Egészségügyi adatok biztonsága a kibertérben – zsarolóvírusok és felhasználói biztonságtudatosság

Doktori tézisek

Dr. Palicz Tamás Gyula

Semmelweis Egyetem
Mentális Egészségtudományi Tagozat

Témavezető: Dr. Joó Tamás, Ph.D., egyetemi docens

Hivatalos bírálók: Dr. Bödör Csaba, MTA doktora, egyetemi tanár
Dr. Krasznay Csaba, PhD, egyetemi docens

Komplex vizsga szakmai bizottság:
Elnök: Dr. Szíjártó Attila, MTA doktora, egyetemi tanár
Tagok: Dr. Németh Orsolya, Ph.D., egyetemi docens
Dr. Bányász Péter, Ph.D., egyetemi docens

EDT tag: Dr. Domján Gyula, Ph.D., egyetemi docens

Budapest
2025

1. BEVEZETÉS

Doktori munkám témájául az egészségügy digitális transzformációjával együtt járó adat és információbiztonsági változásokat, illetve ezen belül is a kiberbiztonságot választottam.

A kutatásokat megalapozó irodalmi áttekintés alapján az mondható el, hogy az elmúlt évek digitális átalakulása az egészségügyet is jelentős mértékben érintette, és ez igaz a magyar egészségügyi rendszerre is. Ezek a fejlesztések elsősorban technológiai fókuszúak, és csak mérsékelten érintették a felhasználót, vagy az egészségügyi fejlesztések végső kedvezményezettjeinek, a betegeknek a digitális készségeit. A fejlesztések kiegyensúlyozatlansága hátterében az egyik lehetséges ok, hogy nem rendszerszintű megközelítést alkalmaznak, amelynek oka részben az, hogy a digitális egészségügyi rendszerek ökoszisztéma jellegű megközelítése és leírása hiányzik. Ennek a rendszerszintű megközelítésnek a hiánya kapcsán adódott az logikus lehetőség, hogy a biológiai rendszerekhez hasonlóan itt is használjuk, és meghatározzuk a digitális egészségügyi ökoszisztéma fogalmát, és vizsgáljuk meg, hogy abban az adat hol helyezkedik el, illetve ezen megközelítéssel hogyan értékelhető a magyarországi helyzet. Ebben a rendszerben az adat kulcsszerepet játszik, azonban ez az adat nemcsak az egészségügyi digitális rendszerekben keletkezhet, hanem „kívülről” is érkezhet, és ez is hozzájárulhat az egészségügyi rendszer eredményeihez, vagyis van lehetőség arra, hogy nem közvetlenül az egészségügyben keletkező adatok is felhasználhatók legyenek az egészségügyi rendszer javítására, monitorozására. Ezen megközelítéssel, megfelelő adat és információbiztonsági feltételek biztosítása mellett a gyakorlati alkalmazással az irodalomban nem találkoztunk. Ezt az igényt különösen felerősítette, hogy a COVID-19 pandémia alatt a különböző adatforrások kreatív, társadalmi hasznosítására szükség volt, és ezt lehetőség szerint nemzeti szinten kellett megoldani.

Az egészségügyi digitális rendszerek működésére, az adatok és információk biztonságára az egyik legnagyobb veszélyt azok a külső tényezők jelentik, amelyek befolyásolják az információk bizalmasság-sértetlenség-rendelkezésre állás hármasát. Ennek tipikus esetei az egészségügyi intézményeket érintő és rendszerszintű hatással is bíró zsarolóvírus támadások. Ez a jelenség különösen felerősödött a 2020-ban indult COVID-19 világjárvány alatt és után. Magyarországon a kibervédelmi tevékenység erősödésével párhuzamosan az egyes szektorok is aktívabbá váltak, azonban a zsarolóvírus esetek csak

korlátozottan váltak ismertté, holott ezen esetekből nagyon sok tapasztalatot meg lehet osztani: jó és rossz példákat lehet megismertetni. A tudományos kutatásom kezdetekor nem álltak rendelkezésre olyan esetleírások, amelyek hazai egészségügyi intézmények esetében írták volna le a zsarolóvírus támadás lefolyását. Ezek megismerése, a rendszerbe kerülés, majd az okozott hatás leírása, tudományos megközelítésű elemzése fontos része a rendszer és egy-egy szervezet tanulási folyamatának.

Végül azt kell kiemelni, hogy ezekben a rendszerekben is emberek dolgoznak, akik ismeretei, viselkedése, attitűdje alapvetően befolyásolja a rendszerek (és benne az adatok és információk) biztonságát. Így a biztonságtudatossággal kapcsolatos emberi szempontok, az azokat meghatározó szociodemográfiai és egyéb jellemzők megismerése kiemelten fontos általában a lakosságot tekintve, majd azt követően az egészségügyi digitális rendszerek, de általában a digitális átalakulások következtében létrejövő elektronikus információs rendszerek biztonsági szintjének emelése érdekében. A kutatás megkezdésekor a magyar lakosságra vonatkozóan nem, vagy korlátozottan álltak rendelkezésre olyan adatok, amelyek a szociodemográfia jellemzőkre vonatkozóan vizsgálták volna, hogy hogyan lehet jellemezni a biztonságtudatos vagy kevésbé biztonságtudatos csoportokat.

A bevezetőben és a fenti összefoglalóban bemutatott és kiemelt problémakör magyar, egészségügyi szempontú feldolgozása - egyelőre - gyakorlatilag nem létezik.

Az irodalmi áttekintés és a gyakorlati tapasztalatom alapján az elkövetkező években az egészségügy fejlődésének, és ezen belül is a diszruptív technológiák (pl. mesterséges intelligencia, telemedicina) elterjedésének az egyik legfontosabb területe, vagy talán a fejlődés „Achilles-sarka” az információbiztonság lesz. Mind a betegek (ügyfelek), mind a rendszerben dolgozók számára kritikus lesz, hogy milyen tapasztalatokat szerzünk, milyen ismeretekkel rendelkezünk, milyen kompetenciákat kell használnunk, fejlesztenünk és milyen attitűddel viszonyulunk az ehhez kapcsolódó változásokhoz ebben az adatgazdag, de rendkívül sérülékeny világban.

Talán azt is lehet mondani, hogy általában a digitális átalakulás, és az azzal járó változtatások egyik kritikus sikertényezőjéről beszélünk: bár számos nemzetközi irodalom már található, azonban az egészségügy sajátosságai miatt kevés referencia

található erre a szektorra vonatkozóan, illetve különösen érintetlen még a magyar egészségügy ebből a szempontból.

Különösen fontosnak tartom, hogy a magyar egészségügyi digitalizáció, amelynek tervezésénél, a kezdeti lépésinél - kiemelt uniós projektek révén - személyesen is ott lehettem, azt a kezdeti versenyelőnyét, amely az EESZT létrejöttével megszerzett, az elkövetkező években is megtartsa.

Erre elsősorban azért van szükség, hogy mindezen fejlesztések a magyar egészségügy javát szolgálják, vagyis a betegek számára több egészséget eredményezzenek.

2. CÉLKITŰZÉSEK

Általános célkitűzésként azt fogalmaztam meg, hogy az információ- és kiberbiztonság területén megjelenő kihívásokat az egészségügy szemszögéből tekintsem át, annak specialitásait figyelembe véve, különösen koncentrálva azokra a tényezőkre, amelyek a betegek biztonságát érdemben befolyásolhatják. Ilyen terület lehet például az egészségügyi intézmények folyamatos működésének biztosítása (üzletmenet folytonosság tervezés és menedzsment) illetve az emberi erőforrás biztonságtudatossága. Az alábbi specifikus célkitűzéseket (C), kutatási kérdéseket (K) és hipotéziseket (H) fogalmaztam meg:

C1. célkitűzés: Annak feltárása és bemutatása, hogy a digitalizáció révén létrejövő, megváltozó digitális egészségügyi rendszer egységes szempontok alapján leírható és értékelhető (rövidítve: C1: digitális egészségügyi ökoszisztéma).

K1.1. kutatási kérdés: Leírható-e a digitalizációs átalakulás során megváltozó egészségügy rendszer egy ökoszisztémaként? Ennek milyen elemei vannak és ezeket mi jellemzi Magyarországon?

C2. célkitűzés: Annak bemutatása, és gyakorlati példával igazolása, hogy az egészségügyi adatokhoz biztonságos környezetben más adatok is kapcsolhatók, és ezen innovatív adathasznosítások olyan értéktöbbletet eredményeznek, amely kormányzati döntéselőkészítési és döntéshozatal szinten is megjeleníthető (rövidítve: C2: biztonságos innovatív adathasznosítás).

Az egészségügyi rendszeren kívül is keletkeznek olyan adatok, amelyek feldolgozása, megfelelő bemutatása az egészségügyi rendszert és állapotot érintő döntések alapjául szolgál. Ezek az adatok különös jelentőséggel rendelkeznek veszélyhelyzetben, amikor az innovatív adathasználat révén egyedi kérdésekre lehet választ találni, illetve ezek a döntések alapjául szolgálhatnak. Ezekben a helyzetekben kritikus fontosságú, hogy az adathasznosítás biztonságos környezetben történjen.

K2.1. kutatási kérdés: Hogyan és milyen módszertannal lehet hasznosítani a digitális egészségügyön kívül keletkezett adatokat, egy globális vagy lokális egészségbiztonsági eseményhez kapcsolódva? Hogyan biztosítható, hogy az adatvédelmi szabályoknak és kiberbiztonsági követelményeknek megfeleljen ez a módszertan?

C3. célkitűzés: Annak bemutatása, hogy az egészségügyben keletkező adatok sértetlensége, bizalmassága és rendelkezésre állása kritikusan fontos a működés szempontjából, és ezt a kibertérből a zsarolóvírus támadások kapcsán reális veszély fenyegeti a kórházak esetében is (rövidítve: C3: zsarolóvírusok az egészségügyben).

K3.1. kutatási kérdés: Milyen hatással voltak zsarolóvírus támadások a magyar kórházak működésre, és milyen mértékben érintették a kórházi informatikai és információs rendszereket, beleértve a szállítói lánc részeként működő szakmai területeket?

K3.2. kutatási kérdés: Hogyan, milyen szempontok és kérdések mentén lehet az eseteket megfelelően összegyűjteni és elemezni annak érdekében, hogy megállapítható legyen: mely funkciók milyen mértékben károsodtak az adott egészségügyi intézményben?

C4. célkitűzés: Annak vizsgálata, hogy van-e összefüggés a demográfiai valamint informatikai használati szokások és a kiberbiztonsági tudatosság között (rövidítve: C4: lakossági biztonságtudatosság)

H4.1. hipotézis: Feltételezésem szerint a magyar lakosság esetében a biztonságtudatos magatartás nincs összefüggésben kor, nem, iskolázottság és informatikai használati szokásokkal.

3. MÓDSZEREK

A kutatás során alkalmazott módszerek interdiszciplináris megközelítést tükröznek, igazodva a téma összetettségéhez és sokrétűségéhez.

Dokumentumelemzés (M1)

A dokumentumelemzés során a releváns irodalmak és források feldolgozását végeztem el, különös tekintettel az ún. szürke irodalomra. Ez utóbbi nem hagyományos tudományos publikációkat jelent, például konferencia-előadásokat, szakértői és kormányzati jelentéseket, vagy újságcikkeket, amelyek értékes információkat tartalmazhatnak új tudományterületek, mint például az egészségügyi kiberbiztonság vizsgálatában. A módszer egyik kulcsa az internetes keresőmotorok használata szigorú szűrési kritériumokkal, mint például meghatározott formátum(ok) preferálása és az adott források szakmai hitelességének ellenőrzése.

Esetfeldolgozás struktúrált interjúkkal (M2)

Az egészségügyi kiberbiztonsági incidensek, például zsarolóvírus-támadások esettanulmányainak feldolgozása a kutatás egyik központi eleme volt. Az eseteket egy 5 fős szakértői csoport válogatta, amely tagjai informatikai, egészségügyi menedzsment, jogi és információbiztonsági területen szerzett több éves tapasztalattal rendelkeztek. Az elemzés szempontjai között szerepelt az incidensek hatása a betegellátásra és a tanulságok megfogalmazása, amelyek más intézmények számára is hasznosak lehetnek. Az előre meghatározott kérdésekre adott válaszok feldolgozását a szakrtői csoport végezte.

Kérdőíves felmérés (M3)

A 2021-ben végzett lakossági kérdőíves kutatás az információbiztonsági tudatosságot vizsgálta, különös tekintettel a szocio-demográfiai tényezőkre és az informtikai használati szokásokra. Az online kérdőív tervezésekor figyelembe vettem a válaszadói motiváció fenntartását, ezért a kérdések száma és terjedelme korlátozott volt. Az elektronikus csatornákon terjesztett kérdőív 1516 válaszának elemzése során a leíró statisztikai jellemzők mellett a válaszokat biztonságtudatosság szempontjából kedvező és kedvezőtlen magatartásokként kategorizáltam és ezeket a csoportokat Khi-négyzet próbával hasonlítottam össze.

Adatok másodlagos elemzése (M4)

A COVID-19 járvány kapcsán a mobilszolgáltatók által biztosított anonimizált Call Detail Records (CDR) adatok alapján végzett elemzések célja a mozgási minták megértése volt. A feldolgozáshoz kapcsolódó módszertan kialakításának legnagyobb kiívása az volt, hogy olyan adat- és információbiztonsági szempontból megfelelő környezet kerüljön kialakításra, amely révén döntés előkészítés számára értékelhető és megjeleníthető eredményeket lehet a Microsoft Power BI Pro szoftverrel bemutatni.

Az egyes módszerek alkalmazása során külön figyelmet fordítottam az adatvédelmi és információbiztonsági szempontok betartására, különösen a kérdőíves kutatás és az anonimizált adatelemzések esetében. Ez a komplex megközelítés lehetővé tette a kutatás célkitűzéseinek átfogó vizsgálatát, hozzájárulva a tudományos és gyakorlati megközelítés egyensúlyához.

4. EREDMÉNYEK

Digitális egészségügyi ökoszisztéma

Az egészségügyi digitalizáció ökoszisztémáját egy olyan modell keretében vizsgáltam, amely középpontjában az egszségügyi adat áll. Ez az adat az alapja a rendszerszintű döntéshozatalnak, és meghatározza az innovációs folyamatokat is. A kutatás során megalkotott modell elemei a következők: felhasználók, digitálisan felkészült szakemberek, IT és távközlési infrastruktúra, digitális szolgáltatások, irányítási és üzemeltetési modellek, pénzügyi háttér, szabályozási környezet. A hazai környezetben az elemek áttekintése segítséget nyújt a fejlesztések rendszerszintű, kiegyensúlyozott megközelítéséhez, amely biztosíthatja a rendszer fenntarthatóságát.

Biztonságos innovatív adathasználat

A kutatás második nagy témaköre a COVID-19 járvány kapcsán felhasznált cellaadatok elemzésére épült (1,2 TerraByte adat, közel 4,3Mrd rekord). Az adatok anonim módon történő kezelése és a kiberbiztonsági feltételek biztosítása érdekében egy speciális környezetet fejlesztettünk ki (fizikai, adminisztratív és logikai védelem kialakítása mellett a kutató csoport működési rendjének meghatározása), amelyre a döntéstámogató rendszer épült. Ez a rendszer lehetővé tette a lakossági mozgásmonitorozást és az ennek alapján történő célzott kormányzati intézkedések megvalósítását. Az adatbiztonság és a GDPR előírásainak való megfelelés kiemelt jelentőségű volt a projektben.

Zsarolóvírusok az egészségügyben

A zsarolóvírusok hatásait négy esettanulmányon keresztül elemeztem. A vizsgálat során bemutattam, hogy a támadások okoztak fennakadásokat, azonban ezek a betegellátást csak mérsékelten érintették. Az esettanulmányok alapján levont legfontosabb tanulságok az alábbiak voltak:

- az egészségügyi intézmények esetében a külső (fizikailag nem kórházban levő) munkavégzés különösen magas kockázatot jelentett, hiszen azokat a külső (nem a kórház által tulajdonolt és felügyelt) számítógépeket és hálózati eszközöket nem ellenőrizték, illetve a kórházi informatikai hálózatba történő becsatlakozásuk sem biztonságos csatornán keresztül történt.

- a kórházi rendszerbe szállítókon, alvállalkozókon keresztül is kerülhetnek be rosszindulatú programok, ezek terjedése nagyon gyorsan történhet.
- a nem rendszergazdák által létrehozott nem megfelelő jogosultsággal rendelkező publikus könyvtárak jelentették az egyik legnagyobb veszélyt a fertőzés szempontjából.
- az informatikai rendszerben és végpontokon jelentkező rendellenes működésről az informatikai rendszer üzemeltetését végzőket és az információbiztonságért felelős személyeket a lehető leghamarabb tájékoztatni kell.
- ehhez megfelelő riasztási, értesítési rendszer kidolgozása szükséges.
- az informatikai és információbiztonsági szereplőknek azonnali beavatkozást kell tenni a helyzet eszkalálódásának megelőzése érdekében.
- nem megfelelően képzett informatikai csapat információbiztonsági problémát okoz.
- incidens kapcsán a korábbi tapasztalatok nagyon sokat érnek, lehetőség szerint ilyen személy(eke)t igénybe kell venni.
- a probléma megoldásába be kell vonni a szállítókat és a környezetben dolgozó, megbízható informatikai és információbiztonsági szakértőket.
- jelentősen segíti a veszélyhelyzetekben a megfelelő működést és cselekvéseket, ha az intézmény rendelkezik ilyen helyzetekre alkalmazható tervekkel, amelyeket gyakorolnak is.
- amelyik intézet rendelkezett külső mentésekkel, az jelentősen könnyítette a helyreállítást.
- a vezetésnek közvetlenül és közvetetten is kiemelt felelőssége van a biztonságos környezet kialakításában.
- a biztos, hiteles tudást adó központi kapcsolat kiemelt fontosságú ilyen helyzetekben.
- több feladatot párhuzamosan kell végezni és koordinálni, amely a teljes intézmény tekintetében jelentős erőforrást igényel mind szakmai, mind koordinatív szempontból.

Lakossági biztonságtudatosság

Az országos felmérés eredményei azt mutatták, hogy a magyar lakosság információbiztonsági tudatossága összefüggésben áll bizonyos demográfiai tényezőkkel, és informatikai használati szokásokkal.

Áttekintettük a különböző változók és biztonságtudatosság közötti lehetséges kapcsolatokat és az eredmények közül az alábbiakat emelem ki:

1. a nem tekintetében szinte egyértelműnek tűnik az összefüggés: a férfiak biztonságtudatosabbak, és ez statisztikai összefüggést mutat az eszközök magasabb számával, a gyakoribb eszköz használattal, a rendszeres IT biztonsági hírek olvasásával, valamint a biztonságtudatos viselkedési mintákkal (vírusirtóhasználat, jelszóhasználat, kattintás tudatosság, nyilvános wifi használat, stb.)
2. a generációk tekintetében nem olyan egyértelműek az összefüggések, mint a nem esetében: itt összefüggést lehet találni a tájékozottsággal, a biztonsági frissítések tudatosságával és a vírusirtó használatával. A többi biztonságtudatos minta nem mutatott egyértelmű és konzekvens életkorral/generációval összefüggő sajátosságot.
3. a tartózkodási hely szerepe sem teljesen egyértelmű: 2021-ben a kapott válaszoknál nem találtunk olyan összefüggést, amely legalább valamilyen tendenciaként megfogalmazható lenne (pl. azt várhatnánk, hogy a nagyvárosokban több eszközt használnak, vagy több időt töltenek számítógép előtt, de erre utaló összefüggés nem mutatható ki).
4. iskolai végzettség esetében egyértelműbb a kép: a magasabb iskolai végzettségű kategóriák válaszadói gyakrabban adtak biztonságtudatos válaszokat. Emellett az iskolai végzettség összefüggésben van az ezen eszközökkel munkában töltött idővel.
5. az eszközök száma és a munkában az eszközökkel töltött idő összefüggést mutatnak: a több, mint 3 eszközzel rendelkezők, és akik legalább 6 órában a munkaidejükből számítástechnikai eszközt is használnak, azokra jellemzőbb a biztonságtudatos viselkedés.
6. a legerősebbnek tűnő összefüggés az IT hírek olvasási gyakorisága és a biztonságtudatos viselkedés között van, vagyis aki rendszeresen olvas ilyen híreket, ott szinte minden esetben, kivétel nélkül biztonságtudatos viselkedésre utaló válaszokat kaptunk

5. KÖVETKEZTETÉSEK

Kutatásomban az egészségügy digitális átalakulásához kötődően vizsgáltam meg az adat- és információbiztonság aspektusait.

Újdonságok

Elsődlegesen egy olyan modellt alkottam, amely segítheti a digitális fejlesztéseket kiegyensúlyozottá tenni: a digitális egészségügyi ökoszisztéma modelljének bevezetése, és az elemeinek meghatározása abban segít, hogy az egyes elemek egyensúlyának megteremtése révén egy működőképes, fenntartható és forrásallokációs szempontból hatékony digitális rendszer jöjjön létre. A modellben az egészségügyi adat kap központi szerepet: ennek van és lesz az elkövetkező időszakban a legnagyobb szerep és értéke.

A kutatásomban azt is bemutattam, hogy az egészségügyi adatok mellett más adatok is bevonhatók az egészségügyi döntéshozatalba, különösen veszélyhelyzet esetén. A biztonságos innovatív adathasználat megteremtésével bemutattam, hogy mobilszolgálatók által biztosított cellatorony adatokkal olyan mutatók alakíthatók ki, amelyek képesek döntés előkészítésére, vagy egy-egy beavatkozás monitorozására.

Az egészségügyi adatok bizalmasságát, rendelkezésre állását és sértetlenséget napjainkban leginkább a zsarolóvírus támadások veszélyeztetik. Hazai esetek feldolgozásával sikerült bemutatnom, hogy megfelelő adatgyűjtés és adatfeldolgozás után olyan tapasztalatok oszthatók meg, amelyek segíthetik a sikeres felkészülést egy lehetséges támadásra. Ehhez a jelenlegi formákon változtatni szükséges, szélesebb körűnek kell lennie az adatfelvételnek, és az adatok kutathatósága mellett kiemelt fontosságú a tudományos és egészségügyi szakmai disszemináció.

A fenti információbiztonsági események kapcsán az egyik legfontosabb szempont, hogy ezeket az eseményeket lehetőség szerint megelőzzük, amelyhez célcsoport specifikus biztonságtudatosítás szükséges. A célcsoportok sajátosságainak meghatározáshoz országos lakossági felmérést végeztünk és a beérkezett több, mint 1500 választ feldolgoztuk. Munkám során kimutattam, hogy a szociodemográfiai tényezők közül a nem és az iskolai végzettség összefüggést mutat a biztonságtudatos magatartással. Emellett a kutatás azt is kimutatta, hogy a biztonságtudatosság jellegzetes magatartásmintázattal jár, és ebben meghatározó volt, hogy a válaszadó milyen olvasottsággal rendelkezik az információbiztonság területén.

A bemutatott kutatásokkal az egészségügyi kiberbiztonság területén új kutatási eredményeket és tudást hoztam létre.

Limitációk

Az egyes kutatási területeken külön-külön számos korláttal szembesültem, amelyeket fontos figyelembe venni az eredmények értelmezésekor.

A digitális ökoszisztéma leírása során felmerült egyik nehézség, hogy az alkalmazott elméleti megközelítések és keretek túlnyomórészt nemzetközi példákon alapultak, amelyek nem mindig illeszkednek a magyar egészségügyi rendszer sajátosságaihoz, különösen, ha figyelembe vesszük, hogy az egészségügyi rendszerek működése, és különösen a fejlesztések, változtatások kapcsán a kulturális vonatkozások nagy hangsúlyt kapnak. Az ökoszisztéma elmeinek, szereplőinek és folyamataiknak részletes feltérképezése nem minden esetben lehetett teljes, elsősorban erőforrásbeli korlátok miatt.

A mobiladatok kapcsán az interoperabilitási problémák és az adatminőség eltérései nehezítették az elemzést, míg a viselkedési minták és mozgási adatok kontextusának hiánya, illetve az aggregáltság foka az eredmények torzításához vezethetett. Ezek a korlátok befolyásolják a mobiladatok felhasználásának lehetőségeit az egészségügyi rendszerek és folyamatok fejlesztése érdekében.

A zsarolóvírus-kutatás esetében az adatgyűjtés jelentette a legkomolyabb limitációt: az érintett szervezetek gyakran nem hozzák nyilvánosságra az incidenseket, ami retrospektív elemzésekre, másodlagos adatokra és információkra való támaszkodást tett szükségessé. Ezáltal az eredmények pontossága és általánosíthatósága korlátozott lehet. Az esetek mélyebb megértésére alkalmazott interjúk korlátozott következtetések levonására alkalmasak, különösen mert jelentős idő telt el az esemény és a feldolgozás között, másrészt pedig nem teljeskörűen lehetett minden korabeli résztvevőt és érintettet bevonni az esetfeldolgozásba.

A lakossági biztonságtudatosságot célzó felmérés során az egyik legfőbb limitáció az, hogy a minta jellemzői alapján korlátozottan lehet következtetéseket levonni a teljes populációra. A válaszadói minta reprezentativitása korlátozott lehetett, különösen az életkor vagy a digitális írástudás tekintetében. Az önbevalláson alapuló adatok torzíthatják az eredményeket, mivel a résztvevők hajlamosak saját

biztonságtudatosságukat idealizált módon bemutatni. Emellett fontos limitáció az is, hogy ez egy pillanatfelvételnek megfelelő keresztmetszeti képet adott, és nem tette lehetővé az adatok időbeli változásainak követését.

Fejlesztési javaslatok

A digitális egészségügyi ökoszisztéma leírása nagyban segítheti a kiegyensúlyozott, fenntartható fejlesztések kereteinek megalkotását. Önmagában nem elegendő pl. az infrastruktúra fejlesztés, vagy digitális szolgáltatások, és alkalmazások előállítása, hanem ahhoz, hogy fenntarthatók legyenek a fejlesztések, a többi ökoszisztéma elemet is fejleszteni kell. Szintén fontos hasznosíthatósága ennek a megközelítésnek, hogy ezt egy kisebb területen is lehet alkalmazni. Például általában az információbiztonság esetében is érdemes az ökoszisztéma fogalmát meghatározni, de az egészségügyön belül is lehetnek speciális vonatkozásai ennek a kisebb ökoszisztémának, mint ahogy azt a mesterséges intelligencia fejlesztésekre vonatkozóan is megemlítettem.

A biztonságos innovatív adatfeldolgozás kapcsán alkalmazott módszertani fejlesztéseknek köszönhetően új lehetőségek nyílnak meg, például a közismert GPS, vagy a CDR adatok és egyéb, az egészségügyi döntéshozatalban hasznosítható információk integrálása. Emellett egy olyan rendszer prototípusát alakítottuk ki, amely számos veszélyhelyzetben alkalmazható, illetve más tudományterületek bevonásával ki is terjeszthető.

A zsarolóvírusok elleni védekezésben kidolgozott új esetfeldolgozási módszertan jelentős előrelépést jelenthet az események megértése és a következmények megítélése terén. A módszertan alapja egy átfogó és strukturált megközelítés, amely célzottan az egészségügyi intézmények sajátosságaira és a zsarolóvírusok jellegzetességeire összpontosít. Az új módszertan segítheti az egészségügyi intézmények és hatóságok közötti kommunikációt, a tapasztalatok feldolgozását, és ez alapján a reagálást és a helyreállítást is egy esetleges támadás után. Emellett ezek az esetek jól felhasználhatók az egészségügyi felsőfokú képzésben, az egészségügyi dolgozók élethossziglani továbbképzésében, valamint különböző érzékenyítő és tudatosító tréningeken.

A lakossági adatfelvétel és feldolgozás kapcsán fontos kiemelni, hogy a kérdőív folyamatos fejlesztésével lehetőség van még árnyaltabban megismerni a biztonságtudatossággal kapcsolatos ismereteket és attitűdöt, illetve a későbbiekben

lehetőség szerint a különböző ágazati sajátosságok beépítésével ágazatspecifikus megismerés válik lehetővé, amely alapján pontos beavatkozások tervezhetők érzékenyítésre vagy éppen a tudatosság szintjének növelésére. Ezt a fejlesztési munkát már elkezdtük a Nemzeti Kibervédelmi Intézettel. A kérdőíves feldolgozással lehetőség van kockázatos célcsoportok azonosítására, és a kockázatok alapján specifikus képzések kialakítására a csoportok számára. Emellett a fejlesztések révén ki lehet alakítani olyan kérdőívet is, amelyben már nemcsak csoportos, hanem egyéni kockázatok is azonosíthatók, és például egy-egy munkakör betöltésénél, vagy éppen egy munkahelyi továbbképzésnél személyre szabható a kiválasztás, vagy a belső képzési programok.

6. SAJÁT PUBLIKÁCIÓK JEGYZÉKE

Értekezés témájához kapcsolódó saját publikációk:

1. Balogh J., Szócska M., **Palicz T.,** Kontsek E., Pollner P., Varga G., Ugrin I., Davidovics K., Joó T. (2022) A mesterséges intelligencia alapú megoldások fejlesztése és bevezetése az egészségügyben –kézműves manufaktúrától a gyártósorig?, IME 21: 2 pp. 56-63.

2. **Palicz T.,** Bonnyai T., Bencsik B., Pintér L., Dombrádi V., Joó T., Bor O., Hornyik Zs. (2022) Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei, Belügyi Szemle 70: 2 pp. 395-418.

3. Tobiás B., Klujber V., Kósa J., **Palicz T.** (2022) Digitalizáció szerepe a genetikai vizsgálatokban: döntéstámogató rendszer fejlesztése a hazai genetikai tanácsadás segítésére, IME 21: 4 pp. 40-48.

4. Ugrin I., Dombrádi V., Joó T., Nagyjánosi L., **Palicz T.,** Varga G., Lakatos B., Szerencsés V., Lám J. (2022) Élethosszan át tartó oltási stratégia mint eszköz a pandémiák elleni védekezésben Magyarországon [Lifelong vaccination strategy as a tool against pandemics in Hungary] Orvosi Hetilap 163: 14 pp. 535-543.

5. Gaál P., Joó T., **Palicz T.,** Pollner P., Schiszler I., Szócska M. (2021) Adattudományi innováció az egészségügy környezeti kihívásainak kezelésében: a nagy adatállományok hasznosításának jelentősége és lehetőségei a járványkezelésben Scientia et Securitas 2: 1 pp. 2-11.

6. **Palicz T.,** Bencsik B., Szócska M. (2021) Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai Scientia et Securitas 2: 1 pp. 78-87.

7. **Palicz T.,** Sas T., Szabó ZA., Tóth T., Tisóczki J., Bencsik B., Joó T. (2021) Magyar kórházakban előfordult zsarolóvírus támadások esetei IME 20: 1 pp. 32-38.

8. Szabó ZA., Szócska M., **Palicz T.,** Szerencsés V., Joó T. (2021) A digitális egészségügyi ökoszisztéma fogalmának és elemeinek nemzetközi és hazai áttekintése [Global and national overview of the digital health ecosystem] Információs Társadalom 21: 3 pp. 47-66.

9. Szerencsés V., **Palicz T.,** Joó T., Lám J., Demeter-Fülöp V., Ugrin I. (2021) A Covid19 járvány során hozott egészségügyi intézkedések és hatásaik Magyarországon és Ausztriában Belügyi Szemle 69: 1 pp. 123-141.

10. Szócska M., Pollner P., Schiszler I., Joó T., **Palicz T.,** McKee M., Asztalos Á., Bencze L., Kapronczay M., Petrecz P., Tóth B., Szabó Á., Weninger A., Áder K., Bacskai P., Karaszi P., Terplán Gy., Tuboly G., Sohonyai Á., Szőke J., Tóth Á., Gaál P. (2021) Countrywide population movement monitoring using mobile devices generated (big) data during the COVID-19 crisis Scientific Reports 11: 1 Paper: 5943, 9 p

11. Vida Z., Vissi B., **Palicz T.,** Lám J. (2021) Smart & Safe – intézményi digitalizációs stratégia a betegbiztonság szemszögéből [Smart & Safe –digitalisation strategy from a patient safety perspective] Orvosi Hetilap 162: 47 pp. 1876-1884.

12. **Palicz T.,** Sas T., Tisóczki J., Bencsik B., Joó T. (2020) „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben ["Your money or your life!" –Ransomwares in healthcare information systems] Orvosi Hetilap 161: 36 pp. 1498-1505.

13. Tóth T., **Palicz T.,** Szócska M. (2020) A magyar egészségügyi szakemberek digitális technológiákkal kapcsolatos attitűdjének vizsgálata IME 19: 2 pp. 44-48.

14. Mikesy G., **Palicz T.,** Sinka LAE. (2020) COVID-19 menedzsment ajánlás a telemedicina használatáról In: Belicza Éva, Lám Judit, Safadi Heléna, Sinka Lászlóné Adamik Erika (szerk.) COVID-19 kórházi menedzsment-ajánlásaink Budapest, Magyarország: Semmelweis Egyetem Egészségügyi Menedzserképző Központ pp. 115-120.

15. **Palicz T.,** Joó T. (2020) Az infrastuktúra-védelem és az információbiztonság kapcsolata In: Deák, Veronika (szerk.) Az IBTV. gyakorlata: Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet 50 p. pp. 21-32.

16. Szócska M., Joó T., Gál AL., Lőrincz O., Auer A., **Palicz T.** (2019) A hálózatkutatás alkalmazhatósága a közszolgáltatások fejlesztésében In: Auer Ádám, Joó Tamás (szerk.) Hálózatok a közszolgálatban Budapest, Magyarország: Dialóg Campus Kiadó 247 p. pp. 9-25.

Értekezés témájától független saját publikációk

1.Kilim O., Olar A., Joó T., **Palicz T.,** Pollner P., Csabai I. (2022) Physical imaging parameter variation drives domain shift Scientific Reports 12: 1 Paper: 21302, 11 p.

2.Schutzmann R., Nistor K., Albert F., **Palicz T.** (2021) A szociális vezetőképzés: körkép a hazai és európai uniós képzési kínálatról Szociálpolitikai Szemle 7: 1 pp. 89-104. (2021)

3.Kovács R., Aszalós Z., Cserháti Z., **Palicz T**. (2021) Krónikus beteg munkavállalók támogatása, munkahelyi betegségmegelőzés: Az Európai Unió Chrodis Plus közös fellépésének munkahelyek számára kínált jógyakorlatai IME 20: 4 pp. 38-44.

4.Bálity Cs., Cserháti Z., Lám J., **Palicz T.,** Safadi H. (2020) Humán szolgáltatások képzési programjainak értékelési rendszere IME 19: 3 pp. 9-14.

5.Antal Zs., Cserháti Z., **Palicz T.,** Lám J. (2020) Intézményi menedzsmentfejlesztő továbbképzés vezető szakdolgozók részére IME 19: 4 pp. 21-26.

6.Joó T., **Palicz T.,** Szócska M. (2018) A népegészségügyi termékadó dohánytermékekre való kiterjesztésének lehetősége IME 17: 7 pp. 30-33.

7. Palicz T., Vártok J., Szócska G. (2003) A folyamat-újraszervezési (BPR) projektek tapasztalatai az egészségügyben IME 2: 2 pp. 17-22.

8. Szócska G., **Palicz T.,** Vártok J., Karádi I. (1999) Minőségügyi fejlesztés a gyakorlati orvosképzésben az ellátás minőségéért: Az oktatás, mint a gyógyítófolyamatok minőségét meghatározó eljárás Lege Artis Medicinae 9: 4 pp. 322-327.

9. Szombathy T., Szalai Cs., Barna K., **Palicz T.,** Romics L., Császár A. (1998) Association of angiotensin II type 1 receptor polymorphism with resistant essential hypertension Clinica Chimica Acta 269: 1 pp. 91-100.

10. Szalai Cs., Császár A., **Palicz T.,** Halmos B., Czinner A., Romics L. (1997) Pontmutációk kimutatása familiáris hypercholesterinaemiás betegekben Magyar Belorvosi Archivum 50: 3 pp. 263-268.