematika szerint épült fel:

Első nap - Egy informatikai rendszer állapotának felmérése:

- Projektindítás (az informatikai oldalon)
- Az informatikai technológia vizsgálata
- Az informatikai folyamatok vizsgálata
- Releváns fenyegetettség vizsgálat

Második nap - Az üzleti oldal elvárásainak felmérése:

- Projektindítás (az üzleti oldalon)
- A felmérés gyakorlati eszközei
- Paraméterek meghatározása
- Az informatika nélküli élet biztosítása

Harmadik nap - Az optimális biztonsági szint kialakítása:

- A projekt lebonyolítása
- Értékelési skálák
- Az optimális kockázati szint meghatározása
- A kockázatmenedzsment élete egy szervezetben

transzfer

Technológiai transzfer

A technológia transzfer célja, hogy a futuriT keretében létrejövő eredmények hasznosításáról, illetve a futuriT számára szükséges, a világban már létező eredmények meghonosításáról gondoskodjon. A futuriT technológia transzfer tevékenysége a Tudásmenedzment laboratórium munkájára épül, amely a projektek keretében megvalósított kutatási programok szakmai eredményeinek összefogását és a létrehozott „best practice” ismeretek publikálását végzi. A technológia transzfer célcsoportjai és az átadás folyamatának technikai a különböző típusú kutatás-fejlesztési eredmények esetén merőben eltérnek egymástól. Az alap kutatási eredményeket publikációjukkal és az eredményeikre épülő módszertanokkal hasznosítja a futuriT. Az alkalmazott kutatás-fejlesztési és termékfejlesztési eredményeket a kutató-fejlesztő laboratóriumok nem önmaguk értékesítik, hiszen ők a termékek fejlesztéséhez értenek legjobban, abban van komparatív előnyük. Ezért hoz létre a futuriT a termékek értékesítésére spin-off vállalkozásokat. E spin-off vállalkozások a termékek értékesítéséhez szükséges tudományos kompetenciát az egyetemről, míg az üzleti és szakmai kompetenciát az üzleti szférában tevékenykedő konzorciumi part-

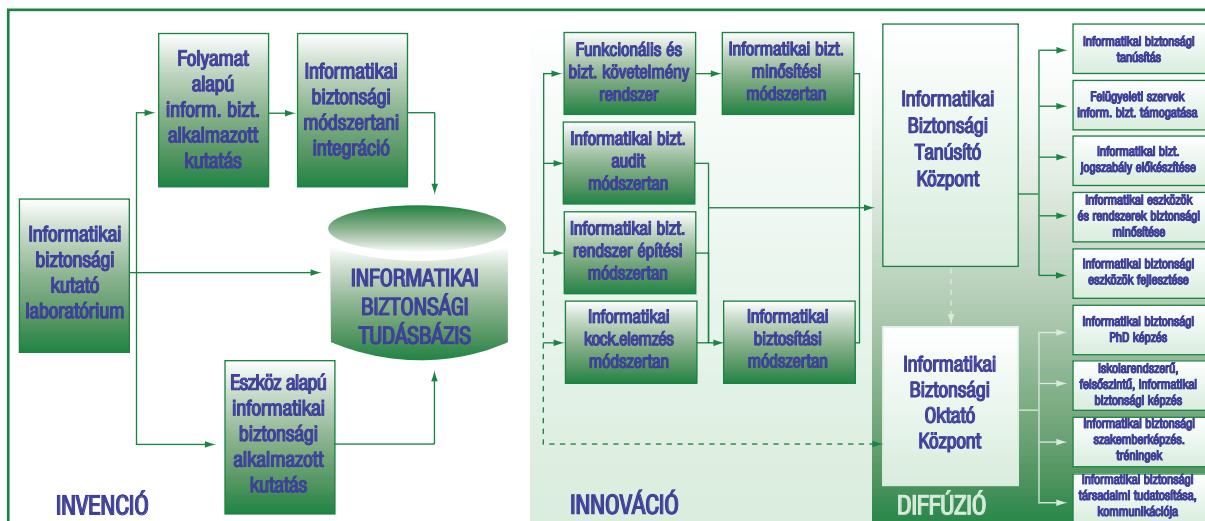
nerek szakembereitől szerzik meg.

Az előállított módszertanok, szoftver és hardver termékek jól értékesíthetők az alprojektek technológiáit hasznosító nagyvállalatok számára. Így az eredmények egyaránt piacra kerülhetnek Magyarországon, az Európai Unióban és világszerte. Jó példa erre a laborok eredményeit felvásárolni szándékozó európai-amerikai-közel-keleti biztonsági nagyvállalkozás, az Alacera International (www.Alacera.com) 2007. júniusában aláírt szándéknyilatkozata a futuriT-tal.

A későbbiekben a spin-off vállalkozások értékesítése a vállalkozások életciklusának különböző szakaszaiban különböző célcsoportok számára lehetséges.

Az induló spin-off vállalkozások alaptőkeigényét úgynevezett „üzleti angyal” befektetők számára kívánjuk elsősorban promótálni. Ebben az esetben egy alacsony befektetési hányadért alacsony üzlet rész átadása történik meg.

A befutott - már némi referenciával rendelkező - spin-off vállalkozásokat szakmai befektetők és kockázati tőkések számára kívánjuk elérhetővé tenni, így vonva be jelentős tőkét a megkezdett fejlesztések hosszú távú fenntarthatóságának biztosítására.



Konferenciák

2006. november 23-án került megrendezésre Budapesten az Intelligens Rendszerek - **Fiatalkutatók Szimpóziuma 2006** c. konferencia, melynek szervezője a NJSZT Mesterséges Intelligencia szakosztálya volt. Az MTA SZTAKI Kende utcai nagytermében megrendezett egynapos szimpózium célja az volt, hogy áttekintést adjon az intelligens rendszerek elméleti és gyakorlati kérdéseivel foglalkozó kutatók munkáiról - ennek kapcsán betekintést adjon a vonatkozó hazai műhelyek jelenlegi helyzetébe, és megvitassa azokat a kihívásokat és problémákat, amelyekkel a kutatók, az oktatók és az üzleti szférában munkálkodó kollégák találkoznak. A konferencián a PE MIK kutatói a Sokügynökös rendszerek és alkalmazások szekcióban ismertették eredményeiket, a nagy érdeklődésre számot tartó előadás címe a következő volt: Kombinatorikusan gyorsított korlátozás és szétválasztás algoritmus biztonsági rendszerek szintézisére. A szimpózium továbbá jó alkalmat biztosított eredményeink és kutatási munkánk megvitatására.

A KÜRT „**Hej! Réáérünk arra még?**” Az üzleti folyamatok és az információmenedzsment (v)iszonya címmel rendezett nagy sikerű szakmai konferenciát 2007. május 17-én. A konferencia célja az volt, hogy felhívja a figyelmet az üzlet és az informatika közti kommunikáció javításának szükségességére, annak érdekében, hogy az informatika optimálisan tudja támogatni a vállalatot, szervezetet üzleti céljainak megvalósításában. A KÜRT ennek keretében bemutatta a futurIT első munkaszakaszának eredményeire épülő azon új üzleti megoldásait és portfólió elemeit, amelyek segítségével a fenti kapcsolatok erősítése megvalósíthatóvá válik.

A Magyar Operációkutatási Társaság, a Bolyai János Matematikai Társaság és a Gazdaságmodellezési Társaság 2007. június 7-9. között rendezte Balatonőszödön a **XXVII. Magyar Operációkutatási Konferenciát**, melyen elsősorban az operációkutatás elméleti ill. módszertani területeivel foglalkozó kutatók vettek részt. A konferencia szervezőbizottsága kiemelt jelentőséget tulajdonított az alkalmazások, esettanulmányok bemutatásának, a gyakorlatban megvalósult vagy megvalósulás alatt lévő operációkutatási eredményekről szóló előadásoknak. A konferencián a PE MIK kutatói biztonsági rendszerek leírására és optimalizálására felépített modelljüket ismertették a P-gráf módszertan alkalmazásai szekció keretein belül; az előadás címe P-gráf módszertan alkalmazása biztonsági rendszerek leírására és szintézisére volt. A konferencián lehetővé vált a felépített matematikai modell szakmai megméretése, amely az eddigi kutatások fontos mérföldkövét jelentette.

Veszprémi Optimalizálási Konferencia: Korszerű Algoritmusok (VOCAL 2006) angolul: Veszprém Optimization Conference: Advanced Algorithms (VOCAL), Veszprém, 2006. december 13-15.

A VOCAL konferencia az optimalizálási algoritmusokhoz kapcsolódó legújabb eredményeket ismerteti a nemzetközi szakmai közösség által elismert kutatók előadásában. Az előadások áttekintik a folytonos és diszkrét optimalizálás jelenlegi helyzetét, beleértve az algoritmusok komplexitását és konvergencia tulajdonságait, valamint az alkalmazási területeket. A rendezvény célja lehetőséget teremteni az elméleti és a gyakorlati területen dolgozó kutatók és fejlesztők találkozására, ismereteik megosztására rangos nemzetközi konferencia keretében.

A konferencián megjelenő előadások a javasolt optimalizáló módszerek elméleti matematikai háttere mellett bemutatják azok mérnöki alkalmazási területeit is. Ilyen területek például az összetett ipari folyamatok, logisztikai ellátó láncok, információ biztonsági rendszerek tervezése, irányítása és kockázatelemzése.

Pannon Egyetem, Műszaki Informatikai Kar
MTA Veszprémi Területi Bizottsága (VEAB)

Meghívott előadók

- Lorenz T. Biegler, Department of Chemical Engineering, Carnegie Mellon University
- Hans Georg Bock, Interdisciplinary Center for Scientific Computing (IWR), University of Heidelberg
- J. Frederic Bonnans, The French National Institute for Research in Computer Science and Control (INRIA)
- Dorit S. Hochbaum, Haas School of Business and Department of IE&OR, Etcheverry Hall, University of California
- Etienne de Klerk, Department of Econometrics and Operations Research, Faculty of Economics and Business Administration, Tilburg University
- Yurii Nesterov, Center for Operations Research and Econometrics (CORE), Catholic University of Louvain (UCL)
- András Prékopa, Rutgers Center for Operations Research (RUTCOR), Rutgers, The State University of New Jersey
- Annick Sartenaer, Departement of Mathematics, Notre-Dame de la Paix University (FUNDP)

Résztevők

A 2006 évi konferenciára négy kontinens számos országából adtak be kutatók előadásokat (Algéria, Belgium, Dél-afrikai Köztársaság, Egyesült Államok, Egyesült Királyság, Észak-Ciprus, Franciaország, Hollandia, India, Irán, Kanada, Magyarország, Nigéria, Norvégia, Szlovénia, Törökország)

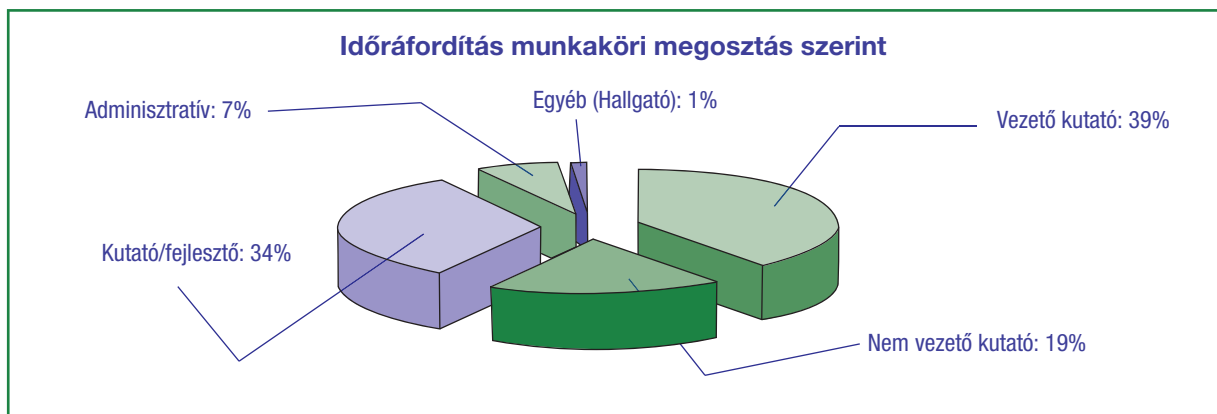


erőforrás

Erőforrások időráfordítása

Meghatározó személy	Konzorciumi tag	Feladatok	Ráfordított idő (nap)
Vezető kutató			
Dr. Kürti Sándor	KÜRT Zrt	II/1,2; III/2	100
Homola Zoltán	KÜRT Zrt	II/3; III/2	100
Kmetty József	KÜRT Zrt	II/1,2; III/2	100
Kürti János	KÜRT Zrt	II/1,2; III/2	100
Papp Attila	KÜRT Zrt	II/3; III/2	100
Remzsó Tibor	Pannon Egyetem	II/1,2; III/2	75
Bertók Botond	Pannon Egyetem	IV/2,3	50
Friedler Ferenc	Pannon Egyetem	IV/2,3	25
Terlaky Tamás	Pannon Egyetem	IV/2,3	20
Thokozani Majozsi	Pannon Egyetem	IV/3	13
Kovács Zoltán	Pannon Egyetem	II/3	10
Maros István	Pannon Egyetem	II/1,2; III/2	10
Simon Gyula	Pannon Egyetem	IV/2,3	10
Tuza Zsolt	Pannon Egyetem	IV/2,3	10
Dominich Sándor	Pannon Egyetem	II/1,2; III/2	5
Góth Júlia	Pannon Egyetem	II/1,2; III/2	5
Lakner Rozália	Pannon Egyetem	II/1,2; III/2	5
Nem vezető kutató			
Hamos Krisztián	KÜRT Zrt	II/1,2; III/2	100
Kertész Zoltán	KÜRT Zrt	II/1,2; III/2	100
Kovács Ferenc	KÜRT Zrt	II/1,2; III/2	75
Michael Wellington	KÜRT Zrt	II/1,2; III/2	75
Kutató/fejlesztő			
Megyeri István	KÜRT Zrt	II/1,2; III/2	100
Nemkin Róbert	KÜRT Zrt	II/1,2; III/2	100
Szekeres Gábor	KÜRT Zrt	II/1,2; III/2	100
Kürti Tamás	Pannon Egyetem	IV/2,3	75
Adonyi Róbert	Pannon Egyetem	IV/2,3	37
Halász László	Pannon Egyetem	IV/2,3	30
Keresszegi Attila	Pannon Egyetem	IV/2,3	30
Kalauz Károly	Pannon Egyetem	IV/2,3	25
Sarkadi Károly	Pannon Egyetem	IV/2,3	25
Süle Zoltán	Pannon Egyetem	IV/2,3	25
Tarczali Tünde	Pannon Egyetem	IV/2,3	25
Ujvári Orsolya	Pannon Egyetem	IV/2,3	25

Meghatározó személy	Konzorciumi tag	Feladatok	Ráfordított idő (nap)
Kristóf Orsolya	Pannon Egyetem	IV/2,3	13
Stahl Anita	Pannon Egyetem	IV/2,3	13
Raffai Csilla	Pannon Egyetem	IV/2,3	6
Adminisztratív			
Cziráki Katalin Virág	KÜRT Zrt		50
Sárosi Júlia	KÜRT Zrt		50
Blaskó Tímea	KÜRT Zrt		25
Egyéb (Hallgató)		II/3	
Összesen			26
Összesen:			1867
Teljes munkaidőre átszámított kutatói létszám			7.78 fő



2006-2007

Teljesítmény indikátorok 2006-2007

Mutató/publikáció	Terv	Tény
Hazai publikációk	25db	
szakmai		6db
általános		48db
Nemzetközi publikációk	1pcs	
szakmai		2db

Mutató/állások	Terv	Tény
PhD kutatói állás	6db	6 fő
Posztdoktori állás	4 fő	4 fő
Egyetemi kutatói jobs	5 fő	7 fő
PhD doktori disszertáció	3 fő	3 fő
BSc és MSc képzésben résztvevők száma	20 fő	20 fő
Felnőttképzésben résztvevők száma	20 fő	14 fő

Mutató/szakmai rendezvények	Terv	Tény
Konferencia előadások száma	25db	26db
Konferenciák száma	3db	2db KÜRT 2007 Conference Veszprém Optimization Conference: Advanced Algorithms (VOCAL)

Média szereplések

RET szakmai

2006.11.23 • **Süle Z., Bertók B., Friedler F.** • Kombinatorikusan gyorsított korlátozás és szétválasztás algoritmus biztonsági rendszerek szintézisére, Intelligens Rendszerek Fiatal Kutatók Szimpóziuma • SZTAKI

2007.06.07-09. • **Süle Z., Bertók B., Friedler F.** • P-gráf módszertan alkalmazása biztonsági rendszerek leírására és szintézisére • XXVII. Magyar Operációkutatási Konferencia, Balatonőszöd

2007.05.01 • **Simon, G., M. Molnár, L. Gönczy, B. Cousin** • Dependable k-coverage algorithms for sensor networks • CD-ROM ISBN 1-4244-1080-0 Proceedings of the Instrumentation and Measurement Technology Conference - IMTC 2007

2007.10.15-17. • **Simon, G., L. Szabados, A. G. Tóth** • Model based code generation for fast-deployment security applications • 2nd International Workshop on Secure Information Systems (SIS'07), Wisla, Poland

2006.11.22 • **Papp Attila** • Biztonsági megoldások integrációja • Hadmérnök különszám 2006

2007.05.08 • **Papp Attila** • Sárkány ellen sárkányfű • Computerworld XXXVIII évf 19 sz

2007.05.08 • **Papp Attila** • Biztonsági megoldások integrációja • Computerworld XXXVII évf 40 sz

Média szereplések

RET PR

2006.02.16 • **Kürti Tamás** • Veszprémi tudásközpont • Gazdasági Rádió

2006.02.16 • **Kürti Sándor, Kmetty József, Dr. Gaál Zoltán** • Piac & Profit • Biztonságosabb információkezelés • Piac & Profit

2006.02.17 • **Kmetty József** • Egyetemmel fejleszt a KÜRT • Népszabadság

2006.02.17 • **Kürti Sándor, Kmetty József, Kürti Tamás, Dr. Gaál Zoltán, Dr. Friedler Ferenc** • Kutatók a biztonságért - A KÜRT Zrt. és a Veszprémi Egyetem informatikai együttműködése • Veszprém Megyei Napló

2006.02.21 • **Dr. Gaál Zoltán, Kmetty József** • Információbiztonsági Kutató-Fejlesztő Központ nyit a KÜRT és a Veszprémi Egyetem együttműködésében. (www.terminal.hu) • www.terminal.hu

2006.03.02 • **Kürti Tamás, Dr. Gaál Zoltán** • Csúcsbiztonságban az információ • Népszabadság

2006.05.19 • **Boda Miklós, Kürti Tamás, Beck György** • A támogatáshoz eredmény kell • NKTH

2006.06.01 • **Dr. Friedler Ferenc** • Hozzájárul a régió fejlődéséhez • Veszprém Megyei Napló

2006.08.03 • **Kürti Sándor** • Veszprémi tudásközpont •

2007.02.25 • **Kürti Tamás** • Mint egy amerikai álom - idehaza (Veszprém Megyei Napló, 2007. február 25.) • Veszprém Megyei Napló

2007.04.18 • **Kürti Tamás, Friedler Ferenc** • RET • Napló

2007.04.18 • **Kürti Sándor** • K+F központok • Menedzsment Fórum- Staféta

2007.04.18 • **Dr. Friedler Ferenc, Kürti Tamás, Dr. Rédey Ákos** • Tudásközpont alakult • Veszprém Megyei Napló

2007.05.10 • Veszprém Megyei Napló • Egyetem a programban • Veszprém Megyei Napló

2007.06.08 • **Kürti Tamás, Tóth G. Árpád, Friedler Ferenc** • Tsec • Napló Online

2007.06.08 • **Kürti Tamás, Tóth G. Árpád, Friedler Ferenc** • Amerikai-magyar együttműködés - Biztonságtechnikai fejlesztőközpont alakul • Veszprém Megyei Napló

2007.06.11 • **Kürti Tamás, Tóth G. Árpád** • Tsec • Computerworld online, Hirtv.hu, HWSW.hu, IT.News, Híradó.hu, Menedzsmentforum, PC World, Portfolio.hu, Prímonline, Terminal, MTI, Eduport.hu, Infolilág, Euroastra

2007.06.11 • **Kürti Tamás, Tóth G. Árpád, Friedler Ferenc** • Új biztonsági fejlesztő központ az Alacera International, a KÜRT és a Pannon

Média szereplések

Egyetem együttműködésében • EuroAstra Internet Magazin

2007.06.12 • **Kürti Tamás, Tóth G. Árpád, Friedler Ferenc** • Tsec • Piac & Profit Online, Infomedia, Origo, Biztonságportál, Computerworld, HR Portál, Veszéprém index, Világgazdaság online, Tranzit-hu, aHírek.hu

2007.06.14 • **Kürti Tamás** • Napi Gazdaság/Girnt József • Tsec • Napi Gazdaság

2007.06.14 • **Kürti Tamás, Tóth G. Árpád, Friedler Ferenc** • Tsec • Metro

2007.06.14 • **Kürti Tamás, Friedler Ferenc** • Tsec • FM Portál

2007.06.16 • **Kürti Tamás, Friedler Ferenc** • Tsec • Webbusiness

2007.06.19 • **Kürti Tamás** • Kováxs M. Veronika./Metro • Tsec, Pannon Egyetem/Biztonságtechnika • Metro

2007.06.21 • **Kürti Tamás** • Tsec • Echo TV

2007.06.21 • **Kürti Tamás, Friedler Ferenc** • Tsec • Echo TV

2007.06.21 • **Kürti Tamás, Dr. Friedler Ferenc, Tóth G. Árpád** • Új technológiai centrum alakul • METRO

KÜRT szakmai

2006.01.11 • **Csász László** • Sláger Rádió, Bochkor Gábor • Adatmentés a Nasa-nal • Sláger Rádió

2006.01.13 • **Dolánszky György** • Szilvay Balázs • péntek 13 vírus • Kossuth Rádió

2006.01.19 • **Molnár Géza** • Beregi Nagy Edit • Miért lesz egyre kevesebb a CD, DVD élettartama • Info Rádió

2006.01.19 • **Kmetty József** • Kárász Róbert • Van-e jelenleg biztos védekezési forma a hackerek ellen? • Echo TV

2006.01.23 • **Kürti Sándor, Molnár Géza** • Kálmán Alida • Miért lesz egyre kevesebb a CD, DVD élettartama • Duna TV

2006.01.23 • **Molnár Géza** • Lukács Csaba • Adathordozók - adatvesztési arányok • Magyar Nemzet

2006.01.23 • **Dolánszky György** • Girnt József • Ingyen telefonálás - Skype • Napi Gazdaság

2006.01.26 • **Dolánszky György** • Obrusánszky Borbála • Internetes veszélyek • Privát Kopó Magazin

2006.02.02 • **Kmetty József** • Bárány Róbert • CD adamentés kérdőjelei • TV2

2006.02.17 • **Kürti Sándor** • Kósa Melinda • Fidesz feltrökte az MSZP szerverét • "M1, M2"

média

Média szereplések

- 2006.02.17 • **Kürti Sándor** • Havas Henrik • Fidesz feltörte az MSZP szervert • TV2
- 2006.06.14 • **Kürti Sándor** • Esti Judit • integrált információbiztonság • Kossuth Rádió
- 2006.06.15 • **Kürti Sándor** • Fehér Mariann • Fidesz feltörte az MSZP szervert • Klub Rádió
- 2006.08.12 • **Molnár Géza** • Viharos adatvesztés • Info Rádió
- 2006.08.14 • **Frész Ferenc** • Litauszky Balázs • Biometrikus kódok • Info Rádió
- 2006.08.22 • **Kürti Sándor** • Bercsény Luca • Finn rendelkezés a dolgozók e-mailjeinek vállalati ellenőrzéséről, - a vállalati e-mailek kockázatáról (adatlopás,...) • Klub Rádió
- 2007.01.10 • **Kürti Sándor Sándor, Megyeri István** • Kossuth Rádió • Adatmentés flash memoriáról • Kossuth Rádió-Digitális
- 2007.02.06 • **Dolánszky György** • “Kránit Balázs, P. Kiss Zsuzsa” • Adatvesztés / adatvédelem • Kossuth Rádió - Napközben
- 2007.02.12 • **Dolánszky György** • Kántor Endre • Radio Cafe
- 2007.04.01 • **Megyeri István, Kertész Zoltán, Kmetty József** • Flash adatmentés • M1/Delta
- 2007.04.01 • **Frész Ferenc** • Biztonsági tudatosság • Számítástechnika- CIO melléklet
- 2007.04.13 • **Kmetty József** • Átláthatóbb állam az IT révén? • IT business
- 2007.04.18 • **Molnár Géza** • Adatéség • Interfax, EuroAstra, Hírvadász, SG, Digitalege, Tranzit
- 2007.04..19 • **Molnár Géza** • Adatéség • Computerworld, Infovilág, Biztonsagportal.hu, 3hackers.hu, Hírfal.hu, Számítástechnika online
- 2007.04.20 • **Csuba Dea** • Adatmentés • Magyar Computer Club
- 2007.04.24 • **Molnár Géza** • Adatéség • IT business
- 2007.05.1 • Cebit, logelemzés • Chip
- 2007.05.15 • **Szekeres Gábor** • Adatéség • Echo Tv
- 2007.06.08 • **Kürti Sándor** • Vermes Péter/Asztallap • Adatvédelem, adatmentés • Asztallap (A Mensa Hungarica havilapja)
- 2007.06.19 • Adatmentés • Computerworld
- 2007.07.06 • **Kürti Sándor** • Lánchíd rádió/Kovács Anita • Adatmentés, külföldi terjeszkedés • Lánchíd Rádió

rendezvények

Szakmai rendezvények

RET szakmai

- 2006.12.13-15. • Veszprém Optimization Conference Veszprém, Hungary • Advanced Algorithms (VOCAL) • **Bertók Botond, Kovács Zoltán**
- 2007.05.01-03. • Proceedings of the Instrumentation and Measurement Technology Conference IMTC 2007 Warsaw, Poland • Dependable k-coverage algorithms for sensor networks • **Simon, G., M. Molnár, L. Gönczy, B. Cousin**
- 2007.06.07-09. • XXVII. Magyar Operációkutatási Konferencia • P-gráf módszertan alkalmazása biztonsági rendszerek leírására és szintézisére • **Süle Z., Bertók B., Friedler F.**
- 06.11.23 • Intelligens Rendszerek Fiatal Kutatók Szimpóziuma, Budapest, SZTAKI, • Kombinatorikusan gyorsított korlátozás és szétválasztás algoritmus biztonsági rendszerek szintézisére • **Süle Z., Bertók B., Friedler F**
- 2007.10.15-17. • 2nd International Workshop on Secure Information Systems (SIS'07), Wisla, Poland • Model based code generation for fast-deployment security applications • **Simon, G., L. Szabados, A. G. Tóth**

KÜRT szakmai

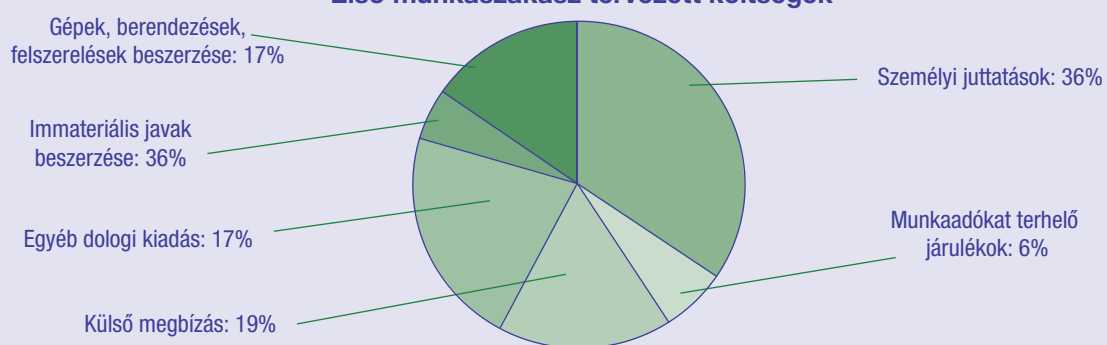
- 2006.04.13 • Microsoft • Információmenedzsment, avagy túl a képességeink határain? • **Kürti Sándor, Frész Ferenc, Zsilinszky Sándor**
- 2006.06.08. • Internethajó • 7. Európa Internethajó Magyar innováció és tudásexport az informatikában • **Kmetty József**
- 2006.09.19 • HM előadás • Információmenedzsment, avagy túl a képességeink határain? • **Kürti Sándor, Frész Ferenc, Zsilinszky Sándor**
- 2007.05.17 • KÜRT Konferencia • Az üzleti folyamatok és az információmenedzsment (v)iszonya • **Dakó Balázs, Pécsi Richárd, Bartal László, Horváth Balázs, Zsilinszky Sándor, Frész Ferenc, Oroszi Norbert, Papp Attila, Kis György**
- 2007.09.26 • Információbiztonság Napja • Biztonsági Intelligencia: Gyógymód és megelőzés az informatikában • **Kürti Tamás**

finanszírozás

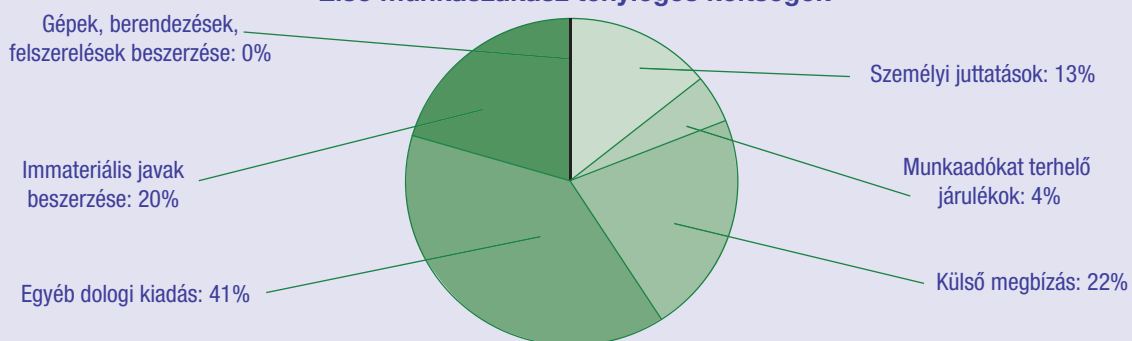
Finanszírozás, összesített pénzügyi mutatók

Költségtypusok	Terv		Összesen	Tény
	Támogatás	Saját forrás		
Személyi juttatások	44,260	42,000	86,260	20,256
Munkaadókat terhelő járulékok	14,640	0	14,640	6,564
Külső megbízás	30,000	16,000	46,000	32,722
Egyéb dologi kiadás	15,500	25,000	40,500	61,149
Immateriális javak beszerzése	12,000	0	12,000	30,675
Gépek, berendezések, felszerelések beszerzése	41,000	0	41,000	0
Összesen	157,400	83,000	240,400	151,366

Első munkaszakasz tervezett költségek



Első munkaszakasz tényleges költségek



monitoring

Monitoring adatszolgáltatás

Eredmény	
A projekt hasznosítható eredménye	
• Kifejlesztett új*	
• Termék	0db
• Szolgáltatás	0db
• technológia	0db
• alkalmazás	0db
• prototípus	0db
• Benyújtott szabadalmak száma*	
• hazai	0db
• PCT	0db
• Külföldi	0db
• Megadott szabadalmak száma	
• hazai	0db
• PCT	0db
• Külföldi	0db
• Egyéb iparjogvédelmi oltalom.(0db)* (pl: védjegy, mintaoltalom, stb.)	
Tudományos eredmények	
• Publikációk (előadásokat is beleértve)	
• hazai	54db
• nemzetközi	2db
• Disszertációk	
• PhD	3db
• MTA Doktora	0db
• Eredményezett-e új nemzetközi projektet?	IGEN (elbírálás alatt)
Emberi erőforrás	
• Oktatásban/képzésben hasznosítják-e a projekt eredményeit?	IGEN (BSc kurzusokon)
• A projektbe bevont	
• egyetemi hallgatók száma	20db
• PhD hallgatók száma	6db
• fiatal kutatók száma	6db
• A projekt révén tudományos fokozatot szerzett kutatók száma	3db
• A projekt révén létrejött munkahelyek száma	
• vállalkozásokban	0db
• kutatóhelyeken	6db
• Ebből kutatói munkahely	6db
(Megj.: teljes munkaidő egyenértékben)	
Gazdasági hasznosítás	
• A központ tevékenységében résztvevő	
• kutatóhelyek száma	3db
• vállalkozások száma	2db
• A létrejött új vállalkozások száma	0db
• A létrejött új vállalkozások árbevétele	0Ft
• Megtörtént-e a projekt eredményeinek gazdasági hasznosítása?	NEM
• Az eredményt hasznosító cég(ek) száma (db), elérhetősége	
• A projekt eredményként létrejött	
• Többlet árbevétel	0Ft
• ebből export árbevétel	0Ft
• Költségek csökkenése	0Ft
Társadalmi hasznosítás	
• A projekt hozzájárult	
• a fenntartható fejlődéshez és a környezetvédelemhez?	IGEN
• az esélyegyenlőség megvalósításához?	IGEN
• a biztonsághoz?	IGEN
• a regionális egyenlőtlenségek mérsékléséhez?	IGEN
• egyéb (I/N), mégpedig	NEM
• A projekt eredményeinek nyilvános bemutatása megtörtént-e (I/N) és milyen módon:*	
• Szakmai körökben	IGEN
(szakmai konferencia, publikációk, honlap)	
• Nagyközönség körében	IGEN
(szakmai konferencia, írott sajtóban és televízióban, rádióban, interneten)	
Egyéb, a projekt jellegéből adódó, speciális monitoring mutató	
	NINCS

Elérhetőségek

Kürti Tamás

futurIT vezető

1112 Budapest, Péterhegyi út 98

kurti.tamas@kurt.hu

Prof. Friedler Ferenc

Konzorcium vezető

8200 Veszprém, Egyetem u. 10

friedler@dcs.vein.hu

Minárovits Balázs

AlbaComp szakmai vezető

8000 Székesfehérvár, Mártírok útja 9.

info@albacomp.hu

Ilyenek vagyunk.....



futurIT Biztonsági Tudásközpont

8200 Veszprém, Egyetem u. 10. • Telefon/Fax: +36 88 624 025

A kiadvány a Pázmány Péter Program keretén belül
a Nemzeti Kutatási és Technológiai Hivatal támogatásával készült.

Kiadja a Pannon Regionális Tudásközpont - futurIT Biztonsági Tudásközpont

A kiadásért felel: Dr. Friedler Ferenc
Grafikai tervezés: Arttom Grafika
Nyomdai kivitelezés: TradeORG Nyomda

