Védelem Tudomány 2024. különszám - Természeti Katasztrófák Csökkentésének Világnapja
Nemzeti Közszolgálati Egyetem nemzetközi tudományos konferencia
Konferenciaközlemény

A vízkezelő üzemek 21. századi kihívásai, a lakosságvédelem aspektusaiból

21st-century challenges of water treatment plants through the public safety aspects

Vásárhelyi Örs László
Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar,
Katonai Műszaki Doktori Iskola
doktorandusz
Email: vasarhelyi.ors.laszlof@stud.uni-nke.hu
ORCID: 0000-0002-6752-2546

Bevezetés

A 21. században a vízkezelő üzemek, mint kritikus infrastruktúrák, egyre növekvő kiberbiztonsági fenyegetéssel néznek szembe. [1] A kutatás a vízkezelő üzemek elektronikus információs rendszereit és kiber-fizikai (OT) rendszereit érintő kibertámadások lakosságvédelmi vonatkozásaira összpontosít, különös tekintettel az ivóvíz potenciális szennyezésére és az azt követő elhárító tevékenységekre. A legalapvetőbb erőforrásunk, mint a víz nélkülözhetetlen az élethez, így a szennyvíz és ivóvíz kezeléssel foglalkozó vállalatok védelme kiemelten fontos, hiszen súlyos egészségügyi kockázatot jelenthet ezen vállalatok ipari folyamatainak kompromittálódása.

Jelen tudományos munka ismerteti a közelmúltban bekövetkezett biztonsági események által a leggyakoribb támadási formákat, a vízkezelő rendszerek sebezhetőségeit, valamint az ilyen események elhárítására, beleértve a lakosságvédelmet, helyreállítására és utólagos kivizsgálására vonatkozó tevékenységeket.

A publikáció a jövőre vonatkozóan javaslatokat fogalmaz meg ezen üzemek rezilienciájának fokozására. Így hazánk vízbiztonságán keresztül jelentősen csökkennének az ellátási zavarokból fakadó társadalmi és gazdasági kockázatok, valamint a lakosságvédelmi képesség fokozódna.

Introduction

As critical infrastructures in the 21st century, water utilities face an increasing cyber security threat. This research focuses on the public security implications of cyber-attacks on electronic information systems and cyber-physical (OT) systems of water utilities, with a particular focus on the potential contamination of drinking water and subsequent response activities. Water, our most basic resource, is essential for life, and the protection of companies involved in the treatment of wastewater and drinking water is of paramount importance, as there is a serious health risk if their industrial processes are compromised.

This scientific work describes the most common forms of attack caused by recent security incidents, the vulnerabilities of water treatment systems, and the activities involved in responding to such incidents, including public security, recovery, and post-investigation.

The publication makes suggestions for the future to enhance the resilience of these plants. This would significantly reduce the social and economic risks from supply disruptions through water security in our country and increase the ability to protect the citizens.

Kulcsszavak: lakosságvédelem, kibertámadás, vízkezelő üzemek, kritikus infrastruktúra

Keywords: protection of civilians, cyberattack, water utility, critical infrastructure

A vízkezelő üzemek kompromittálásának lehetőségei

A mai modern ipari infrastruktúrák rendszerelemei nemcsak hagyományos fizikai berendezésekből vagy elektronikus információs rendszerekből épülnek fel, hanem úgynevezett kiber-fizikai rendszerek (másnéven OT) is részét képezik, ezek olyan integrált rendszerek, amelyekben a fizikai folyamatok és a digitális vezérlés szorosan összekapcsolódik. Az ipari rendszerek és rendszerelemek általában be vannak csatornázva egy felügyeleti rendszerbe, amit SCADA rendszernek neveznek, ezek lehetővé teszik a vállalatok számára, hogy valós időben nyomon kövessék és irányítsák a gyártási folyamatokat. Amennyiben egy támadó sikeresen hozzáfér egy ilyen rendszerhez, akkor könnyedén képes lehet az ipari folyamatok bizonyos paramétereit felülírni, ezzel pedig akár súlyos, a fizikai világra is kiható károkat okozni egy üzemben.

Hogyan lehetséges ez? Manapság már nem elég az ipari berendezéseket a jogosulatlan fizikai hozzáféréssel, természeti és civilizációs környezeti hatásokkal szemben kialakított épületekkel védeni. [2] A vízkezelő üzemek esetén alkalmazott kiber-fizikai rendszerek tervezése és üzemeltetése során kevesebb hangsúlyt fektetnek a biztonság kérdésére, mint az informatikai rendszerek esetén. Sokszor az IT vagy irodai környezet nem kerül megfelelően logikailag leválasztásra a gyártó vagy OT hálózattól. Így a támadók az IT infrastruktúrán keresztül képesek „átszivárogni" az OT környezetre. Ha ezek a környezetek nincsenek megfelelően elkülönítve (például tűzfalak vagy szegmentációs szabályok révén), egy támadó kihasználhatja a közös kommunikációs csatornákat az IT-rendszerről az OT-rendszerre való átjutáshoz.

A nem megfelelő konfiguráció miatt az internet felé feleslegesen nyitott portok utat biztosíthatnak a támadók számára az OT rendszerek eléréséhez. Továbbá a rossz konfigurációin túlmenően, a legtöbb ipari hálózat elavult kommunikációs protokollokat alkalmaz, mint például a modbus-t, ami számos egyszerűsége miatt népszerű lett, ugyanakkor nem rendelkezik megfelelő integritással ahhoz, hogy megvédje az adatforgalmat a jogosulatlan lehallgatással - vagy DDoS támadásokkal szemben. Továbbá a Modbus-t alkalmazó eszközök sebezhetőek lehetnek a parancsinjekciós (command injection) támadásokkal szemben, ami a rendszer jogosulatlan irányításához vagy manipulálásához vezethet. [3]

A vízkezelő üzemek esetén általában a víz kezeléséhez használt kemikáliák hozzáadott mennyiségét dúsítják fel. Mely következtében az ivóvíz vegyi anyag koncentrációja meghaladhatja a fogyasztásra javasolt értékek szintjét, ezzel pedig az emberi fogyasztásnak az egészségügyi kockázata megnőhet. Hazánk esetén az 5/2023 (I.12.) Korm. rendelet 1. sz. melléklete például a fertőtlenítés céljából használt klór-dioxid vagy nátrium-hipoklorit vagy kálcium-hipoklorit miatt az ivóvízben maximum 0,25mg/l klorit valamint klorát koncentrátum lehet (max. évi 30 napig 0,70mg/l előfordulhat). A nagy mennyiségű klór fogyasztásnak akkut hatásai is vannak, mint a hányinger, hányás, hasmenés, valamint izomgyengeség. Természetesen ehhez az kell, hogy a támadók jelentős mennyiségű fertőtlenítőszert adagoljanak az ivóvízhez. Továbbá az is egy lehetséges forgatókönyv, hogy a fertőtlenítésre használt klórgázt, amennyiben automatizált mechanizmusok révén történik az

adagolása, egy kiengedő szelep kinyitásával a környezetbe juttatják, ezzel veszélyeztetve az ott tartózkodó munkavállalók életét. A klórgáz már kis koncentrációban is halálos hatású lehet az emberi szervezetre, valamint a támadó ezzel is fennakadást idézhetne elő az üzem-folytonosságban. [4]

A támadóknak dönthetnek úgy is, hogy fertőtlenítési folyamatokat felfüggesztik és kezeletlen víz kerül a háztartásokba. Ekkor fertőző ágensek lesznek megtalálhatók a vízben, mint például baktériumok vagy vírusok, ezek akár e. coli fertőzést okozhatnak, melyeknek akkut egészségügyi hatásai vannak. [5] Budapest esetén 750 parti szűrésű kút biztosítja a nyersvíz kinyerését, ezek a kutak közel ivóvíz minőségű vizet adnak a természetes tisztítási folyamatoknak köszönhetően. Így hazánk fővárosának vize, vélhetően fogyasztható maradna fertőtlenítő fázis nélkül is. [6]

Támadás következményei

A vízkezelő vállalatokat érő kibertámadásoknak hatásai három kritikus területen jelentkezhetnek, a támadók mögöttes motivációjától függően. Az első a **nemzetbiztonsági hatás**: ezek a létesítmények alapvető fontosságúak az állam stabil működése szempontjából, és bármilyen zavara veszélyezteti a gazdaságot, valamint a lakosság biztonságát.

Másodszor, ott van a **lakosság védelmét kiváltó hatás**, amennyiben a vízellátás megszakad vagy szennyezetté válik, az azonnali krízist és pánikot idézhet elő a mindennapi életben, és komoly egészségügyi következményekkel járhat.

A kritikus infrastruktúrák, köztük a vízkezelő üzemek, sérülése a **katonai műveleti** területeken jelentős hatást gyakorolhat a hadműveletek logisztikai folyamataira, tervezésére és végrehajtására. Ezek az üzemek nemcsak a civil lakosság ellátását biztosítják, hanem kulcsszerepet játszhatnak a katonai objektumok ivóvízellátásában is. A fegyveres konfliktusok során könnyen célponttá válhatnak, hiszen a működésük akadályozása, vagy az ivóvíz minőségének befolyásolása közvetlen hatást gyakorolhat a hadsereg ellátási láncára és moráljára.

A közelmúltbéli vízkezelő üzemek elleni támadások

American Water

Az American Water az Amerikai Egyesült Államok egyik legnagyobb víz- és szennyvízszolgáltatója, 14 államban nyújt vízszolgáltatást több mint 14 millió ember számára, beleértve 18 katonai bázist is. A 2024. október 3-ai támadást követően a szervezet észlelte a hálózatában és rendszereiben történő illetéktelen hozzáférést, és azonnali válaszintézkedéseket tett. Ennek keretében a MyWater nevű ügyfélportál működését leállították és a szervezet számlázó rendszerét is lekapcsolták.

A támadók által végrehajtott műveletek nem meghatározhatók pontosan, mert nem hozták nyilvánosságra, de történhetett zsarolóvírus (ransomware) telepítése, személyes adatok jogosulatlan megszerzésére irányuló kibertevékenységek, vagy olyan műveletek végrehajtása, ami a szervezet ügy- és üzletmenetének folytonosságát vette célba.

A szervezet időben életbe léptette a biztonsági eseménykezelő eljárásait, valamint a hatóságokat értesítette az esetről, továbbá külsős kiberbiztonsági szakértőket vontak be az elhárításba és kivizsgálásba, ezeknek köszönhetően az szenny- és ivóvíz szolgáltatás nem sérült, a lakosság nem került közvetlen veszélybe. Az American Water az esemény kivizsgálását közösen végzi a bűnüldöző szervekkel és szakértőkkel, melynek célja, hogy meghatározzák a támadás technikai tulajdonságait, valamint hatókörét és természetesen az elkövetők azonosítása is célja.

A támadás mögött valamely külföldi állam hacktivistáit sejtik, azonban erre vonatkozóan nem kerültek evidenciák nyilvánosságra.

A szervezet a nem tervezett rendszer leállások mellett, további negatív hatásokat is elszenvedhetett, vélhetően nagy mennyiségű ügyfél adat kompromittálódhatott, továbbá a szervezetet reputációbéli veszteség is érte.

A vállalat úgy nyilatkozott, hogy nem hiszi, hogy a támadás és annak hatásai negatívan érintette volna bármelyik víz- vagy szennyvízlétesítményét, emellett nem számolt be a vízminőség vagy a szolgáltatás veszélyeztetéséről. [7]

Arkansas Water

Kansas állam, Arkansas nevű kisvárosának vízkezelő üzemét ez év szeptemberében kibertámadás érte. A Water Information Sharing and Analysis Center (WaterISAC) szerint valószínűsíthető, hogy zsarolóvírus támadás történt. A támadás ebben az esetben már kihatott a létesítmény általános ügy- és üzletmenetére. Az ipari rendszereit az üzemnek le kellett választania a hálózatról a támadást követően. Az ipari folyamatok irányítását a továbbiakban manuálisan végezték, hogy biztosítsák a vízellátás folyamatosságát és biztonságát. A város vezetése azonnal értesítette a hatóságokat, és együttműködött a Szövetségi Nyomozó Irodával (FBI) és a Belbiztonsági Minisztériummal (DHS) a támadás kivizsgálása érdekében. Ebből kifolyólag az esetről bővebb információk nem érhetők el publikusan

A település városmenedzsere[1] úgy nyilatkozott, hogy a vízellátás biztonságos maradt, és nem történt szolgáltatáskimaradás. Az üzem manuális működésre történő átállása csupán elővigyázatossági okokból kifolyólag történt és a helyzet megoldásáig ebben a módban marad. [8]

A város saját honlapján közzétette a lakosok megnyugtatása érdekében, hogy a biztonsági esemény ellenére a vízellátás biztonságban van és nyugodtan fogyasztható a csapvíz. [9]

A támadást követően a Cybersecurity and Infrastructure Security Agency (CISA) figyelmeztetést adott ki, miszerint a víz ágazat kiber-fizikai rendszerei továbbra is célpontjai a kibertámadásoknak, valamint figyelmeztetett, hogy az ipari rendszerek sokszor alapértelmezett azonosítási és hitelesítési eszközöket használnak, amik az egyszerűbb technikai támadásoknak sem képesek ellenállni. [10]

Libanoni üzemek elleni támadás

2024 szeptemberében az izraeli Red Evil más néven We Red Evils hacktivista csoport részletes bejelentést tett saját online platformjain, hogy sikeres támadásokat hajtott végre 14 vízkezelő létesítmény ellen Libanon déli régiójában és Bejrútban. A csoport szerint az ipari irányítórendszerekbe (ICS) történő behatolásuk célzott akció volt, amely során manipulálták a vízkezelési folyamatokat, beleértve a klórszintek szabályozását. A csoport nyilatkozata szerint ezek az akciók a Hezbollah tagjai és infrastruktúrája ellen irányultak, céljuk politikai üzenetküldés és károkozás volt.

Bár a Red Evil csoport állítása szerint sikeresen módosították a klórszinteket, a szakértők szerint a hacktivisták gyakran eltúlozzák a támadásaik sikerességét és az okozott károk nagyságát. A HMI-k és a programozható logikai vezérlők (PLC-k) adminisztrátori interfészei gyakran elérhetők az interneten keresztül, és sokszor teljesen védtelenek, vagy könnyen kitalálható alapértelmezett jelszavakkal hozzáférhetők. [11] A csoportnak azonban a katonai és politikai célból végrehajtott akciója, valószínűleg pánikot válthatott ki a dél-libanoniakból, így pszichológiai hadviselés szempontjából mindenképpen egy sikeres művelet volt.

Ivóvíz szennyezését követő lakosságvédelmi feladatok Magyarország esetén

[1] szakmai vezető, akit az önkormányzati testület választ meg angolszász területeken

Hazánkban a Nemzeti Népegészségügyi és Gyógyszerészeti Központ (NNGYK), valamint a BM OKF Országos Polgári Védelmi Főfelügyelőségnek és a helyi polgári védelmi szervezeteknek lehetnek elsődleges lakosságvédelmi feladatai. Az NNGYK felelős a vízminőség és a közegészségügy felügyeletéért Magyarországon. Továbbá felügyeli az ivóvíz-biztonsági tervek (VBT) kidolgozását és végrehajtását hazánkban. A VBT-k a vízellátó rendszerek lehetséges veszélyeinek azonosítására, a kockázatok csökkentésére és az egészséges ivóvízellátás folyamatos biztosítására szolgáló dokumentumok. Ezenkívül az NNGYK közhiteles nyilvántartást vezet az ivóvízellátásban használt anyagokról, termékekről és technológiákról, biztosítva azok megfelelőségét és biztonságosságát. [12]

Amennyiben a vízminőség romlana az NNGYK egyből érzékelné a változást és értesítené a lakosságot az óvintézkedések megtételéről, valamint kötelezné az állami és szociális intézményeket az általa meghatározott óvintézkedések betartására. A kiesett kritikus infrastruktúra helyreállításában is közreműködnek.

A polgári védelem, valamint a katasztrófavédelmi ügyelet a lakosságot a MoLARi rendszeren vagy más csatornákon keresztül (pl. helyi média szolgáltatók, SMS) értesítené a kialakult vészhelyzetről és a követendő magatartási szabályokról. Jelenleg hazánkban 768 db lakosság riasztó-tájékoztató végpont került kialakításra a veszélyes üzemek környékén a lakosság magasabb szintű biztonságának a garantálása végett. [13] A polgári védelem a teljes helyreállításig gondoskodna az alternatív vízellátás megszervezéséről és biztosításáról, valamint, ha az ivóvíz szennyezetté válik, akár bakteriális ágensek -, akár fertőtlenítésre használt kemikáliák koncentrációja növekedik meg nagy arányban, a víz mentesítésében, ha lehetséges az egészségre káros víz izolálása, akkor abban is részt vesznek. Amennyiben az üzemben az üzemfolytonosságot veszélyeztető károk keletkeztek és a helyreálltás vélhetően hosszabb időt vesz igénybe, a hatóság távolsági védelmet is alkalmazhat, azaz ideiglenesen kitelepítheti az érintett lakosságot, és biztonságosabb területen kerülnek elhelyezésre. Az ivóvíz szolgáltatás helyreállítását követően pedig a kitelepített lakosság visszatelepülhet. [14]

Ezek a lakosságvédelmi intézkedések minimalizálják a pánikot, megakadályozzák a vízszennyezést és annak egészségügyi következményeinek terjedését, és biztosítják a társadalom gyors visszatérését a normális, megszokott állapotba. A jövőre nézve pedig az Európai Bizottság uniós katasztrófavédelmi rezilienciacélokat fogalmazott meg, többek között a katasztrófariasztás, illetve a korai előrejelzés hatékonyabbá tételére vonatkozóan, és a lakossági felkészítésnek fejlesztésére és a kockázatokkal kapcsolatos tudatosság fokozására vonatkozóan. Ennek köszönhetően a jövőben a legújabb technológiák felhasználása mellett rugalmas, gyors és hatékony lakosságvédelem valósítható majd meg. [15]

Biztonsági események utólagos kivizsgálása

A kibertámadások kivizsgálásakor a digitális forensic (kriminalisztika) tudományterület segítségével megvalósulhat a támadás eredetének, módszereinek és hatásainak pontos feltárása, ezáltal lehetőség nyílik az elkövetők azonosítására és a jogi lépések megtételére. A folyamat során a szakértők speciális eszközöket és technikákat alkalmaznak a digitális bizonyítékok gyűjtésére és elemzésére, biztosítva azok integritását és hitelességét. A digitális forensic nemcsak a bűnüldöző szervek számára fontos, hanem a vállalatoknak is segít a biztonsági rések azonosításában és a jövőbeni támadások megelőzésében. Módszertanaira számos nemzetközi szabvány és ajánlás létezik, az amerikai NIST SP 800-86-os ajánlás 4 fő lépést határoz meg a folyamat során: az adatok azonosítását és gyűjtését, majd az összegyűjtött evidenciák vizsgálatát, ezeknek az eredményeknek az elemzését és az összefüggések feltárását például gyanús adatátviteli minták alapján, végül pedig az esemény körülményeinek és az evidenciaként begyűjött adatok dokumentálását, bírósági eljárásoknak megfelelő tartalmi és formai követelményekkel összhangban. [16]

Összegzés

Napjainkban a vízkezelő üzemek számos kihívással szembesülnek, ezek közül kiemelkednek a kibertámadások növekvő fenyegetése. Az ilyen típusú támadások nemcsak az alapvető szolgáltatások ellátásának folytonosságát veszélyeztetik, hanem jelentős lakosságbiztonsági problémákat is felvethetnek. A vízkezelő szervezetek és más alapvető szolgáltatást nyújtó szervezetek kiberkitettsége komoly nemzetbiztonsági kockázatot jelent. A dolgozat által bemutatott esettanulmányok rávilágítanak arra, hogy az ilyen jellegű támadások ellen gyors és hatékony reagálás szükséges, valamint megfelelő felkészültség, ami magába foglalja a biztonsági eseménykezelési -, üzletmenet-folytonossági - és katasztrófahelyreállítási képességeket.

A vízkezelő szervezeteket érő kibertámadások vagy szabotázs akciók a lakosság egészségét is veszélyeztethetik az ivóvíz szennyezése által vagy épp a szolgáltatás folytonosságának megszakadása révén, valamint ezek mellett jelentős mennyiségű személyes adat kompromittálódhat. Továbbá a dél-libanoni eset jól példázza, hogy az ipari vezérlő rendszerekhez történő jogosulatlan hozzáférésnek katonai műveleti és politikai céljai is lehetnek, ami tovább fokozza egy támadás kockázatát ezen létfontosságú rendszerelemek ellen.

A lakosságvédelem érdekében kulcsfontosságú a hatóságok azonnali beavatkozása, a víz minőség faktorainak folyamatos monitoringja, az alternatív vízellátási pontok biztosítása, valamint az állampolgárokkal történő hatékony kommunikáció az óvintézkedésekről.

A jövőre nézve az infrastruktúrák rezilienciáját a teljes Unión belül egységes, magas szintűre kell emelni, aminek elengedhetetlen része, hogy az alapvető szolgáltatást nyújtó szervezetek felett felügyeletet gyakorló hatóságok között, zökkenőmentes, gyors és hatékony szakmai együttműködés alakuljon ki. Továbbá fontos lenne az ipari vezérlő rendszerek megfelelő védelme érdekében kialakítani egy olyan követelménykatalógust, melyet az alapvető szolgáltatást nyújtó szervezetek saját ipari környezetükben képesek implementálni, ezzel pedig az ipari folyamatok digitális sérülékenységeinek kockázatai jelentősen csökkennének.

Irodalomjegyzék

[1] Ambrusz J., Dobor J. és Vásárhelyi Ö., „Létfontosságú rendszerek,- rendszerelemek rezilienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében," *Polgári Védelmi Szemle,* kötetkülönszám, pp. 57-69, 2024.

[2] Érces G., Vass G. és Ambrusz J., „Épületek károsító hatásokkal szembeni rezilienciájának jellemzői," *Polgári Védelmi Szemle,* XV. évfolyam, DAREnet projekt Különszám, pp. 117-130, 2023.

[3] Veridify Security, „Modbus Security Issues and How to Mitigate Cyber Risks," [Online]. Elérhetőség: https://www.veridify.com/modbus-security-issues-and-how-to-mitigate-cyber-risks/. (2024.11.14.)

[4] Dobor J., „Veszélyes gázok felhasználási lehetőségei az iparban és a mezőgazdaságban, illetve e tevékenységek kockázatai," *Hadmérnök,* XIII. évf., "KÖFOP" szám, pp. 28-42, január 2018.

[5] Kovács Z., Ivóvíztisztítás és víztisztaságvédelem, XXVI. kötet, Veszprém: Pannon Egyetem, 2013.

[6] Fővárosi Vízművek, „Költséghatékony és biztonságos ivóvízellátás parti szűrésű ivóvízellátás fejlesztése és rehabilitációja megvalósításával (SAFEWAT.HU)," 2023.08.07. [Online]. Elérhetőség: https://www.vizmuvek.hu/hu/kezdolap/vizplusz-lakossagi/vizplusz-erdekessegek/hir/6557. (2024.11.01.)

[7] Kerner M. S., „The American Water cyberattack: Explaining how it happened," 2024.10.18. [Online]. Elérhetőség: https://www.techtarget.com/whatis/feature/The-American-Water-cyberattack-Explaining-how-it-happened (2024.10.30.)

[8] Water ISAC, „Incident Awareness – Ransomware Attackers Target Kansas Water Treatment Facility," 2024.09.24. [Online]. Elérhetőség: https://www.waterisac.org/portal/incident-awareness-%E2%80%93-ransomware-attackers-target-kansas-water-treatment-facility. (2024.11.10.)

[9] City of Arkansas, „City of Arkansas City Faces Cybersecurity Incident," 2024.09.22. [Online]. Elérhetőség: https://www.arkcity.org/environmental-services/page/city-arkansas-city-faces-cybersecurity-incident?. (2024.11.10.)

[10] Nemzeti Kibervédelmi Intézet, „Kibertámadás érte az amerikai vízügyi ágazat egyik létesítményét," 2024.09.26. [Online]. Elérhetőség: https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-erte-az-amerikai-vizugyi-agazat-egyik-letesitmenyet/.(2024.10.30.)

[11] Kovacs E., „Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks," 2024.09.26. [Online]. Elérhetőség: https://www.securityweek.com/israeli-group-claims-lebanon-water-hack-as-cisa-reiterates-warning-on-simple-ics-attacks/. (2024.10.30.)

[12] Nemzeti Népegészségügyi Központ, Módszertani levél Útmutató ivóvíz-biztonsági tervrendszerek kiépítéséhez, működtetéséhez, Budapest: NNK Közegészségügyi Laboratóriumi Főosztály, 2019.

[13] BM OKF, „MoLaRi-rendszer," [Online]. Elérhetőség: https://www.katasztrofavedelem.hu/49/molari-rendszer.(2024.11.12.)

[14] „2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról," [Online]. Elérhetőség: https://njt.hu/jogszabaly/2011-128-00-00. (2024.09.25.)

[15] Vass Gy., Ambrusz J., Restás Á., Varga F. és Kátai-Urbán L., „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében," *Belügyi Szemle,* 72 . évfolyam, 5. szám, pp. 815-833, 2024.

[16] Kent K., Chevalier S., Grance T. és Dang H., „Guide to Integrating Forensic Techniques into Incident Respons," National Institute of Standards and Technology (NIST), 2006.08. [Online]. Elérhetőség: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. (2024.09.10.)