

SZIMBOLIKUS KÖZÖSSÉGEK

András István–Rajcsányi-Molnár Mónika–Németh István Péter (Szerk.)

BACSA-BÁN ANETTA Mernőktanár a pedagóguspályán
BENCÉNE FEKETE ANDREA Tehetséggondozás a Kaposvári
Egyetem Pedagógiai Karán
BUDAI GÁBOR Dunaújvárosi
középfokú oktatási intézményeinek szakmai kínálata
CSERNÉ ADERMANN GIZELLA Pedagógusok értékelési
kompetenciái
HORVÁTHNÉ LAZAR GABRIELLA Már-
kóthné HERDICS KRISZTINA A portfólió készítése
KESZI-SZEREMLEI ANDREA-NÁDASDI FERENC Az értékelés
oktatásának támogatása online tananyaggal
SZÁVÓ LÁRÉ
GÁBOR A pedagógiai értékelés szubjektív jellege a gyá-
korlatban
CSILLA MARIANNA SZABÓ Preparing Students
for the Labour Market: ESP e-Learning Courses at the
College of Dunaújváros
CSILLA MARIANNA SZABÓ-
ANETTA BACSA-BÁN Students' Drop-out Certificate instead
of Diploma? Present State and Possible Improvements
MEGYESI CSILLA Továbbképzések a közigazgatásban
VÁRALJAI MARIANN Információszerzési szokások vizs-
gálata a változó tanulási-környezetben
ZÁKOTA ZOLTÁN
NÉMETH ISTVÁN PÉTER Románia és Magyarország
felsőoktatása a számok tükrében
GERE ADÁM-KÖVÁRI

ATTILA Költséghatékony moduláris napelemes prototí-
pusrendszer fejlesztése
JÓZSEF KATONA The examination
of the application possibilities of brain wave-based control
UJBÁNYI TIBOR Felhasználók és adatkapcsolataik sérülé-
kenységének vizsgálata a rendszer biztonsági szintjének
meghatározásával
NAGY BALINT-WISZTHALLER ZOLTÁN
A Vally-modell nyereg-csomó bifurkációja
CSISZÉR ANAMARIA Európai Unió-s támogatások magyar kon-
textusban
KOVÁCS LAJOS Élhető világ
PIRICZ NOÉMI Az
üzleti etika aktuális kérdései
HORVÁTHNÉ FÁBIÁN MYRTILL
A népesség-előregedés területi-etnikai vonatkozásai
Bulgáriában az ezredforduló után
H. TÓMESZ TIMEA Új-
media-generáció – digitális közösség
KESZI-SZEREMLEI
ANDREA-PIRICZ NOÉMI A család és a gyerek érték –
Családbarát munkahely cím elnyerésének pozitív hatá-
sai a munkahelyre és az alkalmazottakra a Dunaújvá-
rosi Főiskolán



Dunakavics
KÖNYVEK 8.

D U F PRESS

András István–Rajcsányi-Molnár Mónika–Németh István Péter (Szerk.)

SZIMBOLIKUS

KÖZÖSSÉGEK

© András István–Rajcsányi-Molnár Mónika–Németh István Péter editors 2015

© Bacsa-Bán Anetta, Bencéné Fekete Andrea, Budai Gábor, Cserné Adermann Gizella, Csiszér Annamária, Gere Ádám, H.Tomesz Tímea, Horváthné Fábián Myrtill, Horváthné Lázár Gabriella, Katona József, Keszi-Szeremlei Andrea, Kovács Lajos, Kővári Attila, Markóthné Herdics Krisztina, Megyesi Csilla, Nádasdi Ferenc, Nagy Bálint, Németh István Péter, Piricz Noémi, Szabó Csilla Marianna, Szabó Imre Gábor, Ujbányi Tibor, Váraljai Mariann, Wiszthaller Zoltán, Zakota Zoltán 2015

Lektorálta Kukorelli Katalin és Váczi Mariann
Nyelvi lektor Kiss Gabriella

DUNAÚJVÁROSI FŐISKOLA
www.duf.hu
DUF PRESS
Kiadóvezető Németh István

Felelős kiadó András István
Felelős szerkesztő Nemeskéry Artúr

Tördelés Duma Attila
Készült a HTSART nyomdában
Felelős vezető Halász Iván

ISBN 978 963 9915 61 9

SZIMBOLIKUS KÖZÖSSÉGEK

András István–Rajcsányi Molnár Mónika–Németh István Péter (Szerk.)



Dunakavics
KÖNYVEK 8.

D U F PRESS
Dunaújváros, 2015

Tartalom

Előszó	7
<u>BACSA-BÁN ANETTA</u> Mérnöktanárok a pedagóguspályán	9
<u>BENCÉNÉ FEKETE ANDREA</u> Tehetséggondozás a Kaposvári Egyetem Pedagógiai Karán	21
<u>BUDAI GÁBOR</u> Dunaújváros középiskolái oktatási intézményeinek szakmai kínálata	31
<u>CSERNÉ ADERMANN GIZELLA</u> Pedagógusok értékelési kompetenciái	42
<u>HORVÁTHNÉ LAZÁR GABRIELLA – MARKÓTHNÉ HERDICS KRISZTINA</u> A portfólió készítése	51
<u>KESZI-SZEREMLEI ANDREA – NÁDASDI FERENC</u> Az értékelemzés oktatásának támogatása online tananyaggal	60
<u>SZABÓ IMRE GÁBOR</u> A pedagógiai értékelés szubjektivitása a gyakorlatban	72
<u>CSILLA MARIANNA SZABÓ</u> Preparing Students for the Labour Market: ESP e-Learning Courses at the College of Dunaújváros	83
<u>CSILLA MARIANNA SZABÓ – ANETTA BACSA-BÁN</u> Students' Drop-out, Certificate instead of Diploma? Present State and Possible Improvements	91
<u>MEGYESI CSILLA</u> Továbbképzések a közigazgatásban	100

<u>VÁRALJAI MARIANN</u>	
Információszerzési szokások vizsgálata a változó tanulási környezetben	119
<u>ZAKOTA ZOLTÁN-NÉMETH ISTVÁN</u>	
Románia és Magyarország felsőoktatása a számok tükrében – szerkezet, konvergencia, mobilitás	131
<u>GERE ADÁM-KÓVÁRI ATTILA</u>	
Költséghatékony moduláris napelemes prototípusrendszer fejlesztése	155
<u>IOZSEF KATONA</u>	
The examination of the application possibilities of brain wave-based control	167
<u>UJBÁNYI TIBOR</u>	
Felhasználók és adatkapcsolataik sérülékenységeinek vizsgálata a rendszer biztonsági szintjének meghatározásával	177
<u>NAGY BALINT-WISZTHALLER ZOLTÁN</u>	
A Vallis-modell nyeregcsomó bifurkációja	186
<u>CSISZÉR ANNAMÁRIA</u>	
Európai Uniós támogatások magyar kontextusban	194
<u>KOVÁCS LAJOS</u>	
Elhető világ	201
<u>PIRICZ NOÉMI</u>	
Az üzleti etika aktuális kérdései	209
<u>HORVÁTHNÉ FABIÁN MYRTILL</u>	
A népesség-előregedés területi-etnikai vonatkozásai Bulgáriában az ezredforduló után	217
<u>H. TOMESZ TÍMEA</u>	
Újmédia-generáció – digitális közösség	236
<u>KESZI-SZEREMLEI ANDREA-PIRICZ NOÉMI</u>	
A család és a gyerek érték – Családbarát munkahely cím elnyerésének pozitív hatásai a munkahelyre és az alkalmazottakra a Dunaujvárosi Főiskolán	245

Előszó

Egy intézmény életében kiemelkedő fontosságú a falai között létrejövő szellemi és /vagy kutatási termékek kommunikációja, a nyilvánossággal való ismertetése.

A Dunaújvárosi Főiskolán sincs ez másképp. Büszkék lehetünk és vagyunk is országos színvonalú laborparkunkra, a nálunk folyó tudományos és kutatói munkára, az oktatóink és hallgatóink által elért eredményekre, sikerekre és arra a számos pályázatra, melyben részt veszünk, melyet megvalósítunk.

Projektünk címe „Tudományos eredmények elismerése és disszeminációja a Dunaújvárosi Főiskolán” és fő célja volt, hogy a magyar tudomány kutatás-fejlesztési és innovációs eredményei minél szélesebb körben elterjedjenek továbbá, hogy a kutatói életpálya vonzóvá tételével a tehetséggondozás és tudományos utánpótlás biztosítva legyen. DF-es sikereket és más felsőoktatási intézményben folyó tudományos munkát is ismertettünk, így tágítva a kutatások iránt fogékony célközönség persepktíváit.

A támogatás segítségével számos olyan rendezvényt tudtunk megvalósítani, melyek a sikereink és eredményeink közvélemény felé történő kommunikációját segítette elő, pl. egyhetes nemzetközi tudományos konferenciasorozatot, Science Cafét és Nyugdíjas Egyetemet szerveztünk, ipari kapcsolataink tapasztalatait és véleményeit vitattunk meg, középiskolások számára rendeztünk szakmai fórumokat és innovációs előadásokat, online tudományos folyóiratot szerkesztettünk, kutatói adatbázist hoztunk létre.

Ez a kiadvány azt a célt szolgálja, hogy csokorba szedje az elmúlt egy év kutatói termését és ismertesse a közvéleménnyel az eddigi eredményeket.

Kedves Olvasó, bízunk benne, hogy Ön is talál kedvére való olvasmányt!

(A Szerkesztők)

Felhasználók és adatkapcsolataik sérülékenységének vizsgálata a rendszer biztonsági szintjének meghatározásával

Összefoglalás: Egy összetett informatikai rendszerben az informatikai biztonságra kiemelt figyelmet kell fordítani. A rendszert úgy célszerű kialakítani, hogy szerkezetileg ne tartalmazzon kritikus jelentőségű pontokat, amelyek külső és belső támadások alapjai lehetnek. A rendszer modellezésével és különböző mérőszámok meghatározásával ezek a kritikus részek feltárhatók. A cikk a rendszer biztonsági szintjének meghatározásával arra keresi a választ, hogy melyek a biztonság szempontjából sérülékenyebb adatkapcsolatok és felhasználói csoportok, amelyek veszélyt jelenthetnek az információvagyonra.

Kulcsszavak: IT biztonság, adatkapcsolatok, sérülékenység.

Abstract: IT security is important in a complex IT system. The system shall be so constructed that not contain critical points which can be based on internal and external attacks. These critical areas revealed by defining different metrics and modelling the IT system. This paper examine vulnerability of user groups and data links by define vulnerable levels.

Keywords: IT Security, data links, vulnerability.

Bevezető

Több felhasználós informatikai rendszer esetén az egyes rendszerek és az azok részét képező adatok védelmére még nagyobb hangsúlyt kell fektetni. Az információs vagyon részét képező adatokat az összes lehetséges módon óvni kell az illetéktelen hozzáférésektől. Ahhoz, hogy egy informatikai rendszerben védelemről és biztonságról beszélhessünk, ismernünk kell a rendszer komponenseit, hierarchikus felépítését, az egyes elemek és az

* Dunújvárosi Főiskola,
Informatikai Intézet
E-mail: ujbanyit@mail.duf.hu

- [1] J Katona, J. (2014): *Examination and comparison of the EEG based Attention Test with CPT and T.O.V.A., Proceedings of 15th IEEE International Symposium on Computational Intelligence and Informatics*. Budapest: IEEE Hungary Section. Pp. 117–120.
- [2] Dukán, P.–Kővári, A. (2013): *Cloud-based smart metering system, Proceeding of the 14th IEEE International Symposium on Computational Intelligence and Informatics*. Pp. 499–502.
- [3] Kővári, A.–Dukán, P. (2012): *KVM & OpenVZ virtualization based IaaS open source cloud virtualization platforms: OpenNode, Proxmox VE, Proc. of 2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics*. Pp. 335–339.
- [4] Farkas, I.–Dukán, P.–Katona, J.–Kővári, A. (2014): *Wireless Sensor Network Protocol Developed for Microcontroller-based Wireless Sensor Units, and Data Processing with Visualization by LabVIEW, Proceedings of the IEEE 12th International Symposium on Applied Machine Intelligence and*

alrendszerek, illetve a tágabb környezet közötti kapcsolatokat. A maximális védelemi szintet tehát nem csak a külső támadások elleni védekezés, hanem az informatikai rendszer adatai és az azokhoz hozzáférő felhasználói csoportok eloszlása, és e csoportok kapcsolatai is meghatározzák. Ezért már a rendszer kialakításakor figyelembe kell venni az informatikai rendszeren belüli alrendszerek és az azokhoz hozzáférő felhasználók és felhasználói csoportok halmazát.

Ahogy azt már korábban vizsgáltuk, az informatikai rendszerek támadhatóságánál azok a felhasználók és alkalmazások játszanak kiemelt szerepet, amelyek minél több információhoz férnek hozzá az adott rendszerben. Ha egy felhasználói csoport vagy egy alkalmazás hozzáférést kap a kritikus adatok többségéhez, akkor elmondható, hogy biztonsági szempontból ezek a tényezők jelentik a legnagyobb veszélyt a rendszerre egy esetleges sikeres külső támadás esetén. Amennyiben egy felhasználónak, vagy a felhasználók egy csoportjának nagy adathalmazhoz van hozzáférése, akkor az adott felhasználó vagy felhasználói csoport az adatok biztonságára kiemelt hatással van.

A rendszer tervezésekor körültekintően kell eljárni, ugyanis az sem mindegy, hogy melyik felhasználónak milyen jogokat osztunk. Lehetőségeinkhez mérten a rendszert úgy célszerű kialakítani, hogy ne legyenek benne támadások szempontjából kritikus jelentőségű egységek, vagyis a rendszerünknek ne legyenek olyan pontjai, amelyek nagyobb mértékben lehetnek kitéve a támadásoknak. Ezért a rendszer topológiájának meghatározásakor, az adati hozzáférések kialakításánál figyelni kell, hogy az adott rendszerkomponenshez történő hozzáféréskor a felhasználók a feltétlenül szükségesnél nagyobb jogkört ne kapjanak. Egy ilyen koncepció alapján tervezett sruktúrával biztosítható, hogy a rendszer biztonsági szintje a rendszer vonatkozásában maximális legyen.

A felhasználók megtevesztésén alapuló illetéktelen adathozzáférés komoly kockázatot jelent, amely emberi tényezőre vezethető vissza. Az emberi befolyásolhatóság vizsgálata esetleg a jövőben az agyi működés megfigyelésével is kimutatható. [1] A felhő infrastruktúra adta távoli adatkapcsolatok elterjedése [2], a virtualizációs megoldások [3] a vezetékek nélkül átvitel [4] a rendszerek biztonsága, hozzáférhetősége, összetettsége szempontjából további problémát jelentenek.

maximális
s, hanem az
csoportok
a rendszer
eren belüli
i csoportok

rendszerek
ak kiemelt
i az adott
hozzáférést
biztonsági
dszerre egy
lónak, vagy
érése, akkor
gára kiemelt

ugyanis az
at osztunk.
ni, hogy ne
ű egységek,
ek nagyobb
oológiájának
i kell, hogy
használók a
n koncepció
sági szintje a

lathozzáférés
ő vissza. Az
gyi működés
adta távoli
3] a vezetékek
összetettsége

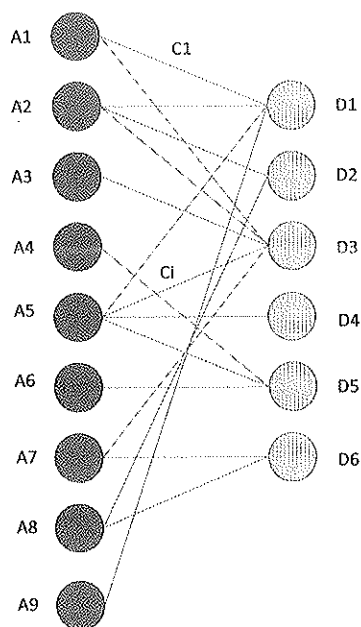
Amennyiben IT biztonság szempontjából számszerűsíteni tudjuk az egyes csoportok fontosságát, rámutathatunk az egyes csoportok számának, méretének és adathozzáférés kapcsolatainak az informatikai biztonságra gyakorolt hatására.

Az így rendelkezésünkre álló adathalmazból pedig lehetőség van további mérőszámokat is meghatározni, amelyek segítségével feltérképezhetjük a rendszer biztonsági szintjét.

Felhasználók és adatkapcsolataik modellezésének lehetőségei

Ahogy a [5] cikkben már említésre került, a felhasználók és azok adatkapcsolatai jól ábrázolhatóak páros gráf segítségével, mint ahogy azt az 1. ábra is mutatja.

1. ábra. A felhasználók és adatok kapcsolatait leíró páros gráf.



[5] Ujbányi T.– Ká-
tona J.–Kővári A.
(2014): IT bizton-
ság egy gráf alapú
modellje. *Dunakavics*.
2014. II. évf. VI.

[5] Ujbányi T.–Katonai J.–Kővári A. (2014): IT biztonság egy gráf alapú modellje. *Dunakavics*. 2014. II. évf. VI.

[6] Ujbányi T.–Katonai J.–Kővári A. (2014): Felhasználói csoportok és adatkapcsolatok vizsgálata az IT biztonság szempontjából. *Dunakavics*. 2014. II. évf. VIII. szám

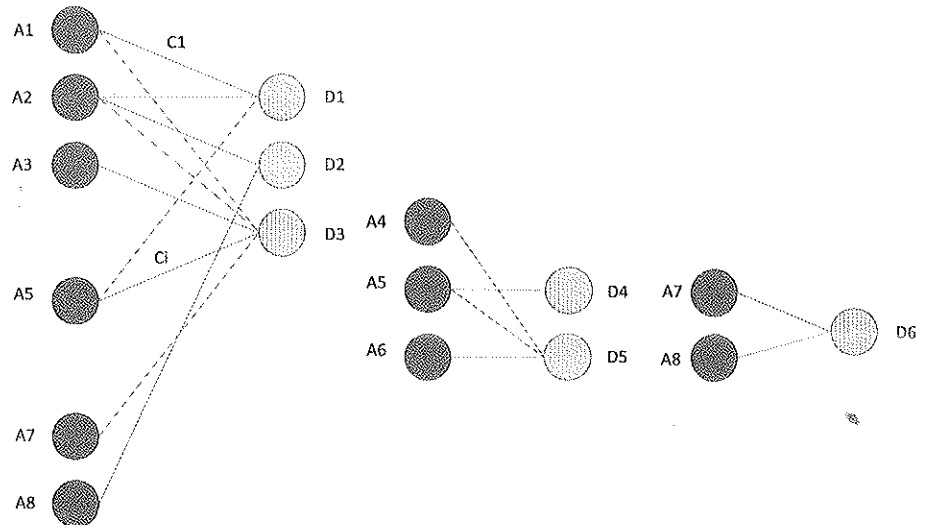
Az 1. ábrán látható gráfban az egyes aktorok az egyes adatstruktúrákat a C_i kapcsolaton keresztül megosztottan használják/férnek hozzá.

A csúcsok halmazát felosztva, ezzel A és B halmazt kapva egy G páros gráf jelölése a következő:

$$G = (A, B) \quad (1)$$

A [5] cikkben megállapítottuk, hogy a páros gráf komplexitása könnyen ábrázolható Venn-diagrammok segítségével. Eszerint a 2. ábrán azon aktorok által alkotott csoportok láthatóak, amelyek a teljes gráf egy részgráfját adják:

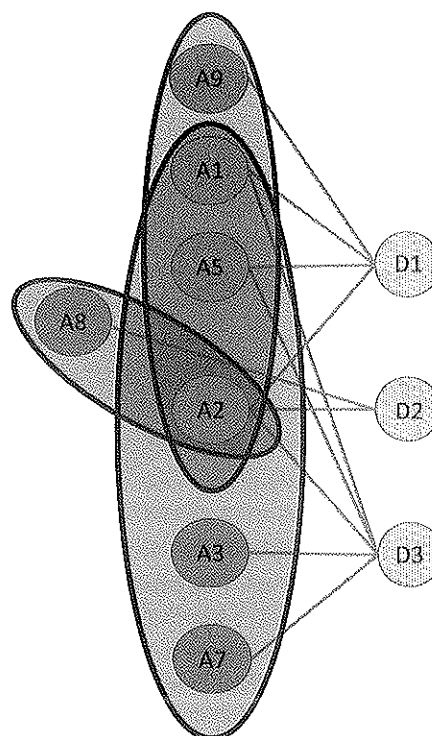
2. ábra. az egyes felhasználói csoportok és azok adat hozzáférései alapján definiálható részgráfok.



A [6] cikk szerint a Venn-diagram alapján megvizsgálható, hogy valamilyen biztonsági rés kihasználása esetén az egyes adathozzáférés szempontjából elkülönített csoportok között milyen esetekben jöhet létre ún. „kiszivárogó” információ. Az egyes aktori csoportokat leíró halmazok közötti információs csatornák ábrázolhatóak a 3. ábrán látható Venn-diagram szerint.

3. ábra. Az adatkapcsolatok ábrázolása Venn-diagramm segítségével.

Aktor	Kapcsolatok száma
A9	1
A1	2
A5	2
A8	1
A2	3
A3	1
A7	1

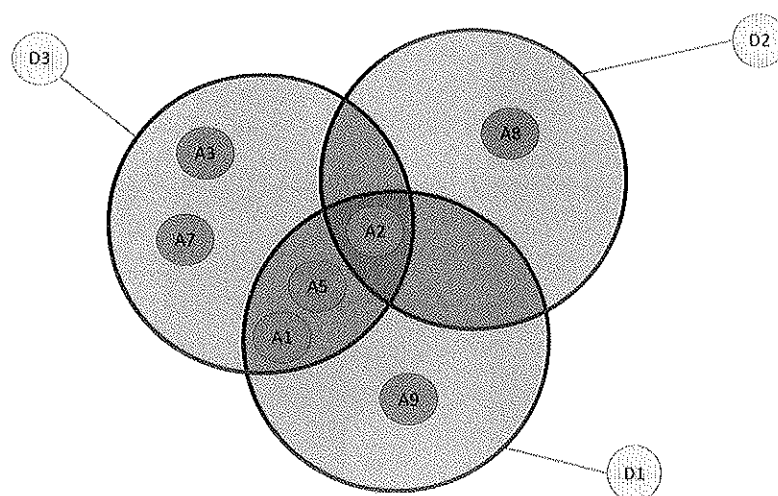


Adott számú aktor esetén, melyet jelöljünk N_a -val, ha megvizsgáljuk az egyes lehetséges csoportok maximális számát, akkor az alábbi összefüggés írható fel:

$$Cl_{max} = 2^{N_a} - 1 \quad (2)$$

A 2. ábrán megadott Venn diagram a 3. ábra szerinti halmaz ábrázolással is megadható, amelyben a halmazok metszetei jelentik az egyes csoportok közötti kapcsolatokat.

4. ábra. Adatkapcsolatok ábrázolása halmazok segítségével.



A rendszer biztonságának optimalizálása érdekében ismernünk kell az egyes kapcsolatok jelentőségét. Egy kapcsolat jelentősége jellemzi azt, hogy hány aktor hány adatstruktúrához fér hozzá egy kapcsolaton keresztül. A kapcsolat jelentősége nő a kapcsolathoz hozzáférő aktorok számával, valamint a kapcsolaton keresztül elérhető adatstruktúrák számával is. Ez alapján definiáljuk a kapcsolat jelentőségét (C_j) az adott csoportban lévő aktorok számának (Na) és az általuk elérhető adatstruktúrák számának (Nd) szorzatával:

$$C_j = Na_i \cdot Nd_i \quad (3)$$

Egy adott kapcsolat teljes rendszerre vonatkoztatott súlya (j_i) az alábbiak szerint definiálható:

$$Cp_i = \frac{C_j}{\sum_{j=1}^n C_j} \quad (4)$$

Célszerű a modellben figyelembe venni azt is, hogy az egyes adatok eltérő jelentőséggel bírnak, mint például gazdasági, személyes adatok vagy a kevésbé jelentős, nyilvános adatok. Ezt az egyes adatstruktúrákhoz rendelt adatjelentőségi tényezővel (D_j) jellemezzük. Ebben az esetben a (3) képlet szerinti összefüggés az alábbiak szerint módosul:

$$CDj_i = Na_i \cdot Nd_i \cdot Dj_i \quad (5)$$

Az így kapott kapcsolatok és adatok teljes rendszerére vonatkozó súly (Vli) az alábbiak szerint definiálható:

$$Vl_i = \frac{CDj_i}{\sum_{i=1}^C CDj_i} \quad (6)$$

Ez az érték az egyes csoportok nagyságára és az általuk hozzáférhető adatok jelentőségére vonatkozó mérőszámot adja meg. Ez a mérőszám jelöli, hogy egy felhasználói csoportot érő negatív esemény milyen mértékben okoz kárt az információvagyonban, vagyis a kockázat szintjét határozza meg.

Felhasználói csoportok sebezhetőségének vizsgálata

jelentőségét.
kapcsolaton
kapcsolaton
(C_j) az adott
szorzatával:

ató:

ggel bírnak,
zt az egyes
a (3) képlet

A vizsgált modellben egy fiktív, 3000 hallgatóval rendelkező felsőoktatási intézmény struktúráját vesszük alapul. A főiskola állami oktatási intézmény. Annak érdekében, hogy az intézményben hatékony munkafolyamatok valósuljanak meg, különböző szervezeti egységek kerültek kialakításra. Ennek megfelelően a különböző adatokhoz, információkhoz való hozzáférés (beleértve a kritikus/érzékeny adatokat, információkat) felügyelt módon történik. Az egyes szervezetek egyedi rendszereket is használnak, az adatokhoz való hozzáférés eltérő jogosultsági csoportok bevezetésével valósul meg. Minden csoport más-más jogosultsági szintet képvisel. A főiskola személyi állománya alapvetően három csoportra bontható: oktatók, hallgatók és a nem oktatók csoportjára. A nem oktatók csoportja adathozzáférések szempontjából további alcsoportokra bontható: technikai- és adminisztratív személyzetre. A technikai személyzet tagjai közé sorolhatók a rendszeradminisztrátorok, karbantartók és a biztonsági szolgálat munkatársai. Az adminisztratív személyzet körébe az intézetek/osztályok adminisztrátorai és irodai asszisztensei tartoznak.

A három csoport közül a hallgatók csoportja (~ 3000 fő) rendelkezik a legkevesebb jogkörrel, a fontosabb rendszerek közül a Neptun-t és valamilyen eLearning keretrendszert (pl.: Moodle) érik el, hallgatói jogosultsággal (olvasási, illetve írási jog, ahol szükséges). Az adminisztratív munkatársak (~ 44 fő) jogosultsági köre már kiterjed a különféle nyilvántartásokhoz, központi iratkezelő rendszerekhez (pl.: dokumentumkezelő rendszer, könyvtári adatbázisok) és hálózati meghajtókhoz (intézeti, ill. saját meghajtók) történő hozzáférésekre is. A technikai dolgozók (~ 10 fő) csoportja jogosultság szerint több alcsoportra bonthatók: a karbantartók minimális jogkörrel bírnak: használni tudnak személyi számítógépeket, egy-egy nyilvántartás kivételével a fontosabb belső rendszerekhez nincs hozzáférésük. A rendszeradminisztrátorok azonban az adatokhoz/rendszerekhez való hozzáférések szempontjából kritikus jelentőséggel bírnak. Ők menedzselik a jogosultsági csoportokat, a rendszerekhez történő

hozzáféréseket: jogokat osztanak és vonnak meg a felhasználóktól, akiknek egyéni beállításaik is lehetnek. A rendszeradminisztrátorok csoportja is tovább bontható tartományi és lokális rendszergazdai csoportra. A tartományi adminok további jogkörökkel ruházhatják fel a lokális rendszergazdákat. Az alábbi táblázat reprezentálja a vizsgált modellt.

1. táblázat. Felhasználói csoportok sebezhetőségének vizsgálata.

	Hallgatók	Oktatók	Vezető oktatók	Adminisztrátorok (HR)	Adminisztrátorok (THH)	Adminisztrátorok (GH)	Technikai személyzet	Rendszergazdák	T. rendszergazdák
CI	1	2	3	4	5	6	7	8	9
Na	3000	88	11	7	15	22	10	12	6
Nd	3	3	4	4	4	3	2	6	8
Cj	9000	264	44	28	60	66	20	72	48
Dj	0,001	0,1	0,3	0,5	0,3	0,5	0,6	0,8	1
CD	9	26,4	13,2	14	18	33	12	57,6	48
VI	4%	11%	6%	6%	8%	14%	5%	25%	21%

A táblázatban meghatározásra kerültek az aktori csoportok, ezzel együtt a csoportokba tartozó aktorok száma (*Na*) is. Tovább haladva leolvasható az egyes aktori csoportok által elérhető információs rendszerek száma (*Nd*), amely az aktorok számával együttesen határozza meg a kapcsolatok jelentőségét (*Cj*). Ez az érték jelöli az egy kapcsolaton keresztül történő hozzáféréseket (hány aktor hány adatstruktúrához fér hozzá). Az adatjelentőségi tényező (*Dj*) egy olyan mérőszám, amely az egyes aktori csoportok által hozzáférhető adatok és információk fontosságát jelöli a rendszerbiztonság szempontjából. A táblázatban egy 0-1-ig terjedő skálán jelöltük az egyes csoportok által hozzáférhető adathalmaz jelentőségét.

A táblázatból leolvasható, hogy a rendszeradminisztrátorok és a tartományi rendszeradminisztrátorok – teljes vagy minimálisan korlátozott jogosultsági szintjeik okán – az adatkozzáféréseket tekintve legveszélyesebbek a rendszer egészére, addig a hallgatók csoportja egészen minimális kritikussági szintet képvisel. A fenyegetettségi szint az aktorok számának (*Na*), az általuk elérhető információs rendszerek számának (*Nd*) és az adatjelentőségi tényező (*Dj*) szorzatából tevődik össze. A táblázat jól reprezentálja az egyes aktori csoportok által képviselt fenyegetettségi szintet a rendszer egészére nézve: a hallgatók tekinthetők a legkisebb veszélyforrásnak, addig a rendszergazdák és a tartományi rendszergazdák csoportja adatbiztonság szempontjából már erős fenyegetést jelent. Ennek megfelelően az aktori csoportok által képviselt kockázati szint egyenesen arányos a fenyegetettségi szinttel. Megfigyelhető, hogy a kapcsolatok és

s lehetnek.
csoportra.
bi táblázat

T. rendszer- gazdák
9
6
8
48
1
48
21%

ozó aktorok
rendszerek
jét (Cj). Ez
truktúrához
portok által
táblázatban
ét.

nisztrátorok
ket tekintve
ssági szintet
s rendszerek
eprezentálja
a hallgatók
lák csoportja
pportok által
apcsolatok és

adatok teljes rendszerére vonatkoztatott súly (kockázati szint, VI) mértékét aktorok és az adatahozzáférések száma erősen befolyásolja: a tartományi adminisztrátorok hiába rendelkeznek az összes létező jogkörrel a rendszerben, a lokális adminisztrátorok csoportja (létszámfölényükből adódóan) nagyobb mértékben okozhat kárt az információvagyonban.

Összefoglalás

Az informatikai biztonság szempontjából egy felhasználói csoportot tekintve a külső támadások száma és az adott csoport információs kapcsolatainak száma határozza meg a csoport biztonság szempontjából betöltött jelentőségét. A cikkben egy modell segítségével feltérképeztük, hogy ezek a csoportok (figyelembe véve a csoportok által hozzáférhető információs rendszerek számát, meghatározva különböző mérőszámokat) milyen hatással lehetnek az információvagyonra egy-egy negatív esemény bekövetkeztekor. A kockázati szint ismerete segíthet bennünket a rendszer védelmének megtervezésében.