ZSIGOVITS LÁSZLÓ

A BIG DATA MINT A RENDVÉDELEM EGYIK NAGY KIHÍVÁSA

1. Bevezetés

Az informatikai eszközök rohamos fejlődésétől elválaszthatatlan az információtechnológiák gyors ütemű előrehaladása is. Az eszközökre többek között meghatározó jellemző a méretcsökkenés mellett a több funkciósság, a mobil alkalmazhatóság és az internet használhatóság biztosítása. Az információtechnológiák ezen eszközök gyors adatátvitelét és adatfeldolgozását, a különféle hagyományos analóg adatok digitalizálását, integrálását, az óriási adatmennyiség tárolását, információként történő megjelenítését teszik lehetővé, amellyel a felhasználónak kényelmi, ergonómiai élményt nyújtanak. Alig ismerkedtünk meg az új információtechnológiával, a Felhővel[251], máris bekopogott egy újabb technológia, a Big Data.

Ezek az új információtechnológiák a mellett, hogy a felhasználóknak számos korszerű szolgáltatást nyújtanak, veszélyes kockázatokat is hordoznak magukban. A kényelmi szempontok mellett számolni kell a kiszolgáltatottság fokozódásával is. A korszerű információtechnológiákat a kiber- és szervezett bűnözés is ellenünk fordíthatja,[252] de az állam is visszaélhet[253] vele.

A Big Data ismételten egy olyan új, ugyan a felhasználónak számos előnyt nyújtó információtechnológia, amely a szervezett bűnözés kezében felmérhetetlen károkozásra alkalmas lehetőség és az állam is erősen korlátozhatja rajta keresztül az emberi szabadságjogokat.

A fentiek miatt jelent a Big Data a rendészet számára jó néhány kihívást. Egyrészt, magának a rendészetnek is alkalmaznia kell ezt az információtechnológiát, különben lemarad a kor szintjének megfelelő rendvédelem szavatolásáról, másrészt meg kell védenie az állampolgárokat a kiber- és szervezett bűnözés kártékony tevékenységétől, harmadrészt biztosítani kell, hogy egy hatósági szervezet se élhessen vissza lehetőségeivel.

2. Mi is az a Big Data?

A Big Data legegyszerűbben úgy jellemezhető, hogy óriási adatmennyiség, amely a korszerű informatikai eszközökön keresztül közvetlen kapcsolatba hozható a mindennapi életünkkel, képes azt befolyásolni. Naponta 2500 petabájtnyi[254] adat keletkezik, ez az óriási

---

[251] Zsigovits László: Rendvédelmi szervek informatikai fejlesztési lehetőségei az informatika világfejlődési trendje tükrében. Rendvédelem 2012/2. sz. 99-113. o.

[252] http://www.vg.hu/vallalatok/infokommunikacio/rohamosan-terjed-a-kiberbunozes-magyarorszag-a-10-europaban-402394 (letöltve: 2013.07.02.)

[253] Edward Snowden, az amerikai titkosszolgálatok internetes és telefonos adatgyűjtését leleplező informatikus vagy a korábbi amerikai követségek adatgyűjtési botránya.

[254] Tera 10 a 12-en, peta 10 a 15-en, exa 18-on, zetta 10 a 21-en, 10 a 100-on googl – zettabyte

adatmennyiség a Big Data - az új természeti erőforrás[255]. Az adatok sokasága a régmúltban is létezett, de főként nyomtatott formában, az egyes adathalmazok egymástól elszigetelten funkcionáltak, egy jól meghatározott kör érdekeit szolgálták. Kívülállóknak nehezen lehetett hozzáférniük. Most ez változott meg. Egyrészt az elszigetelődés megszűnt, másrészt a digitalizáció következtében, a nagy távolságban tárolt adathalmazok is kapcsolatba hozhatók egymással. Ezáltal kialakul az óriási adattömeg, a Big Data. Persze, most is vannak adatszigetek, amelyek nem nyilvánosak, de ezek is többnyire digitalizáltak, valamilyen távoli eléréssel rendelkeznek, mert egyes szervezetek használják őket. Ez pedig a hackerek számára hozzáférési esélyt jelent. Mint ez már jó néhányszor megtörtént. Kormányzati, banki adatbázisokba törtek be a kibertámadók.

A Big Data, azon kívül, hogy egy halmazba integrálja a számtalan adatféleséget, még számos más jellemzővel is bír. Az egyik, hogy nagymértékben alkalmazza a klasszikus két információszerzési mód mellett az utóbbi 5-10 évben megjelent globális elektronikai információgyűjtés módszerét is. Ez nem más, mint a térfigyelő és biztonsági kamerák felvételeinek, a műholdképeknek a digitalizálása, feldolgozása és annak a sok digitális nyomnak a felhasználása, amit naponta hagyunk magunk után[256]. A Big Data magába olvasztja ezen adatokat is, ezzel kiszélesítve az egyén teljes kiszolgáltatottságát az informatikának. Egységes, egymással kapcsolatba kerülő rendszerben léteznek a számítógépi adatok, a térinformációs- és távérzékelési adatok, a digitalizált szöveg, kép, hang, video (médiák), a digitalizált dokumentumtárak, a műhold- és térfigyelő kamera felvételek, a web, az internetes szolgáltatások, az e-mailok, a 3D szkennelés eredményei. Továbbá az a számtalan digitális nyom, amit naponta hagyunk magunk után, úgymint az internetes letöltések és kalandozások, GPS jelek, cellainformációk, háttérzaj, PIN kód, vásárlói kártya, elektronikus tranzakció, elektronikus ügyintézés bitsorozatai. Újonnan kialakuló digitális nyomokat képeznek a digitalizált biometrikus adataink. A jövőben a jelszavakat felváltják a weboldalak és szolgáltatások elérésekor az ujjlenyomat-, retina-, hang- vagy arcfelismerés alapján generált azonosítási módszerek. Az Apple kezdett ilyen kísérletekbe, megvett egy ujjlenyomat-olvasókat fejlesztő céget, hogy a közeljövőben ilyen szenzorral felszerelt iPhone-t dobjon a piacra. Kialakul körülöttünk egy digitális élettér, amelynek a haszonélvezői, de egyúttal a rabjai és kiszolgáltatottjai is leszünk.

A Big Data másik fontos jellemzője, hogy túllép az adat aggregáción, eseményekkel dolgozik, bonyolult matematikai, statisztikai, hálózatelméleti és algoritmikus elemzési módszereket alkalmazva összefüggéseket, rejtett kapcsolatokat tár fel. A hang és képelemzésen, a szokáskövetésen keresztül, felhasználva az egyéb adatokat, a proaktivitás, szinergia elveit alkalmazva, a payback és heat map technológiákkal prediktív személyiségképet alkot. Már azt is tudják rólunk, hogy mit akarunk a jövőben tenni. Keresőgépekkel, összehasonlító algoritmusokkal (plágium vadászat) az azonosságokat, kapcsolatokat tárják fel. Mindezt tetézi az adatbázisok összekötése, amely során a különböző adatbázisokban tárolt adatok között kapcsolatot lehet teremteni. Számtalan államilag létrehozott és egyéb adatbázis létezik. Ilyenek például a lakcím, gépjármű, bűntettesi, egészségügyi, társadalombiztosítási, képzési adatbázisok. Ezen kívül még jó néhány, legálisan létrehozott, cégszintű adatbázis van. Némelyekben személyes adatokat is

[255] IBM Storage Forum 2013. Adatból információ konferencia. Budapest, 2013. február 28. Forrás: http://www-03.ibm.com/systems/hu/storageforum2013/video.html (letöltve: 2013.07.02.)
[256] Zsigovits László: Az új Nemzeti Közszolgálati Egyetem K+F+I és pályázati tevékenységének lehetséges irányai Hadmérnök 2011/2. sz. Vö: http://www.hadmernok.hu/2011_2_zsigovits.php (letöltve: 2013.07.02.)

nyilvántartanak. Martin Spitz Ted kiderítette, hogy milyen adatokat tárol róla a szolgáltató, 35 000 sor információt gyűjtöttek össze vele kapcsolatban.[257]

A Big Data mindezt tetézi azzal, hogy alkalmazása során a valós folyamatokba intelligencia épül. Ez az intelligencia úgy valósul meg, hogy a háztartási eszközeink, a gépjárműveink az internetre lesznek kötve és különböző programok veszik át a vezérlésüket tőlünk. A hálózatba köthető eszközök 99% -a még nincs az interneten. A hűtőszekrény magától rendel élelmiszert, ha úgy látja, hogy az kifogyóban van, ki is fizeti. 3D nyomtatóval ki tudjuk nyomtatni a reggelinket vagy vacsoránkat[258]. A vezető nélküli gépkocsink magától elmegy gyógyszerért, de abba a patikába, amely előtt épp van szabad parkoló, amelyiket a legoptimálisabb módon lehet elérni és ahol legolcsóbb a gyógyszer.

A magyar állam is látja a Big Data jelentőségét, melynek során beindították a Big Data Nemzeti K+F programot. Az IBM által szervezett Storage Fórum 2013 kerekasztal-beszélgetésén állami intézmények és gazdasági társaságok döntéshozói azokról a konkrét lépésekről beszéltek, amelyeket szervezeteik a nagy adattömegek feldolgozásában most tesznek meg. Egyik ilyen állami intézmény a NAV. A NAV -nál drasztikusan begyorsult az új adatok felhalmozódása.[259] Vágújhelyi Ferenc, a NAV informatikai szakfőigazgatója szerint az adatrobbanás mértékét jól érzékelteti, hogy az adóhatóságnál 1988 és 2000 között összesen gyűlt össze annyi adat, mint a legutóbbi négy hónapban. A feldolgozás már jórészt online folyamat, az évi 80 millió ügyből csak másfél milliót intéznek papíralapon.

A szakértő megerősítette az IBM kutatója, Robyn Schwartz trendjelzését a szingularizáció ügyében. Ma már a NAV sem csak aggregált adatokkal dolgozik, hanem a tételes ÁFA esetében például atomizált, nagyszámú eseményekkel is. A beérkező adatmennyiség a pénztárgépek bekötése miatt hamarosan nagyságrendekkel megugrik majd. A beszerzett petabájtos tároló mellett ehhez pedig egyre bonyolultabb matematikai modellekre, elemzőképességekre van szükség.

A tavalyi év nagy hazai Big Data történetét Kerékgyártó Sándor, az Educatio ügyvezető igazgatója mutatta be. A magyar népszámlálás 11,4 millió kitöltött kérdőívét ugyanis az Educatio dolgozta fel a KSH számára. A továbblépés lehetősége az adatbázisok összekötésében rejlik. Például a felsőoktatásban végzettek elhelyezkedését figyelő, az Educatio által kezelt diplomás pályakövető rendszer még csak a NAV és az OEP adatbázisaival van összekötve, de ha a foglalkoztatási hivatal adatbázisával is összekapcsolódna, akkor a rendszer nem csak regisztrálni tudná a diplomások adatait, hanem munkalehetőséget is ajánlana számukra.

Bóday Tamás, a Vodafone szakértője az IBM és a mobilszolgáltató közös pilot-projektjéről beszélt. Egy sikeres isztambuli Big Data együttműködés nyomán a két cég most Győrben is elkezdte feldolgozni a mobilhasználók anonimizált cellainformációit. A geolokáció segít pontosan rekonstruálni honnan hová, mikor és hogyan mozognak az emberek a városban, és így abban is, milyen minták alapján kerülhet sor a közlekedési rendszer optimalizációjára. Eredmények egy éven belül várhatók.

A Big Data kapcsán felvázolt pár vízió álomnak tűnhet, de nem az, hanem a közeljövő valósága lesz. Erre kézenfekvő bizonyíték a fejezet végén leírt magyarországi Big Data lépések sorozata. További információ.[260]

[257] IBM Storage Forum 2013. Adatból információ konferencia, Budapest, 2013. február 28. Kovács Endre előadása
[258] http://m.hvg.hu/tudomany/20130522_Megoldas_az_ehinsegre_Jonnek_a_nyomtatott (letöltve 2013.05.10.)
[259] http://www-03.ibm.com/systems/hu/storageforum2013/video.html (letöltve 2013.05.10.)
[260] http://www.femina.hu/terasz/jelszo_pin_kod_torlese (letöltve 2013.05.14.)

3. A rendvédelmi folyamatok jellemzői és információigényük

A rendvédelmi folyamatok általánosságban aktív, dinamikus, célratörő jellemzőket hordoznak magukon. A rendvédelmi folyamatok jellegét nézve, azok lehetnek:

- Együttműködők, mint az állományba történő felvétel, képzés. Az események és tevékenységek előre szabályozhatók. Minél több adat áll a rendelkezésre, annál inkább értékesebb lesz az elemzés eredménye, annál inkább felszínre hozhatók a rejtett személyiségjegyek.
- Sztochasztikusak. Ilyen például a járőrszolgálat, bűncselekmény nyomozása, mivel az események és tevékenységek kiszámíthatatlanok, ugyan egy vezérelv kimunkálható, de sok a bizonytalansági tényező, bármi megtörténhet a folyamat zajlása során. Nem tudni mikor, milyen adatra lesz szükség, ezért minden adatot gyűjteni kell, viszont ezeket megfelelően rendszerezni kell, gyorsan elérhetővé kell tenni a felhasználók számára.
- Rejtettek. Embercsempészés, szervezett bűnözés, terrorizmus tartoznak ebbe a kategóriába. A megfelelő konspiráció, leplezés jellemzi őket, céljuk, hogy rejtve maradjanak a kívülállók, főként a hatóságok előtt. Kvázi rejtettek a hamisítások, árú csempészetek, drogárusítás, mivel ezek esetében kell egy felvevő piac, így befejezésükkor kénytelenek a felszínre kerülni. Rendvédelmi tevékenységként elsőként a felderítés kerül előtérbe. Két ellentétes folyamat harca zajlik. Releváns adatok felfedése, kiválasztása kap nagy hangsúlyt. Minden rejtett folyamat is egy környezetben zajlik, a környezetével kapcsolatba kerül, vannak megnyilvánulási jegyei. Ezeket a megnyilvánulási jegyeket kell az adott szakmának tudományos alapossággal feltárnia, melynek birtokában a személyi állományt fel kell készíteni ezek kutatására, felismerésére.
- Agresszívak. Többek között fegyveres bűnöző elfogása, gépkocsi üldözés során alakulnak ki ilyen folyamatok. Itt is két ellentétes folyamatról van szó, de a folyamatok egymás megsemmisítésére törekednek, az intelligencia helyett az erőszak dominál. Az agresszív folyamatok rendvédelmi támogatása során a valós idejű műveletekbe intelligencia vitelével lehet eredményeket elérni.

Áttekintve a rendvédelmi folyamatok információigényeit, azt tapasztalhatjuk, hogy a Big Data az a technológia, amely minden esetben hatékony és elengedhetetlen eszköz a magas szintű rendvédelmi tevékenység folytatásához.

4. Digitális nyomok, digitális élettér szerepe a rendvédelemben

Digitális nyomok alatt értjük azokat a cselekedeteinket, jellemzőinket reprezentáló elektronikus jeleket, biteket, amelyek a különböző, programok által vezérelt központi és használati eszközeinkben keletkeznek, kerülnek létrehozásra és az emberi érzékszervek által nem foghatók fel. A digitális nyomok sokasága és az, hogy a számítástechnika túllépve a támogató szerepén, már az egyes folyamatok, nagy rendszerek működésének az elengedhetetlen eszközévé válik, kialakítja a digitális életteret. A digitális nyomok feloszthatók közvetlen és származtatott digitális nyomokra. Közvetlen digitális nyomokat képeznek a mobiltelefonok, a mobil- és asztali számítástechnikai eszközök, az elektronikus tranzakció és ügyintézés, a vásárlói- és bankkártyák, az internetes böngészés, az e-mail forgalom, a közösségi oldalak, a blogok a különböző műhold, video felvételek, a digitális

fotók, képek, hangfelvételek, GPS jelek, adatbázisok. A mobiltelefon által generált digitális nyomok a cellainformációkból, a készülék- és tulajdonos jellemzőkből, valamint az elhangzott beszélgetések digitális rögzítéséből származnak. A cellainformációk a használat időpontját, időtartamát, illetve helyszínét rögzítik 10-400 m pontossággal. Az elhangzott beszélgetéseket a szolgáltató képes digitalizálni és tárolni, kapcsolni a hívószámhoz, illetve az eszköz más jellemzőihez. Amióta telefon létezik, azóta a rendvédelmi szervek alkalmazzák a telefon lehallgatást. A cellainformációk az embercsempészetek, más bűncselekmények felderítésekor jelentenek hathatós segítséget a rendvédelmi szerveknek. Ha visszaellenőrzik, hogy a bűncselekmény helyszínének közelében és időpontjában milyen beszélgetések történtek, akkor fény deríthető arra, hogy kik lehetnek a feltételezett elkövetők. Ez a módszer már számos bűnügy felderítésénél segítséget jelentett a rendőrségnek, mint például a roma gyilkosságok nyomozása során. A kommunikációs eszközök a háttérzajokat is képesek felfogni, továbbítani. Vannak olyan eszközök is, amelyekről, annak ellenére, hogy nem beszélünk rajtuk, lehet az irányító központból különböző információkat lekérni, mint például a helyszín koordinátáit vagy a háttérzajokat. Számtalan esetben ezek is hasznos információt tartalmaznak. Minden számítástechnikai eszköznek, legyen az a közismerten használt számítógép vagy az intelligens eszközökbe épített célszámítógép, van egy operációs rendszere, amely vezérli az eszköz működését, biztosítja a kapcsolatot a környezetével. Ezen kívül, többek között az operációs rendszerek folytatnak naplózást, rögzítenek minden olyan eseményt, amely a működés során bekövetkezik. Más egyéb fontosabb jellemzők, események mellett nyilvántartják, hogy mikor, milyen jelszóval léptek be a rendszerbe, milyen programokat indítottak el, milyen fájlokon milyen módosításokat végeztek és még számos más dolgot. Az interneten történő böngészés során is több olyan program fut, amely rögzíti, hogy milyen műveleteket hajtunk végre, milyen URL-t látogattunk meg, miket töltöttünk le, illetve ezen programok eltárolják a fontosabb adatainkat. Ezek közül az egyik közismert ilyen kis program az úgynevezett kuki. A különböző kémprogramok sokasága szinte felsorolhatatlan. A bankkártyák, illetve a vásárlói kártyák használata egyértelműen utal a helyszínre és az időpontra. Ezen túlmenően a mozgatott pénzösszeget, vásárolt áruk kódját is rögzítik. Az adatbázisokban személyes adataink és életciklusunk releváns eseményei nyernek eltárolást.

Minden mobiltelefonunk, számítógépünk (kivéve, amelyiket hermetikusan elzárunk minden hálózati kapcsolattól), az összes intelligens eszközünk valamilyen vezérlő központhoz, szerverhez kapcsolódik, amely befolyásolja annak működését és minden adatát eltárolja. Az intelligens eszközök úgy jönnek létre, hogy a hagyományos eszközeink kiegészülnek egy célszámítógéppel, amelyhez egy érzékelő van csatlakoztatva, fut rajta egy beavatkozó program és kommunikál a megfelelő partnerekkel. Egyeseket teljesen automatizálni lehet, az emberi felügyelet és beavatkozás nélkül működnek. A rendvédelmi szervek számára ezen központi vezérlő rendszerek adatai tudnak hathatós támogatást nyújtani. De a hálózatokból kizárt számítógépek is végeznek naplózást, lefoglalásukkor ezen naplóadatok is jól felhasználhatók, illetve a rajtuk tárolt fájlok. A törölt fájlok is visszahozhatók. A Kürt Kft. még összetört wincseszterről is nyert ki adatokat. Továbbá ezen egyedi számítógépek is távolról lehallgathatók, illetve lézerfegyverekkel rombolhatók.

A származtatott digitális nyomok valamely közvetlen digitális nyom feldolgozásával képezhetők. A globális elektronikus információgyűjtés egyik elterjedt módja során, a műhold- és térfigyelő-kamera felvételek, egyéb video, kép- és hangrögzítések, valamint a digitalizált dokumentumok alapján keletkezett közvetlen digitális nyomok különböző módszerekkel feldolgozásra, elemzésre kerülnek, amelyek

eredményeképpen előállnak a származtatott digitális nyomok. Ezek a származtatott digitális nyomok már komoly információtartalommal bírnak. A rendvédelem számára elengedhetetlen támogatást nyújtanak a képazonosító és hangfelismerő programok, valamint a dokumentum- és íráselemző eljárások. A biztonsági kamerák felvételeit feldolgozva a képazonosító programok már több esetben tették lehetővé a tettesek felderítését. A kép- és hangazonosítás a személyazonosítás, személyellenőrzés végrehajtását is elősegíti. A Google megkapta az engedélyt a 3D-s várostérképek elkészítéséhez térképkészítő kocsijainak használatára Magyarországon, azzal a feltétellel, hogy a személyek arcát letakarják. De az eredeti anyagban ott vannak a személyek is, amely esetleg rendvédelmi szempontból egyszer hasznos lehet.

A kép- és hangazonosításon túlmenően alkalmazásra kerülhet a kép- és hangelemzés is, illetve a stílus- és szokáselemzés. A kép- és hangelemzés a személyiségjegyekre, hangulatra, érzelmekre, a személyt ért behatásokra való reagálásra ad információkat. Ezt erősíti a stílus- és szokáselemzés. Milyen jelzőket, fordulatokat használunk az e-mailokban, más dokumentumokban, hogyan reagálunk a különböző eseményekre, érzelmi behatásokra, hol, miket vásárolunk, mi érdekel az interneten, kik a kapcsolataink a közösségi oldalakon, kikkel beszélünk telefonon stb. Amíg ezen elemzések eredményeit a piacgazdaságban a reklámszakmában hasznosítják, addig rendvédelemben a lehetséges bűnelkövetők személyiségképének, profiljának megalkotására alkalmasak. A prediktív személyiségkép állítható elő ezen elemzési módszerekkel.

Az algoritmikus elemzést is ugyanúgy használja a reklámszakma, mint a rendvédelem. Az elemzés legelső szintje a statisztikai adatok feldolgozása a különböző matematikai, kombinatorikai eljárásokkal. A statisztikai módszernél mélyebb információkat ad a kapcsolati rendszert megállapító elemzés. A rendőrségnél erre az Analayst's Notebook programot használják, amely a civil életben is közkedvelt. Ez a program táblázatosan és grafikusan is képes kimutatni az adott bűncselekmény nyomozása során felmerült személyek közötti kapcsolatot, ha minden felmerült adatot rögzítenek egy Excel táblában. De ez csak lineáris kapcsolatokat tud felkutatni. Például egy adott nevű személy kikkel áll kapcsolatban telefonszám, helyiség, gépkocsi rendszám alapján. Azt viszont nem tudja már kimutatni, hogy ha elindulunk egy szálon, például a helyiségeken, történetesen a helyiséghez kapcsolódik egy rendszám, akkor ezen az új ágon fusson tovább és a rendszámok alapján mutasson ki kapcsolatokat. Ha valamely rendszámhoz fűződik valahol egy telefonszám, akkor ezt a vonalat is kövesse. Ezt a több szálon való futást csak egy algoritmusokon alapuló elemzés képes végrehajtani. Ebben az esetben egy bonyolult gráfot kell feldolgozni, amely már Big Data támogatás nélkül nagyon nehezen megy. Algoritmikus elemzés kell azon összefüggések feltárásához, ahol azokat az okokat akarjuk kiszűrni, amelyek kiváltanak egy adott eseményt. Egy kiváltós oknál egyszerűbb a helyzet, de amikor több ok együttes előfordulása szükséges az esemény bekövetkezéséhez, akkor csak a kombináció és a variáció matematikai algoritmusaink közös alkalmazásával lehet eredményre jutni. Ez megint olyan bonyolult eljárás, amely igényli a Big Data technológiák alkalmazást. A szinergia az, ami az egyes elemek hatásainak felismerésével képes arra, hogy elősegítse ezen elemek pozitív egymásra hatásának érvényesülését. Az algoritmikus elemzésen keresztül lehet feltárni azon elemeket, amelyek képesek egymás hatását erősíteni.

A különleges digitális nyomok is egyre fontosabb szerepet játszanak a rendvédelmi munkában. Ilyen például a biometrikus személyazonosítás ujjnyom, arckép, hang vagy más jellemzők alapján, illetve a testbe épített és testre telepített eszközök, csipek.

5. Befejezés

A fentieket alapul véve, a rendvédelemnek óriási lehetőség, de egyben óriási kihívás is a Big Data technológia alkalmazására történő felkészülés. Mind e mellett az állampolgárokat meg kell védenie úgy a hatóságok visszaéléseitől, mint a rosszindulatú, hacker támadásoktól. Mindezek miatt elkerülhetetlen a rendvédelmi képzésbe és menedzsmentbe bevinni ezen korszerű technológiákra történő felkészítést. A gyakorlatban kiterjedtebben kell alkalmazni a proaktivitás, szinergia elvét, a prediktív személyiségkép alkotás technológiáit.