Gradus Vol 11, No 2 (2024)
ISSN 2064-8014

NÉHÁNY PÉLDA A SPAM-EK JELENTETTE GAZDASÁGI KOCKÁZATOKRA - ESETTANULMÁNY

SOME EXAMPLES OF THE ECONOMIC RISKS OF SPAM – CASE STUDY

Tóth Adrienn[0009-0009-2991-7297.1*] *Kasznár Attila*[0000-0001-7790-6722 2]

[1] Gazdaságtudományi Kar, Neumann János Egyetem, Magyarország
[2] Nemzetközi Gazdaságtan Tanszék, Gazdaságtudományi Kar, Neumann János Egyetem, Magyarország
https://doi.org/10.47833/2024.2.ECO.020

Kulcsszavak:
kiberterrorizmus
spam
szervezett bűnözés
adatvédelem
szűrő program

Keywords:
cyberterrorism
spam
organised crime
datasafety
filter program

Cikktörténet:
Beérkezett 2024. április 5.
Átdolgozva 2024. április 15.
Elfogadva 2024. április 18.

Összefoglalás

A tanulmány célja, hogy konkrét példákon keresztül bemutassa a spam-ek jelentette biztonsági kockázatokat. A spam az online banki szolgáltatások, és az online kereskedelem bővülésével egyre nagyobb szerepet kap a lakosságot, a vállalkozásokat, illetve a vállalatokat fenyegető veszélyforrások között. Az internetes bűnözők, köztük a kiberterroristák között is népszerű, könnyen használható, nagy bevétellel kecsegtető, ugyanakkor megfelelő anonimitást biztosító eszköz a spam. A tanulmányban bemutatott példák általánosan megjelenő, a mindennapok reális veszélyét jelentő esetek.

Abstract

The aim of the study is to illustrate the security risks posed by spam through concrete examples. With the growth of online banking and online commerce, spam is becoming an increasingly important threat to individuals, businesses and companies. spam is a popular and easy-to-use tool for cyber-criminals, including cyber-terrorists, offering high revenues while providing adequate anonymity. The examples presented in this study are common and real everyday threats.

1. Bevezetés – háttér és célok

Az elmúlt évtizedekben az online platformok térnyerésének eredményeként a mindennapok részévé vált az internet. Az online tér alapvetően átalakította az emberi élet számos színterét, azonban a kényelmi szolgáltatásokon túlmenően olyan ismeretlen fenyegetettségek sorát is az emberiségre szabadította, amelyekre a lakosság nagy része nincs felkészülve. A bűnözés történetében új dimenziókat nyitott a kibertér, amelyeket tovább tágít annak globális elterjedése, és annak a ténye, hogy napjainkban gyakorlatilag mindenki és mindenhol internet alapú programok és applikációk segítségével intézi az ügyeit. A kibertéren belül is fenyegetettségek újabb dimenzióját jelenti a sokféle felhasználó és felhasználási egység összekapcsolását megvalósító IoT-rendszerek terjedése. „*Az IoT-rendszerek összetettek, különböző környezetben működő sokfajta eszköz összekapcsolását valósítják meg, ami igen széleskörű támadási felületet eredményez.*"[1]

A kiberbűnözés nagyon változatos, egyben rendkívül kiterjedt eszközrendszerrel bír, amelynek jelentőségét a mindinkább szélesedő online tér napról-napra tovább növeli. A kibertér a maga számos rejtett elágazásával széles tárházát biztosítja az illegális online tevékenységnek. „*A*

* Kapcsolattartó szerző. Email: adrienn289@gmail.com

biztonsági események nagyságrendje, gyakorisága és hatása évről évre, mondhatjuk, exponenciális mértékben növekszik, ami súlyos fenyegetést jelent az információs társadalom működésére és tevékenységére." [2] A különböző szervezett bűnözői körök, illetve a magányos bűnözők pedig nem riadnak vissza az alternatívék kifejezetten aktív és kreatív felhasználásától. A lehetőségek végtelensége eredményezte, hogy az online térben elkövetett jogellenes cselekmények ugyanúgy népszerűek a legprimitívebb bűncselekmények elkövetői között ugyanúgy, mint a magas intelligenciával rendelkező, komplex szervező és előkészítő munkálatokat igénylő cselekmények kitervelői között.

A kiberbűnözés egy kezdetleges, azonban egyszerűsége miatt töretlen népszerűségnek örvendő formája a spam, vagyis a kéretlen üzenet. A legegyszerűbb adatátviteli formában megvalósuló „*rövid üzenetküldő szolgáltatás (SMS) a mobiltelefon-felhasználók számának gyors növekedése miatt világszerte az egyik legelterjedtebb kommunikációs módszerré vált. Ez a gyors növekedés felkeltette a nem kívánt (spam) küldő felek figyelmét, és a kéretlen (spam) e-mailekhez hasonlóan az SMS spam üzenetek problémáját okozta.*" [3] A spamek lassan a mindennapi élet részévé váltak, ugyanakkor, bár „*számos modell létezik az SMS- és e-mail- spam felismerésére, amelyek közül a felügyelt tanuláson alapuló modell a leghatékonyabb*" [4], mégis továbbra sincs olyan átfogó *„modell, amely a spam -felismerésről szólna.*" [5]

A *spam* -ek jelenléte ugyanakkor folyamatos, és nem csak bosszantó kellemetlenséget jelent, de gazdasági veszélyt is magában hordoz. Jelen tanulmány elsősorban esettanulmány kíván lenni, amelyben a szerzők azt kívánják bemutatni, hogy a mindennapokban a *spam* -es segítségével egyes bűnözői körök miként fenyegetik a személyes biztonságot, valamint a vállalkozások gazdasági biztonságát is.

2. Fókuszban a *spam*

Nap, mint nap, számolatlanul érkeznek kéretlen üzeneteket a felhasználók leveles ládáiba. Eleinte egyfajta nyomuló reklámként működtek, a cégek ilyen üzenetekkel igyekeztek terjeszteni ismeretségüket. A *spam* alapvetően a „*kéretlen kereskedelmi küldemények összefoglaló megnevezése. Ennek keretében a feleslegesen szétszórt e-mail-címeket használják fel reklámok küldésére.*" [6] Mára már egyre több az ártó szándékkal az e-mail-fiókba érkező *spam* -ek száma.

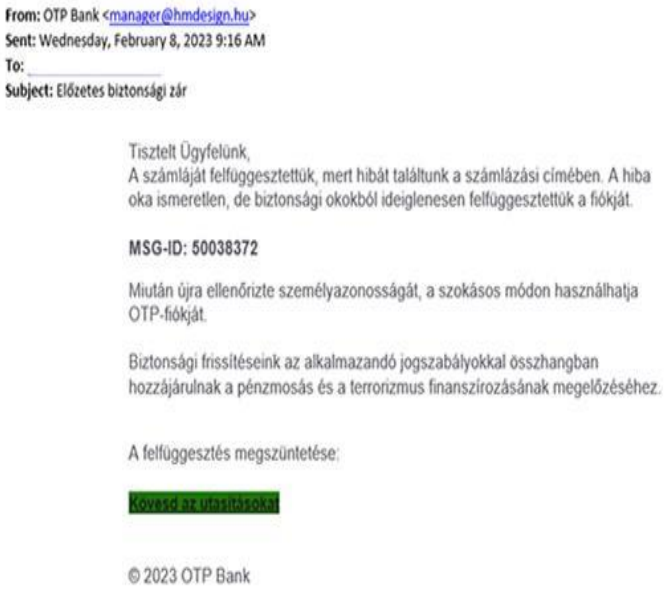
A legfontosabb ártó szándék pedig elsősorban az adathalászat, amelynek célja pedig a legtöbb esetben az anyagi károkozás. Az adathalászok a legtöbb esetben azzal a céllal „dolgoznak", hogy a megszerzett információk segítségével az adatok valódi gazdájának pénzét megszerezzék. Ez egy egyszerű gazdasági bűncselekmény, azonban számos esetben ezen túl mutat az elkövetők célrendszere, és az áldozat a valóságban terroristák, vagy velük együttműködő körök hálójába kerül. Az adathalászat révén megszerzett összegek pedig ebben az esetben igen könnyen kerülhetnek a terroristák kezébe, amely azt is jelenti, hogy az adathalászat áldozatától eltulajdonított összeget terrorfinanszírozásra használják fel.

A *spam* -ek régóta nehezítik a felhasználók életét, az átlagember számára is ismert a létezésük. A pénzintézetek és bankok rendszeresen frissítik weboldalaikat, figyelmeztetéseket küldenek a csalásokról, a média különböző csatornáin is gyakori téma a *spam* -ek jelentette veszély, ennek ellenére, egyre többen esnek az adatlopás áldozatává. Manapság igen könnyen hozzá férnek személyes adatokhoz, telefonszámokhoz és az e-mail címekhez. Elég csak egy kevésbé biztonságos internetes oldalra beregisztrálni, és máris bárki hozzáférhet a felhasználó személyes adataihoz, internet használati szokásaihoz, és még rengeteg egyéb információhoz. Azt a folyamatot, amelyen keresztül a személyes adatokat megszerzik, adatlopásnak nevezzük. Az adatlopás három, legalapvetőbb fajtája:

1. A Vishing, a telefonhívások. Ez a legritkábban előforduló példa. Ebben az esetben a személyt telefonon keresik a csalók általában banki intézetekre hivatkozva, de előfordul, hogy egy szállítmányozó cég nevében mutatkoznak be. Minden esetben egy problémára hívják fel a figyelmet: Illetéktelen utalás történt, vagy a csomagot nem sikerült kiszállítani. Ilyenkor a telefonáló fél elkéri a címet, illetve a bankkártya adatokat. Már olyan is előfordult, hogy egy alkalmazás telepítésére kérték meg az érintettet, ami a jövőben megvédi őt az adatlopástól. Ironikusan ezek a szoftverek azok, melyek pont információ gyűjtésre lettek fejlesztve.

Legjobban úgy lehetséges védekezni ezen álhívások ellen, ha olyan információkra kérdez rá a felhasználó, amelyekre csak a bank vagy a szállítmányozó cég tud választ adni. Ilyen lehet a kártya hátulján található CVC kód, a számlaszám utolsó néhány karaktere, vagy a rendelésszám.

2. Egy másik, igen jellemző forma a spearphising, az e-mail-en keresztül történő csalás. Ezek a nem kívánatos üzenetek a legjobb esetben automatikusan a *spam* -ek közé kerülnek, feltéve, ha a felhasználó jó e-mail szűrő rendszert használ. Olykor azonban elkerüli a szűrőprogramok figyelmét néhány jól álcázott e-mail. Többnyire ilyenkor is banki vagy más pénzintézet megszemélyesítésére kerül sor, de előfordulhat hamis e-mail mobilszolgáltatótól, postai intézményektől, csomagküldő cégektől, szolgáltatóktól.


From: OTP Bank <manager@hmdesign.hu>
Sent: Wednesday, February 8, 2023 9:16 AM
To: _____
Subject: Előzetes biztonsági zár

Tisztelt Ügyfelünk,
A számláját felfüggesztettük, mert hibát találtunk a számlázási címében. A hiba oka ismeretlen, de biztonsági okokból ideiglenesen felfüggesztettük a fiókját.

MSG-ID: 50038372

Miután újra ellenőrizte személyazonosságát, a szokásos módon használhatja OTP-fiókját.

Biztonsági frissítéseink az alkalmazandó jogszabályokkal összhangban hozzájárulnak a pénzmosás és a terrorizmus finanszírozásának megelőzéséhez.

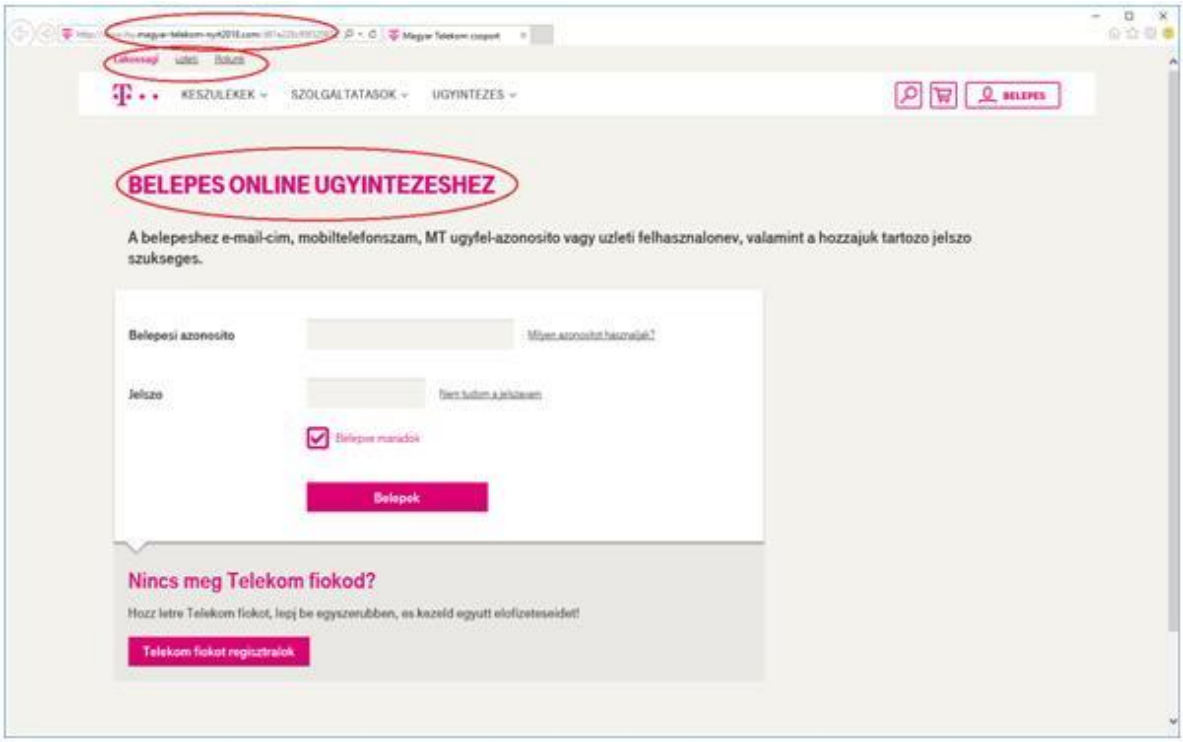
A felfüggesztés megszüntetése:

Kövesd az utasításokat

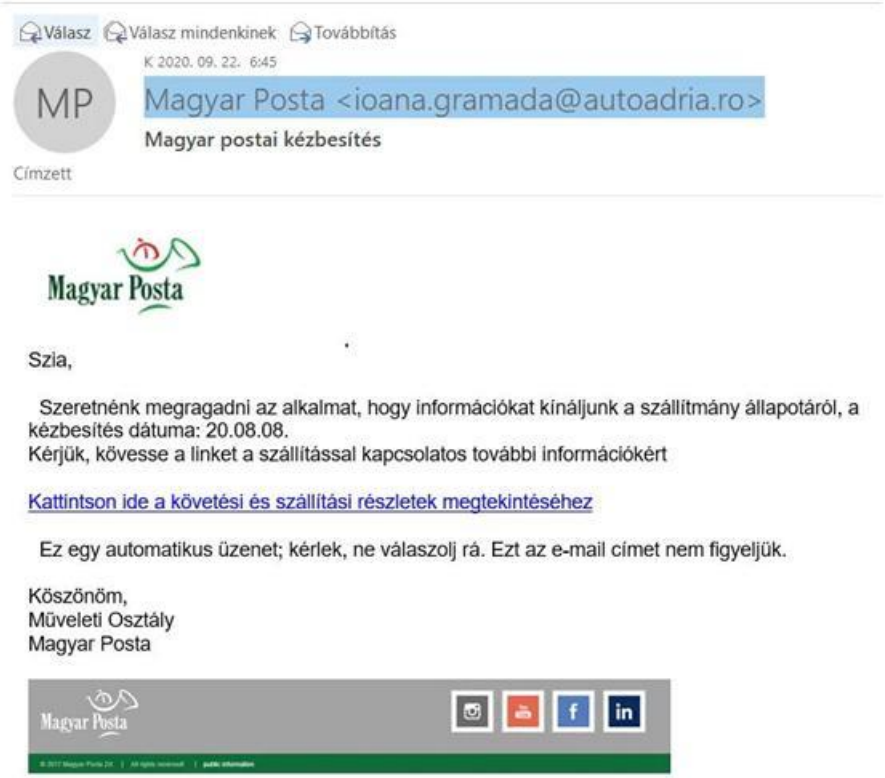
© 2023 OTP Bank

1. ábra. ***https://www.otpbank.hu/portal/hu/Adathalaszat-korabbi***

Jellegzetességük ezeknek az üzeneteknek, hogy a megszólítás teljes mértékben személytelen, a megfogalmazott probléma pedig sürgetésre késztet, egyfajta pszichológiai manipulációt használva. Ez által a felhasználó hajlamos elhamarkodott, átgondolatlan lépést tenni.
Gyakori a már megszólalásig azonos, mégis gyanút keltő logó alkalmazása, azonban sok esetben a hivatalos emblémát jelenítik meg.
Milyen módon lehet biztosan felismerni egy ilyen üzenetet? Érdemes minden esetben megvizsgálni valóban indokolt volt-e az üzenet, és ellenőrizni a levél megfogalmazását is. Mindig szemügyre kell venni a feladó e-mail címét, ugyanis az eredeti e-mail nem hamisítható.



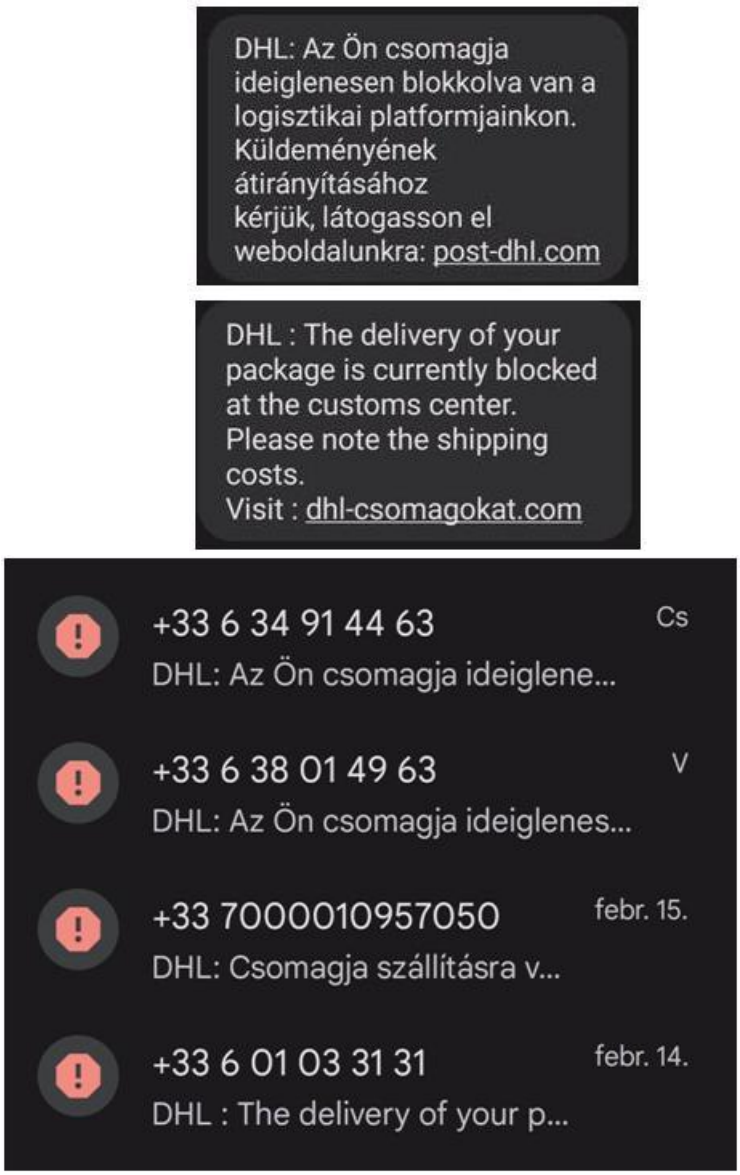
2. ábra. ***https://www.fws.hu/blog/hogyan-vedekezz-az-adathalasz-e-mailekkel-szemben***



3. ábra
https://www.telekom.hu/rolunk/telekom_vilaga/biztonsagi_tartalmak/csalas/adathalaszat

3. A harmadik, napjainkban egyre nagyobb rendszereséggel terjedő forma a smishing, azaz az SMS-ben érkező *spam*. 2022 októbrétől, napi szinten érkeznek bejelentések a fővárosi rendőrkapitányságra kéretlen üzenetekről, a legtöbbje külföldi telefonszámról. Tegyük föl, hogy ön rendelt egy terméket online. Az oldalt is ismeri,

biztonságos. A terméket egy országon kívüli cég forgalmazza, amit majd át kell hozni a határon.
A rendelést követő napon egy különös üzenettel kerül szembe:



4. ábra ***a szerzők saját telefonjára érkezett üzenetek***

A „DHL” küldte? Hitelesnek tűnik? A helyesírás stimmel. A csomag külföldről érkezik, tehát előfordulhat, hogy megállították egy vámvizsgálaton, vagy bármilyen más, a felhasználó/vásárló által nem ismert, sokszor csak feltételezett bürokratikus intézmény „tette arra rá a kezét.” A felhasználó/vásárló gyakran pánikba esik: mi történhetett a csomagjával, mert tényleg csomagot rendelt, amely valóban késhet.

Az üzenet azonban hamis. A megbízható cégek honlapján fellelhető egy részletes lista, arról, hogy milyen futárszolgálatokkal dolgozik együtt. Mindegyiknek külön fel van tüntetve telefonos és e-mail-es elérhetőségük. A fent említett esetben viszont nem szerepelt a ”DHL”. Az üzenet tüzetes átvizsgálása pedig egyértelművé teszi azt is, hogy a weboldal címe nem is s “DHL”-re mutat.

3. Összegzés

A tanulmányban bemutatott példák olyan, az online térben mozgó átlagfelhasználót fenyegető veszélyhelyzeteket teremthetnek, amelyek tudatos felkészüléssel, körültekintő, józan gondolkodással, valamint egy kis odafigyeléssel elháríthatóvá válnak. Ugyanakkor figyelembe kell venni, hogy „*sok felhasználó belefáradt a spamek fogadásába és eltávolításába. 2012-ben egy felmérés szerint Ázsiában naponta körülbelül 30%-a a mobiltelefonon érkező sms-knek spam. Így az egyik fontos dolog, amit figyelembe kell venni, hogy a felhasználó időt pazarol és bosszankodik a spam üzenetek olvasása és törlése miatt, és ezek az sms-k talán csalásra is alkalmasak.*” [7]

A fő tanulság, hogy biztonságtudatos gondolkodással, tudatosan irányított figyelemmel, és óvatossággal kell a modern info-kommunikáció nyújtotta lehetőségekkel élni. Az adatok biztonsága rendkívüli fontossággal bír, így a felhasználó nyugodtan lehet és kell, hogy gyanakvó – nevezzük inkább biztonságtudatos – legyen. Ennek a biztonságtudatos viselkedésnek az elemei többek között:

- a megbizonyosodás, hogy a küldő e-mail címe vagy weboldala egyezik-e a hivatalosan megadott oldallal/címmel,
- az ismeretlen, elsősorban külföldi telefonszámról érkező hívásfogadás elutasítása
- az ismeretlen hívóazonosítóról érkező üzenetek megnyitásának kerülése, amennyiben ez megtörtént, akkor a pénzintézet irányába történő jelzést küldése szükséges.

Végső következtetésként elmondható, hogy bár a kiberbiztonság, és az ahhoz csatolódó biztonságtudatos magatartás az utóbbi években sokat fejlődött, azonban máig igaznak tekinthető Hankiss Ágnes egy évtizeddel korábban megállapítása: „*Mindenekelőtt két olyan állítás fogalmazható meg, amelyben mindenki egyetért, aki így vagy úgy kiberbiztonsággal foglalkozik. Az egyik, hogy a kiberbiztonság, illetve a kiberfenyegetettség a következő évtizedek egyik legfőbb biztonsági kihívását jelenti. A másik, hogy a kiberbiztonság megvalósítására irányuló erőfeszítések jelenleg elég fragmentáltak, azaz a különböző szereplők hatékony együttműködése még hagy maga után kívánnivalót.*” [8]

Irodalomjegyzék

[1] Johanyák Zs. Cs., Pásztor A.: Iot rendszereket fenyegető támadások, Gradus 2023/1, DOI: https://doi.org/10.47833/2023.1.CSC.001

[2] Győrffyné Holló K.: Az információbiztonság jelentősége és története, Gradus 2021/2, pp.102-112, DOI: https://doi.org/10.47833/2021.2.CSV.001

[3] Parlak, B., Üniversitesi, A.: Sms Spam Filtering For Turkish And English Dataset, In.: Kültür, Bilgin & Yayınları, Sanat: Current Debates on Natural and Engineering Sciences, https://www.researchgate.net/publication/371316027_SMS_SPAM_FILTERING_FOR_TURKISH_AND_ENGLISH_DATASETS

[4] Chaturvedi, S A., Purohit, L.: Feature Selection-Based Spam Detection System in SMS and Email Domain, In.: Sentiment Analysis and Deep Learning, Proceedings of ICSADL 2022, DOI: 10.1007/978-981-19-5443-6_4

[5] Tarafdar, A., Halder, C., Dash, D.: Spam Detection using Reference Text: A Preliminary Study for Spam Ground Truth Generation, Research Square DOI: 10.21203/rs.3.rs-3099460/v1

[6] Boda J. (főszerk.): Rendészettudományi Szaklexikon. Dialóg Campus, Budapest. 2019.

[7] Mansoor, H. H., Hameed Shaker, S.: Using Classification Techniques to SMS Spam Filter, International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-8 Issue-12, pp. 1734-1739, DOI: 10.35940/ijitee.L3206.1081219

[8] Hankiss Á.: Kiberbiztonság: az Európai Parlament feladatai. Magyar Rendészet.2013/klnsz. pp. 27-31.