Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ZAŠTITA OD CYBER NAPADA I UPRAVLJANJE PODACIMA NA KRITIČNOJ INFRASTRUKTURI POMOĆU INOVACIONIH 3D A-LATA GIS I BIM

CYBER ATTACK PROTECTION AND CRITICAL INFRASTRUCTURE DATA MANAGEMENT WITH THE INNOVATIVE 3D GIS AND BIM INSTRUMENTS

Pregledni naučni rad

Garaplija Edin
Rizvo Samir[205]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Zaštita kritične infrastrukture (KI) je jedan od ključnih bezbjednosno/sigurnosnih izazova današnjice. Sve učestalije prirodne katastrofe izazvane globalnim klimatskim promjenama, tehničko-tehnološke nesreće i udesi, te teroristička prijetnje i drugi antropogeni rizici nastali usljed ljudskog nemara ili namjere, su realna svakodnevna prijetnja po kritičnu infrastrukturu svakog razvijenog društva.

Ciljevi rada (naučni i/ili društveni): Bosna i Hercegovina, zemlja složenog društveno-političkog uređenja, na svom putu ka Euro-Atlantskim integracijama, kao i njena kritična infrastruktura, sigurno predstavljaju osnovanu bazu za realan scenario od gore pobrojanih rizika.

Metodologija/Dizajn: Ubrzanim razvojem tehnologije, prijetnje po KI, nisu samo od gore pobrojanih rizika i opasnosti, već i od sve učestalijeg "IT terorizma", "cyber napada" na pojedince i institucije razvijenih zemalja i njihovu KI.

Ograničenja istraživanja/rada: Samo NATO je mjesečno preko 500 puta meta "Cyber napada". Međunarodnim standradima i pravnim naslijeđem su definisane standardne operativne procedure za kolektovanje, analizu i razmjenu podataka od važnosti za pojedinca i organizaciju.

Rezultati/Nalazi: Radom se daje prikaz korelacije ove regulative sa novim IT tehnologijama današnjice i budućnosti, Geo-reference information system (GIS) i Building Intelligence Modeling (BIM), koje predstavljaju globalne alate za identifikaciju, analizu i vrednovanje podataka, te njihovu sigurnu pohranu i upotrebu u svakodnevnim zadacima zaštite kritične infrastrukture.

Generalni zaključak: Također, ovim radom se daje osvrt na pitanje zaštita od zloupotrebe i "presretanja" podataka od posebne važnosti za zaštitu KI.

[205] *Doktorant Edin Garaplija, predsjednik Naučnog odbora Asocijacije za upravljanje rizicima u BiH, Dr. Sc. Samir Rizvo, pomočnik ministra sigurnosti/bezbjednosti BiH za međunarodnu saradnju*

Opravdanost istraživanja/rada: Bosna i Hercegovina na svom putu priključenja EU mora ubrzanim koracima poduzeti sve neophodne mjere, kako bi sustigla zemlje regiona u pogledu zaštite kritične infratsrukture i borbe protiv terorizma, pa je s tim u vezi, od izuzetne važnosti institucionalizacija i široka primjena "pametnih" alata za zaštitu sistema kritične infratrukture i ključnih podataka za njihovo nesmetano funkcionisanje.

Ključne riječi
kritična infrastruktura, integrisana zaštita, cyber napad, GIS, BIM

Abstract
Reason for writing and research problem (s): Critical Infrastructure Protection (CI) is one of the key security / security challenges of today. Increasingly occurring natural disasters caused by global climate change, technical and technological disasters and disasters, and terrorist threats and other anthropogenic risks arising from human negligence or intent are a real daily threat to the critical infrastructure of every developed society.
Aims of the paper (scientific and/or social): Bosnia and Herzegovina, a country of complex socio-political order, on its path to Euro-Atlantic integration, as well as its critical infrastructure, is certainly a well-founded base for a realistic scenario of the risks listed above.
Methodology/Design: The accelerated development of technology, threats to CIs, are not only of the above risks and dangers, but also of the increasing frequency of "IT terrorism", "cyber attacks" on individuals and institutions of developed countries and their CIs.
Research/Paper limitation: NATO alone is the target of "Cyber attacks" over 500 times a month. International standards and legal heritage define standard operating procedures for the collection, analysis and exchange of data of importance to the individual and the organization.
Results/Findings: This paper presents the correlation of this regulation with new IT technologies of today and the future, Geo-reference information system (GIS) and Building Intelligence Modeling (BIM), which are global tools for identifying, analyzing and evaluating data, and their secure storage and use in the day-to-day tasks of critical infrastructure protection.
General Conclusion: Also, this paper addresses the issue of protection against misuse and "interception" of data of particular importance for the protection of CIs.
Research/Paper Validity: Bosnia and Herzegovina, on its path to EU accession, must take all necessary steps in order to catch up with the countries of the region in terms of critical infrastructure protection and counter-terrorism, and in this regard, institutionalization and the widespread use of "smart" tools are essential. protection of critical infrastructure systems and key data for their smooth functioning.

Keywords
critical infrastructure, integrated security, cyber attack, GIS, BIM.

1. UVOD

Iako se pojmom zaštite KI bave sve razvijene zemlje svijeta, možemo konstatovati da se po ovom pitanju najviše uradilo u SAD-u. Razvijena kritična a posebno energetska infrastruktura SAD-a potaknula je značajno njihov privredni razvoj u 20-21. vijeku. Bez stabilnog napajanja energijom, životi, zdravlje i napredak bi bili ugroženi, a privreda SAD-a ne bi mogla funkcionisati. Direktiva o predsjedničkoj politici SAD-a (PPD-21), identifkuje energetski sektor kao posebno kritičan, jer "omogućava funkcionisanje" ostalih sektora kritične infrastrukture. Ovdje moramo istaći da je više od 80% energetske infrastrukture SDA-a u vlasništvu privatnog sektora. Taj sektor opskrbljuje energijom infrastrukturu, domaćinstva i preduzeća, te druge bitne dijelove ekonomije i proizvodnje širom SAD-a.[206]

Zaštita kritične infrastrukture od internetskih i fizičkih prijetnji bit će ključni izazov za 2019. i naredni niz godina. Moramo uzeti u obzir činjenicu da je najviše prethodnih istraživanja koja tretiraju ugroze KI, obavljeno na području SAD-a. Ministarstvo domovinske sigurnosti (Department of Homeland Security) i Ministarstvo odbrane (Department of Defence) opisuje kritičnu infrastrukturu kao "fizičke i cyber sisteme i imovinu koja je toliko važna za Sjedinjene Države da bi njihovo onesposobljavanje ili uništenje imalo negativan učinak za fizičku ili ekonomsku stabilnost, javno zdravlje građana ili sigurnost zajednice." *Kritična infrastruktura je ugrožena od strane hakera, zločinačkih organizacija i unutar-državnih destruktivnih faktora, zbog njene vitalnosti za američku ekonomiju. Energetski sektor se ističe kao posebno ranjiv ako se uzme u obzir njegova prostorna zastupljenost i sveobuhvatnost: uključujući nuklearna postrojenja, hidro i termo elektrane, distribuciju, i prenosnu mrežu.* Peter Pry, član Komisije za EMP Kongresa i izvršni direktor Radne skupine za nacionalnu i domovinsku sigurnost stavio je prijetnje u zastrašujuću perspektivu: "*Prirodni EMP iz geomagnetske super oluje, kao što je Carringtonov događaj iz 1859. ili željeznička oluja iz 1921., nuklearni EMP napad od terorista ili nestabilnih država poput Sjeverna Koreja tokom nuklearne krize 2013. godine, predstavljaju egzistencijalne prijetnje koje bi mogle ubiti 9 od 10 Amerikanaca putem gladi, bolesti i društvenog kolapsa*".207

Bosna i Hercegovina je potpisnica Platforme Ujedinjenih Nacija za smanjenje rizika od katastrofa. Gledajući globalno, prekidi kritične infrastructure (KI) su uglavnom nastajali uslijed prirodnih katastrofa, koje su uzlaznim trendom prouzročile ogromne ljudske i materijalne gubitke. Ti su gubici mogli biti znatno manji, da su šira i lokalna zajednica i njena kritična infrastruktura bili pripremljeniji za ove izazove. U periodu 2008/2012. širom svijeta je preko 700 hiljada ljudi izgubilo živote, više od 1,4 miliona je povrijeđeno, a oko 23 miliona su ostala bez krova nad glavom. Više od 1,5 milijardi ljudi je pogođeno katastrofama na različite načine, uključujući žene, djecu i ranjive kategorije društva, te je ukupan

---

[206] US Department of Homeland Security Seal - https://www.dhs.gov/cisa/critical-infrastructure-sectors (31.05.19)
[207] Protecting Energy Critical Infrastructure a Key Challenge for DHS, February 16. 2019., Chuck Brooks

ekonomski gubitak bio veći od 1,3 triliona dolara. Na globalnom nivou oko 144 miliona ljudi je raseljeno uslijed posljedica od katastrofa. Ove su prirodne pojave ostavile dugotrajni trag na ekonomski napredak pogođenih zajednica, koje nisu bile, bez obzira na stepen svoje razvijenosti, pošteđene od prirodnih, tehničko-tehnoloških ili antropogenih rizika koji su imali katastrofalan uticaj na živote i zdravlje ljudi, ekonomiju, društveno političko uređenje i njenu KI.[208]

Aktuelne društvene okolnosti i sve izraženije globalne klimatske promjene, usložnjavaju problematiku zaštite kritične infrastrukture (KI), kako raznovrsnošću načina, tako i svojim intenzitetom. Neuobičajenost oblika ugrožavanja uzrokuje i posebne mjere i načine suprotstavljanja, kao odgovor na istovrsne bezbjednosno/sigurnosne probleme. Ovdje treba imati na umu da se pojam „bezbjednost" (bezbednost) odnosi na širu društveno-političku zajednicu, dok pojam „sigurnost" predstavlja uži kontekst vezan za određeni prostor ili organizaciju. Svjedoci smo sve više prirodnih, tehničko-tehnoloških i antropogenih rizika, koji izazivaju različite opasne incidente (opasnosti) sa velikim posljedicama po živote i zdravlje ljudi, njihovu imovinu i životnu sredinu. Po svom obimu, posljedicama i trajnim uticajima na održivu ekonomiju lokalnih i širih društvenih zajednica, pojedine opasnosti mogu imati karakter katastrofa ili vanrednih situacija.

Ovakvi oblici narušenih normalnih životnih situacija, predstavljaju izmjenjeno stanje društvene zajednice izazvano događajima velikih razmjera, kojima se parališe funkcionisanje društvenog sistema zemlje. Trendovi i štete izazvane ovakvim društvenim situacijama nužno nameću imperativ za organizovanim rješenjem u pogledu smanjenja i upravljanja rizicima u vanrednim situacijama sa posebnim akcentom na zaštiti KI.

Kada je riječ o odnosu nesreća i zaštite KI treba imati u vidu da je KI najčešće i sama pogođena vanrednom situacijom, te se očekuje njena hitna stabilizacija, kako bi svojom osnovnom djelatnošću uzela učešće u aktivnostima otklanjanja posljedica i stabilizacije života i rada na pogođenom području. Dakle, uspješno upravljanje rizicima od prirodnih i drugih nesreća, su u direktnoj vezi sa efikasnim sistemom zaštite KI. Mjere poput prevencije, pripremljenosti i adekvatnog odgovora povećavaju stepen sigurnosti KI.

Da bi smo bolje shvatili značaj organizovanog pristupa zaštiti KI, moraju se sagledati svi aspekti definisanja i shvatanja kritične infrastrukture, pojam kritične infrastrukture i njena klasifikacija. Bez funkcionisanja svih subjekata uključenih u integrisani sistem zaštite, nemoguće je u potpunosti ostvariti pouzdan sistem upravljanja rizicima i zaštitom KI u svim fazama njenog odvijanja. Poseban izazov za stručnu i naučnu javnost, predstavlja zaštita i upravljanje podacima na kritičnoj infrastrukturi, koja po svojoj namjeni i

[208] *Izvještaj za period 2002/2012. osiguravajuće kuće Munich RE*

strukturi, spada pod poseban značaj i šiti bezbjednosni interes za svaku razvijenu društveno-političku zajednicu.

Uporedna analiza međunarodnog upravno-pravnog okvira u oblasti zaštite KI, harmoniziranje zakonodavstva BiH sa upravno-pravnim okvirom zemalja susjedstva, te sa upravnom-pravnom regulativom i direktivama Evropske unije, trasiraju mapu puta kojim i naša zemlja treba što prije zakoračati i ispuniti svoje međunarodne obaveze i dostići najviše norme u oblasti zaštite KI. Obaveze vlasnika i operatera KI koje proizilaze procesom harmonizacije sa evropskim naslijeđem i Direktivom za zaštitu KI[209], te međunarodnim standardom za zaštitu podataka ISO 27000[210], kao i sa evropskom regulativom za zaštitu i upravljanje podacima GDPR[211], su da uspostavi efikasan preventivni sistem, ojača integrisani sistem zaštite i definiše standardne operativne procedure službama zaštite i spašavanja, a posebno sa aspekta zaštite, čuvanja i upravljanja osjetljivim podacima, bilo da se radi o onim organizaciono-procesnim ili ličnim podacima.

„Jedno od ključnih područja nacionalne i međunarodne sigurnosti na početku 21. stoljeća postalo je pitanje energetske sigurnosti i zaštite kritične infrastrukture. Kako je osiguranje transportnih pravaca i vlastite energetske infrastrukture postalo jednako važno kao i sama dostupnost energenata, tako je i zaštita energetske infrastrukture postala integralni dio koncepta zaštite sveukupne kritične infrastrukture. To se može vidjeti i na primjeru Republike Hrvatske koja je u situaciji da mora otpočeti sa sustavnim promišljanjem, planiranjem i provedbom aktivnosti vezanih uz postizanje energetske sigurnosti i zaštite kritične infrastrukture. Svjetski trendovi ukazuju na potrebu stvaranja nacionalnih strategija za zaštitu energetske i ostale kritične infrastrukture država, što se posljedično odražava i na potrebu redefiniranja njihovih temeljnih strateških dokumenata, prije svega, onih koji oblikuju sigurnosne strategije i sigurnosne politike.“[212]

Kritična infrastruktura (KI) je okosnica ekonomije, sigurnosti i zdravlja. Temeljno svojstvo KI sistema je njihova međuovisnost. Rezultat takvog svojstva je dobro poznati „domino“ efekt, što znači da poremećaj određenog IP-a može uzrokovati ogromne gubitke ne samo u razmatranom sektoru, nego i u drugim povezanim sektorima KI. Zbog toga KI mora biti sigurna i sposobna izdržati i brzo se oporaviti od svih predvidivih opasnosti. Čini se prilično jasno da je primjena metodologija procjene rizika na nižim i višim razinama i donošenje odluka na temelju tih metodologija vjerojatno najbolji postupak kojim se može pristupiti tako zahtjevnom cilju. Zapravo, metode analize rizika naširoko se koriste za donošenje odluka u područjima u kojima kvarovi opreme, ljudske pogreške, prirodni fenomeni ili

---

[209] Direktiva za zaštitu kritične infrastrukture 2008/114 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN
[210] ISO standardi za zaštitu podatakahttp://www.27000.org/
[211] GDPR -Evropska regulativa za upravljanje podacima 2016/679 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (18.07.19.)
[212] Energetska sigurnost i zaštita kritične infrastrukture: utjecaj na politike nacionalne sigurnosti, Talović Siniša

namjerno ljudsko ponašanje mogu izazvati značajne utjecaje na društvo. Sada je jasno da se i regija približava ovom konceptu, a što je i obveza koja proizlazi iz Direktive Vijeća 2008/114 / EZ[213].

Danas ne možemo govoriti o pojmu integrisanog modela zaštite KI, ako ga ne povežemo i sa modelom javno-privatnog partnerstva (Public Private Partnership – PPP), što je jedna od jasnih preporuka izdatih u Direktivi 2008/114 EC za zaštitu KI, kojom se ističe: "*S obzirom na vrlo značajnu uključenost privatnog sektora u nadzor i upravljanje rizicima, planiranje poslovnog kontinuiteta i oporavak nakon nepogode, pristupom Zajednice trebalo bi se poticati potpuno uključivanje privatnog sektora*". Ova preporuka je jednako važna i za zemlje članice, kao i za zemlje kandidate i potencijalne kandidate za članstvo u EU, među kojima se u ovom trenutku nalazi i Bosna i Hercegovina.

2. DEFINISANJE POJMA KRITIČNE INFRASTRUKTURE I EUROPSKO PRAVNO NASLIJEĐE ZA ZAŠTITU PODATAKA

U poslednjih dvadesetak godina, pitanje KI je postalo posebno značajno. Moderni stil života i zavisnost ljudi i privrede od struje, goriva, interneta (komunikacije uopšte) je svakim danom sve veća i veća. Bezbjednost KI je ključno pitanje savremene nacionalne bezbjednosti, jer ona predstavlja osnov za opstanak zajednice, a asimetrične prijetnje i potreba za efikasnim mjerama zaštite, postale su uobičajena potreba modernih društava.

Teroristički napad od 11. septembra 2001. godine u SAD, dao je novo značenje i novu dimenziju koncepta zaštite KI, a teroristički napadi u Madridu, Londonu, Moskvi, Mumbaiju i Islamabadu su samo potvrdili potrebu za novim pristupom u zaštiti KI. Pored toga, uragan Katrina u SAD, cunami u jugoistočnoj Aziji i cunami u Japanu su također pokazali da prirodne katastrofe mogu imati razorne posledice na infrastrukturu. Tako možemo zaključiti da je zaštita KI, u kontekstu savremenih globalnih prijetnji, predstavlja prioritetno pitanje za nacionalnu bezbjednost jedne države ili podneblja.

Potreba dinamičkog, proaktivnog i strateškog pristupa naročito je neophodna u procesu planiranja zaštite KI u uslovima različitih tipova kriznih i vanrednih situacija. Prije nego je sintagma „kritična infrastruktura" postala izuzetan predmet interesovanja u brojnim analizama koje su se odnosile na terorizam i unutrašnju bezbjednost, pojam „infrastruktura" osamdesetih godina bio je referentna tačka kreatora javne politike i bezbjednosti.

Naime, zbog sve većeg rizika povredljivosti i isključivanja iz redovnog funkcionisanja bilo je potrebno, za svaki sistem pojedinačno, predvidjeti odgovarajuće mjere. Infrastruktura se posmatrala kao logistička funkcija kojom se obezbjeđuju povoljni uslovi za kvalitetno

---

[213] *National critical infrastructure protection - regional perspective / Zoran Keković, Denis Ćaleta, Želimir Kešetović, Zoran Jeftić - Beograd : University of Belgrade - Faculty of Security Studies, 2013.*

obavljanje drugih funkcija logističke podrške. Porastom opasnosti od asimetričnih pretnji, naročito terorizma, u savremenim teorijskim analizama, ali i u praksi, sve je prisutniji izraz „kritična infrastruktura". Neposredno nakon terorističkih napada od septembra 2001. godine, KI postala je bitan i suštinski dio nacionalne bezbjednosti, a njena zaštita predstavlja jedan od prioriteta svake moderne države i društva.

U zavisnosti od kriterijuma a u cilju definisanja KI, postoji potreba za boljim sagledavanjem njenih različitih tipova. U principu, KI može biti od interesa za: državne, regione ili svijet, a to znači da možemo govoriti o nacionalnoj, regionalnoj (evropskoj, afričkoj, Evro-Azijskoj) i svetskoj (globalnoj) KI. S druge strane, u nekim državama je moguće govoriti o kritičnoj infrastrukturi na lokalnom, regionalnom (ekonomskom ili kulturnom regionu), državnom (nacionalnom) i međunarodnom nivou.

U zavisnosti od vremena potrebnog za zaštitom, KI može biti: stalna, privremena ili potencijalna. Stalna KI je ključna infrastruktura za neke države, propisana zakonom, a koja mora biti sve vrijeme u fokusu interesovanja. U kategoriju privremene KI moguće je uvrstiti neke političke, sportske ili kulturne događaje kratkog vremena trajanja, ali koji su veoma važni za državu ili na međunarodnom nivou. Za ove infrastrukture je poznato da će biti važne u neko vrijeme godine ili tokom nekih događaja. Potencijalna KI je infrastruktura koja nije u fokusu, ali u nekim situacijama može biti veoma važna. Za tu infrastrukturu je poznato da može postati KI u nekim prilikama, ali ove situacije se ne planiraju unaprijed.

Prema nekim autorima, KI u odnosu na vlasništvo unutar jedne države, može biti u posijedu: države, opštine, privatnog lica, lica za upravljanje imovinomu državnom vlasništvu, u vlasništvu pravnih lica čiji su osnivači lokalne samouprave. S druge strane, to znači da može biti KI u javnim, privatnim ili javno-privatnim rukama. Javno-privatno partnerstvo je od suštinskog značaja, jer se procjenjuje da je preko 85% od onoga što se može klasifikovati kao KI u SAD-u privatnom vlasništvu, a u Nemačkoj privatni sektor upravlja sa preko 90% KI.

Dakle, to znači da su tipovi KI veoma različiti i zavise od različitih gledišta onih koji odlučuju šta je KI, kao i od strukture i nivoa vlasti. Ali u oblasti zaštite KI postoji potreba za sveobuhvatnijim pristupom. To znači da svi nivoi vlasti u državi moraju da prepoznaju svoju KI i preduzmu mjere da ih zaštite. Ako samo jedan od nivoa nije uspeo da prepozna i zaštiti svoju KI, to bi moglo dovesti do katastrofe, jer je infrastruktura međusobno povezana i zavisna jedna od druge.[214]

Iako se rad ne bavi konkretnim mjerama integrisane zaštite kritične infrastrukture, niti zalazi u dubine preporuka datih Direktivom EU za zaštitu kritične infrastrukture 2008/114

---

[214] Čemerin, D., Trut, D., Kriteriji za određivanje hrvatske kritične infrastrukture, Zbornik radova "Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb, str. 33, 2010.

EC, radi šitreg sagledavanja ove problematike od strane čitalaca i akadeske zajednice, navest ćemo nekoliko njenih najznačajnijih elemenata. Naime, ovom Direktivom se uspostavlja postupak za utvrđivanje i označivanje evropske kritične infrastructure (EKI-ja) te utvrđuje pristup za poboljšanje njezine zaštite. Direktiva je primjenjiva na zemlje članice, zemlje kandidate i zemlje potencijalne kandidate za članstvo u EU. Ključne tačke Direktive su utvrđivanje i označivanje EKI-ja, na način da se definiše postupak utvrđivanja potencijalnih EKI-ja (uz pomoć Evropske Komisije ako je to potrebno). Pri utvrđivanju potencijalnih EKI-ja trebale bi primjenjivati: međusektorska mjerila kao što su moguće žrtve, gospodarske posljedice i utjecaj na javnost; i sektorska mjerila specifična za vrstu EKI-ja. Potrebno je ostvariti saradnički proces sa zemljama susjedstva, u svrhu označavanja EKI (npr. rasprave i razmjene mišljenja i iskustava s zemljama susjedstva i članicama EU) za potencijalne EKI-je koji se nalaze na njihovu državnom području. Potrebno je redovno preispitivanje utvrđivanja i označavanja EKI-ja. Direktiva je prvobitno definisala primjenu samo na ključne sektore infrastrukture: energiju i prijevoz, ali se s vremenom njezino područje primjene proširilo in a druge sektore (hrana, zdravstvo, školstvo, finanasije itd.).

Sigurnosnim planovima operatera (SPO), osigurava se da za svaki EKI postoji jasno sigurnosno planiranje. Svrha postupka SPO-a jest utvrđivanje kritične imovine EKI-ja, kao i postojećih sigurnosnih rješenja za njihovu zaštitu. Oficiri za vezu su zaduženi za sigurnost a nacionalni autoriteti osiguravaju da njihovo imenovanje u skladu sa pravilima i međunerodnim standardima. Oficir za vezu služi kao tačka za kontakt između vlasnika/operatera EKI-ja i odgovarajućeg tijela zemlje EU-a. Osigurava se pravovremeno izvještavanje, te ocjenjivanje prijetnje u odnosu na EKI-je u roku od jedne godine nakon što je označena kritična infrastruktura. Svake dvije godine Komisiji se dostavljaju izvještaji s općim podacima o vrstama rizika, prijetnjama i slabostima. Direktiva se primjenjuje od 12. januara 2009., a sve zemlje ćlanice, kandidati za članstvo i potencijalni kandidati bi je trebale uključiti u svoje nacionalno pravo.

Pet godina poslije, 2013. godine, Evropska Komisija je donijela radni dokument o novom pristupu Europskom programu za zaštitu kritične infrastrukture, European Programme for Critical Infrastructure Protection (EPCIP). Njime se definiše potreba za interoperabilnošću i međusektorskom saradnjom jer je narušavanje kritične infrastructure uzročnoposljedično povezano, npr. prekid napajanja električnom energijom, narušava telekomunikacionu, saobraćajnu i privrednu infrastrukturu. EPCIP, također definiše i uspostavu Mreže za rano upozoravanje na kritičnoj infrastrukturi, Critical Infrastructure Warning Information Network (CIWIN), čiji je zadatak da osigura sistem za razmjenu i raspravu o informacijama, studijama, dobrim praksama vezanim za KI, te razmjenu informacija i komunikacija putem digitalnog prijenosa podataka među organizacijama KI. Ova mreža ima za cilj analizirati i prikazati odabrane slučajeve paneuropskih kritičnih infrastruktura, te primati korisne i zaštićene povratne informacije od korisnika CIWIN-a. Također, mrežom se daje mogućnost pristupa savremenim IT alatima, koji uključuju i metodologije procjene rizika sa gotovim predlošcima. Mreža predstavlja digitalnu platformu domaćina za nekoliko nacionalnih CIP područja u državama članicama i može sadržavati sve relevantne informacije o saradnji sa trećim zemljama, kao što su SAD, Kanada, zemlje EFTA-e i

kandidati za članstvo. Upravo ovakav vid umrežavanja, te prikupljanja i obrade ogromnog broja informacija, predstavlja izazov za sagledavanje sigurnosne i šireg bezbjednosne problematike zaštite i upravljanja podacima. Savremene tehnike presretanja ("cyber napadi" i sl.), zahtijevaju i savremene alate za odbranu od te vrste rizika.

Međunarodni standard za informacijsku sigurnost i zaštitu podataka ISO 27000, daje smjernice za primjenu ovih normi, kojima se osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, te se povećava pouzdanosti sistema u slučaju katastrofe, što pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja svih aktera sistema vezanih uz informacijsku sigurnost[215]. Sastoji se od četiri osnovna poglavlja: sistemi za upravljanje informacijskom sigurnošću (engl. ISMS – Information Security Management System); odgovornost uprave (engl. Management Responsibility); ispitivanje sistema upravljanja (engl. Management Review); poboljšanje suistema za upravljanje informacijskom sigurnošću (engl. ISMS Improvement).

U pogledu upravljanja ova četiri poglavlja mogu se sažeti u dva bloka i to: sistem za upravljanje sigurnošću koji obuhvata: dokumentiranje, pregled, ispitivanje, odgovornost uprava, korektivne i preventivne mjere te stalno poboljšanje sistema i upravljanje informacijskom sigurnošću koji je ciklus uspostave, implementacije, rukovanja, pregledavanja, ispitivanja i poboljšanja sistema za upravljanje informacijskom sigurnošću (ISMS), a koji je opisan modelom PDCA (engl. Plan-Do-Check-Act). Faze PDCA ciklusa su: PLAN: Uspostava sistema za upravljanje informacijskom sigurnošću; DO: Upravljanje sistemom informacijske sigurnosti; CHECK: Nadzor i ispitivanje sistema informacijske sigurnosti; ACT: Poboljšanje sistema informacijske sigurnosti;

General Data Protection Regulative (GDPR) je opšta Uredba EU 2016/679 EC, o zaštiti ličnih podataka. Uredba se bavi harmonizacijom zaštite ličnih podataka na nivou EU, te definiše veći stepen kontrole za lica čiji se podaci obrađuju i unapređuje upravljanje savremenim rizicima iz ove oblasti. Kritična infrastruktura spada među najveće rukovaoce podataka o ličnosti i u postupku usklađivanja sa obavezama utvrđenih Uredbom treba da izvrši punu analizu svog postojećeg regulatornog i infrastrukturnog okvira zaštite ličnih podataka. Također, primjenom Uredbe pruža se prilika za ispravke eventualnih ranijih nedostatka u postojećim procesima, te se od organizacija očekuje podizanje opšte svijesti o standardima zaštite ličnih podataka, a posebno imajući u vidu zaprijećene stroge sankcije za slučaj neusklađenosti.

Uredbom se definišu sljedeće oblasti: područje primjene, ujednačeni propisi i jedinstveni mehanizam, odgovornost i transparentnost, pravne osnove za obradu, privola, službenik za zaštitu osobnih podataka, pseudonimizacija, povrede podataka, sankcije, pravo

---

[215] Stručni rad: Norme informacijske sigurnosti ISO/IEC 27K, Javor Bogati, Ministarstvo obrane Republike Hrvatske,

pristupa, pravo na zaborav, prenosivost podataka, integrirana zaštita podataka i evidencija o aktivnostima obrade.

Sa aspekta vanjske i unutrašnje zaštite podataka, najvažnija poglavlja su definisanje rada službenika za zaštitu ličnih podataka i integrirana zaštita podataka, kojima se daju precizne smjernice za izradu procedura i primjenu određenih mjera zaštite tajnosti podataka.

Ako se osnovne djelatnosti voditelja obrade sastoje od postupaka obrade, koji zbog svoje prirode, obima ili svrhe, iziskuju redovno i sistemsko praćenje ispitanika u velikoj mjeri, odnosno ako aktivnosti obrade uključuju opsežnu obradu posebnih kategorija podataka, potrebno je imenovati stručnu osobu sa znanjima u području zaštite podataka koja će pomoći voditelju ili izvršitelju obrade, te nadzirati usklađenost s mjerama iz GDPR-a. Od službenika za zaštitu podataka očekuje se stručnost u upravljanju IT procesima, sigurnosti podataka (uključujući odgovor na "cybernapade") i ostalim kritičnim pitanjima koja se tiču pohrane i obrade ličnih i osjetljivih podataka. Potrebni nivo znanja širi je od samog razumijevanja zakonskih propisa. Više podataka o pojedinostima i funkciji službenika za zaštitu podataka dati su u dokumentu "Smjernice o službenicima za zaštitu podataka," izdanom od strane Radne skupine za zaštitu podataka.

Mjere tehničke i integrirane zaštite podataka propisuju primjenu zaštitnih mjera u sam postupak razvoja procedura, proizvoda i usluga. Treba od početka primijeniti visoki nivo mjera za zaštitu privatnosti, a voditelj obrade mora osigurati da tehničke i prodecuralne mjere budu adekvaatne i u skladu s propisima za vrijeme cjelokupnog trajanja postupaka obrade. Voditelji obrade trebaju primijeniti mehanizme kojima bi se spriječila obrada osobnih podataka, osim ako je to potrebno za svaku od određenih svrha.

Izvještaj Agencije Evropske unije za mrežnu i informacijsku sigurnost[216] objašnjava što je potrebno da se usvoje metode integrirane i tehničke zaštite podataka. U izvještaju se navodi kako se aktivnosti enkriptiranja i dekriptiranja moraju odvijati lokalno, a ne na udaljenom poslužitelju, jer ključevi moraju biti u posjedu voditelja obrade ako je cilj zaštita privatnosti podataka. Također se navodi da je korištenje usluga za pohranu podataka, poput onih u oblaku, praktično i relativno sigurno u slučaju da samo vlasnik podataka, ali ne i pružatelj usluge u oblaku, ima pristup ključevima za dekriptiranje.

Zaštita podataka unutar sistema kritične infrastrukture je poseban izazov za stručnjake i nacionalne autoritete, ako se uzme u obzir njena osjetljivost i ranjivost na terorizam, kao jednu od najvećih prijetnji današnjice. Dosadašnji teroristički napadi na saobraćajnu infrastrukturu (metroi u Londonu, Madridu i Tokiju), su uglavnom bili usmjereni na ciljane posljedice po živote i zdravlje običnih građana, sa ciljem izazivanja panike i masovne

[216] *ENISA - https://europa.eu/european-union/about-eu/agencies/enisa_hr (pristup 18.07.19.)*

histerije i straha. Međutim, učestali "cyber" napadi na privatnost pojedinaca i organizacija, posebno onih finansijskih, te nedavni napad na elektroenergetsku infrastrukturu Venecuele u danima pokušaja "vojnog puča" otvaraju i pitanje zaštite sistema kolektovanja i upotrebe podataka, od mogućih terorističkih napada ovakve vrste. Posljedice po nezaštićenu KI, možda neće biti iskazane trenutnim brojem žrtava kao u ranijim terorističkim napadima ali će sigurno biti dugoročnije i direktno i indirektno štetnije po društveno politički poredak napadnute zemlje. Tako npr. u najgorem scenariju višednevnog prekida elektroenergetske KI, mora se uzeti u obzir i međusektorska ovisnost te posljedice koje će dugoročno a neke i trajno povećati ukupnu ranjivost zajednice. Iz tog razloga, zadatak svih vlasnika i operatere na KI, jeste da svakodnevno tragaju i čine maksimalne napore za uspostavu integriranog sistema zaštite KI, sa posebnim osvrtom na zaštitu i upravljanje osjetljivim podacima primjenom inovativnih tehnologija.

3. UPRAVLJANJE PODACIMA POMOĆU SOFTVERSKIH ALATA "GIS" I "BIM"

Pod pojmom zaštite podataka podrazumijevamo uspostavljanje sistema kolektovanja, operacionalizacije i upotrebe podataka. Kolektovanje podataka se vrši putem identifikacijskih formi, koje trebaju biti usklađene sa EUROSTAT kasifikacijom i kategorizacijom kako podataka o samim rizicima, tako i podataka o uticajiima tih rizika na ljude, imovinu i životnu sredinu, te podataka o kapacitetima integrisanih službi i mjera zaštite na KI. Pri kolektovanju podataka treba slijediti smjernice proizašle iz direktive EU za zaštitu KI. Operacionalizacija podataka dobijenih pravilnim identificiranjem i kolektovanjem, predstavlja centralni dio sistema u kome se nalaze oni najosjetljiviji podaci za nesmetan rad KI, odnosno podaci koji se svakodnevno analiziraju i odnose na, kako vanjske tako i unutrašnje, ranjivosti sistema KI. Vanjski faktori ranjivosti KI su potencijalni terorizam, te „cyber napadi" u svrhu ucjene i iznude, odnosno u cilju sticanje prednosti za konkurenciju. Unutrašnji faktori rizika predstavljaju potencijalno nezadovoljstvo samih uposlenih unutar sistema KI ili njihov nemar i neodgovorno ponašanje koji mogu dovesti do ozbiljnog narušavanja sigurnosnog sistema. Da bi se uspostavila efikasna operacionalizacija podataka i njihova adekvatna zaštita od vanjskih i unutrašnjih prijetnji, potrebno je primjeniti smjernice date međunarodnim standardom ISO 27000. Upotreba podataka predstavlja izuzetno osjetljivu fazu iz razloga što se njome mora garantovati ne samo adekvatna zaštita osjetljivih podataka o samom sistemu, već i zaštita privatnih podataka uposlenih i posjetilaca po raznim osnovama, kojima se mora garantovati potpuna privatnost i zaštita ličnih podataka od zloupotreba, u skladu sa regulativom GDPR.

Zaštita podataka dobijenih u procesu integrisane zaštite KI, predstavlja veoma važan preventivno-operativni segment koji se izvodi u tri faze: pripremnoj, operativnoj i arhivnoj. Ovaj proces počinje planiranjem sistema zaštite podataka, izradom procjene i plana IT zaštite shodno smjernicama i međunarodnim standardima. Od izuzetne je važnosti pravilno odabrati adekvatne alate za prikupljanje, obradu i arhiviranje podataka, koji svojim akreditovanim i licenciranim softverima garantuju maksimalnu zaštitu osjetljivih i ličnih podataka. Ovim radom ćemo se detaljnije osvrnuti na „GIS i BIM", kao dva najpoznatija alata za identifikaciju, analizu, vrednovanje, kontrolu i upravljanje prostornim podacima.

Odabir ovih alata za analizu je došao sa dugogodišnjim ličnim empirijskim saznanjima i istraživanjima problematike zaštite osjetljivih podataka na kritičnoj infrastrukturi.

Geografski informacionii sistem (GIS) predstavlja osnovni alat za mapiranje rizika, na globalnom svjetskom nivou. Nastao je 1960-tih, za potrebe višeslojnog upravljanja prostornim podacima i njihovim pridruženim osobinama. Kao inovacioni odgovor na izazov zaštite i funkcionalnog upravljanja velikim količinama podataka o rizicima, uticajima i kapacitetima snaga, uporedo sa fazom kvantitativnih i kvalitativnih vrednovanja podataka, potrebno je pristupiti i mapiranju georeferentnih podataka. Pomoću njih generišemo nivo transparentnosti informacije o ranom upozorenju na rizike, te omogućavamo funkcionalan pregled angažovanosti svih zainteresovanih učesnika u sistemu zaštite i spašavanja. Integracija akcija procjenjivanja i mapiranja rizika, doprinosi donošenju preciznijih, odlučnijih i efikasnijih odluka o prioritetnosti postupanja, te se pristupa najtežim rizicima sa najvišim odgovarajućim mjerama prevencije i pripravnosti.

U generalnom smislu GIS predstavlja računalni sistem sposoban za integrisanje, spremanje, uređivanje, analiziranje i prikazivanje geografskih informacija. U specifičnom smislu, GIS predstavlja "pametne karte", koje svojim korisnicima dopuštaju stvaranje interaktivnih upitnika (istraživanja koja stvara korisnik), analiziranje prostornih informacija i uređivanje podataka, preciziranih u prostoru. Najpoznatiji globalni proizvođač alata GIS-a je ArcGis, čija platforma ESRI predstavlja i zvaničnu platformu UN-a za mapiranje i upravljanje rizicima od katastrofa. Pored ArcGis-a, tu su još i proizvođači alata: ArcMap, MapInfo, CARIS i dr.[217]

Današnje GIS vektorske baze, većinom u svom kodu imaju napredni enkripcijski standard, Advanced Encryption Standard (AES), vodeni žig („water mark“), hologramsku i biometrijsku zaštitu svojim pristupima. Zaštita vektorskih mape podrazumijeva šifriranje podataka vektorskih mapa, kontrolu pristupa korisnika i identificiranje operatera, odnosno vlasnika, u cilju sprječavanja šteta, napada ili ilegalnih distribucija, koje se mogu dogoditi u proces integracije niza geografskih informacija. Istraživači su dali rješenja zaštite putem „vodenog žiga“ za zaštitu autorskih prava i metode napredne enkripcije (šifriranja), usmjerenih na različite domene, vodeći računa o međunerodnom upravno-pravnom nasljeđu, Uredbi GDPR i standardu ISO 27000.

Važan segment pripreme za digitalizaciju mapa predstavlja upotreba bespilotnih letilica (dronova), koji za kratko vrijeme mogu precizno snimiti ortofoto snimke velikih prostornih površina, što je od izuzetnog značaja za starteške kritične infrastrukture, saobraćaj i energetiku. Uz pomoć specijalističkih snimka iz vazduha, mogu se relativno za kratko vrijeme, izraditi i 3D modeli prostora i nepristupačnih terena, a posebno objekata kritične infrastrukture na njima (npr. saobrćajnice, energetski objekati, elektroprenosne mreže,

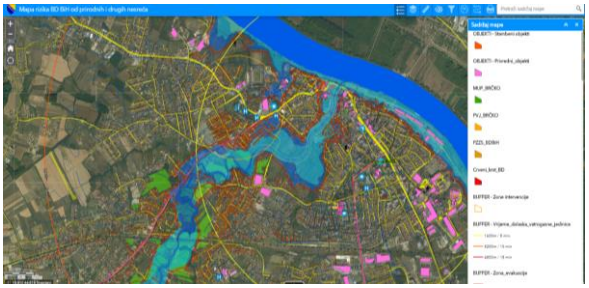
---

[217] "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018“

javne i ustanove od značaja i sl.). Zahvaljujući snimanjima dronovim iz vazduha i GIS bazama, znatno se smanjuje upotreba resursa, te se ubrzava čitav proces digitalizacije i mapiranja. Pored upotrebe u posebnim državnim, industrijskim, sigurnosnim i vojnim svrhama, tehnologija geografskog informacijskog sistema se može koristiti i za naučna istraživanja, upravljanje resursima, planiranje razvoja, geodeziju itd. Za sve ove upotrebe, zajednička je problematika zaštita ogromnih količina osjetljivih podataka. Ovi podaci pored osjetljive operativno-tehnološke vrijednosti imaju i veliku količinu ličnih informacija, koje se putem internetskih mreža mogu zloupotrebiti. GIS, pored svoje enkripcijske zaštite podataka, također omogućava planerima da u slučaju vanjskih ili unutrašnjih ugroza i „Cyber napada", definišu prostor uticaja, vrijeme potrebno za adekvatan odgovor i potrebne kapacitete u akcijama zaštite i spašavanja. Dakle, prednosti GIS-a su u mogućnosti mapiranja putem višeslojnih „layera" (podloga), odnosno unosa više vrsta mapa ili grupa prostornih podataka, te sigurne identifikacije, operativne obrade i arhiviranja ogromnih količina georeferenciranih podataka, dokumenata, slika i drugih vidova audio i video resursa. Svi pohranjeni podaci, se lako svrstavaju i pronalaze pomoću filtera, te je sa njima moguće efikasno upravljati sa ograničenim ljudskim resursima, što također bitno utiče na unutrašnje faktore rizika u pogledu zaštite podataka.

Evropskim smjernicama za procjenjivanje rizika od katastrofa izazavanih klimatskiim promjenama ili ljudskim nemarom ili namjerom, preporučuju se sledeće mape:

1. Mape koje prikazuju očekivani prostorni raspored glavnih opasnosti. Različite opasnosti i intenziteti treba da budu predstavljeni u odvojenim „layerima".
2. Mape uticaja koje pokazuju prostornu distribuciju svih relevantnih elemenata koji treba da budu zaštićeni - kao što su populacija, infrastruktura, prirodno zaštićena područja i sl.
3. Mape kapaciteta, koje daju skupine podataka o brojnosti i materijalnim resursima snaga za suprotstavljanje izazovima i posljedicama od katastrofa.



Ilustracija 1: Interaktivna mapa Brčko distrikta BiH (www.inzagroup.eu[218])

[218] https://inzagis17.maps.arcgis.com/apps/webappviewer/index.html?id=c161bac5370542a5aba10f25bd5c2de9

Ako uzmemo u obzir da GIS predstavlja alat za mapiranje velikih prosotra, npr. lokalnih zajednica, terena i infrastrukture, dajući im njihov vanjski oblik, onda BIM (Building Information Modeling), predstavlja inteligentni softverski alat za modeliranje informacija unutar objekata, dajući im njihov još precizniji i vanjski ali i unutrašnji oblik. Ovaj alat, koji je nastao kao odgovor na sve veću urbanizaciju i globalizaciju je uspostavljen na bazi 3D modeliranja, te stručnjacima arhitekture, inženjerstva i graditeljstva (AEC) pruža uvid i alate za efikasnije planiranje, projektovanje, izgradnju i upravljanje građevinama i infrastrukturom u visoko i nisko gradnji.[219] Obzirom da je ovaj alat nastao na Autodesk projektantskoj platformi, u sebi je integrisao nekoliko značajnih funkcija, pridodatih osnovnoj funkciji projektovanja. To su prije svih 3D modeliranje, odnosno izrada trodimenzionalnog modela (sa visinama, dužinama i širinama), koji vizuelno daje mnogo bolji uvid u projektantskom smislu u odnosu na dvodimenzionalni način projektovanja putem arhitektonsko-građevinskih tlocrta. Kada se 3D modelu pridodaju i funkcije menadžmenta, odnosno upravljanja projektom u svim fazama njegove realizacije: planiranju, projektovanju, izvođenju i održavanju, onda postaje jasno zašto je ovaj alat za veoma kratak period postao pravo osvježenje u građevinarstvu[220].

Uzimajući u obzir da je BIM precizniji i složeniji alat za kolektovanje velikog broja osjetljivih informacija u odnosu na GIS, koje pored prostornih, sadrže i tehničko-ekonomske povjerljive podatke, proces zaštite njegovih podataka je samim tim složeniji izazovniji. U BIM-u se pored napredne enkripcijske zaštite podataka i "vodenog žiga" za zaštitu autorskih prava, moraju primjeniti i odredbe međunarodnog upravno-pravnog naslijeđa za zaštitu podataka.

Stari pristupi upravljanja procesima izgradnje, a posebno održavanja već izgrađenih objekata infrastrukture, nisu više u mogućnosti da budu korak s brzom urbanizacijom i rastom populacije. Evidentan je pritisak i na postojeću infrastrukturu jer njeni sistemi i dalje rastu, grade se novi a stari imaju potrebu za kvalitetnim održavanjem i prepoznavanjem rizika u njihovoj ranoj fazi, kako bi se s njima moglo upravljati prije nego izazovu neku havariju ili štetu na objektima. Urbanizacija, zagušenje, okolišni propisi i ekonomska ekspanzija, potiču potražnju za kvalitetnom gradnjom i održavanjem infrastrukture. McKinsey Global Institut[221] procjenjuje da se gotovo 49 trilijuna dolara vrijednost ulaganja u infrastrukturu treba potrošiti od 2016. do 2030. Osim toga, da bi zadržao korak s projiciranim rastom, svijet mora ulagati još 3,3 bilijuna dolara godišnje do 2030., a trenutno ulaže oko 2,5 trilijuna dolara. U ovoj pozadini, tržište planiranja, projektovanja, izgradnje i održavanja infrastrukture doživljava temeljne promjene. Primjena BIM-a obuhvata veoma širok spektar informacijskih mogućnosti, od upravljanja rizicima u fazama planiranja, projektovanja i gradnje pa sve do simuliranja otpornosti konstrukcije u

---

[219] *Autodesk Handbook, „Strategic industry foresight – The digitalization of Infrastructure"*
[220] "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018"
[221] https://www.mckinsey.com/, (datum pregleda 11.04.2018.)

požarima, zemljotresima, orkanskim vjetrovima, i drugim fizičkim narušavanjima stabilnosti građevine. Posebna prednost BIIM-a na drugim tehnologijama je ta što se podaci kreiraju 3D okruženju, pri čemu se dodaju podaci o dinamici u 4D modelu, tehničkim i finansijski podaci u 5D, podaci neophodni za efikasno održavanje u 6D i sigurnosni podaci u 7D modelu objekta.

Identifikacijske forme, korištene za kolektovanje i klasificiranje podataka, koje sadržavatju lične i osjetljive podatke, trebaju uvrstiti pravne osnove za obradu, te pristanak i pseudonominizacija izvora podataka, tamo gdje zloupotreba podataka može izazvati štetu po organizaciju i pojedinca.

Ilustracija 2: Autodesk Revit BIM Software, u kome se kolektuju svi podaci o građevini ali mogu biti kolektovani i lični podaci izvođača i nadzora.

4. ZAKLJUČAK

Izazov zaštite prikupljanja i kolektovanja podataka putem inovativnih alata poput GIS-a i BIM-a koji predstavljaju budućnost u planiranju, gradnji i održavanju infrastrukturnih objekata u okviru lokalnih i nacionalnih prostornih planova, zahtijeva ozbiljan sistemski pristup. Zahtjevi u pogledu zaštite koje je definisala međunaordna zajednica putem svojih uredbi, direktiva i standarda, predstavljaju upravno-pravni okvir u kojem sve države članice, kandidati i potencijalni kandidati za članstvo, trebaju definisati svoje nacionalne strategije i svoju upravno-pravnu regulativu. Globalni izazovi i šarolikost lepeze prijetnji,

među kojima posebno treba istaknuti terorizam kao "modernu pošast" današnjeg vremena, predstavljaju jasne zahtjeve za vlasnike i operatore kritičnih infratsruktura, bilo da su one u javnom ili privatnom vlasništvu, u pogledu potreba za integrisanom zaštitom, koja obavezno mora uključivati planove za zaštitu osjetljivih i ličnih podataka od zloupotreba i napada. Masovnost i složenost gradnje objekata i mreža kritične infrastrukture, kreira veoma složene zadatke stručnjacima koji se bave bezbjednosno/sigurnosnim izazovima, te koji su uvažavajući specifičnosti i težinu ove problematike, usvojili dva osnovna alata GIS i BIM, kao značajnu pomoć pri identifikaciji, kolektovanju, analizi, vrednovanju i arhiviranju prostronih podataka. Ako za GIS možemo reći da predstavljajući prostorno sveobuhvatniji i primjenjiviji alat za identifikaciju, kolektovanje i analizu podataka na makro lokacijama izvan mreža kritične infrastrukture, onda za BIM možemo zaključiti da predstavlja još precizniji i obuhvatniji alat za upravljanje podacima na mikro lokacijama i unutar samih građevinskih cjelina i pojedinačnih termo-energetskih sistema privremeno ili trajno ugrađenih u objekte. Oba ova alata imaju svoju primjenu u procesu upravljanja rizicima, zbog svojih karakteristika funkcionalnog i bezbjednosno/sigurnosnog upravljanja bazama velike količine različitih podataka. Mogućnost 3D, 4D, 5D, 6D i 7D modeliranja sa ovim alatima, omogućava nam potpunu vizualizaciju i upravljanje integrisanim procesom upravljanja i zaštite prikupljenih podataka. GIS i BIM, kao globalne platforme nadopunjuju jedna drugu, te otvaraju mogućnosti funkcionalne upotrebe, dajući efikasniji model upravljanja čitavim procesom upravljanaj i zaštite osjetljivih i ličnih podataka. Dakle, zahvaljujući razvoju GIS i BIM inovativne tehnologije, pored toga što značajno ubrzavamo i čitav proces planiranja, projektovanja, gradnje i održavanja, te smanjujemo troškove i radnu snagu, upravljamo i svim fazama rizika, uključujući i izazove i prijetnje po sigurnost informacija, osjetljivih i ličnih podataka. Da bi ovakav sistem postao u potpunosti efikasan i operativan, potrebno je kreirati čvrstu zakonsku regulative i tehničke smjernice, uvažavajući upravno-pravno naslijeđe EU, te tehnički i kadrovski izgraditi i ojačati postojeće kapacitete. Kritična infrastruktura je sama po svojoj namjeni i svrsi značajna "žila kucavica" svakog modernog društveno-političkog uređenja, te je potrebno sistemski graditi i kapacitet za njenu adekvatnu zaštitu. Ovdje prije svega mislimo na edukacijsko jačanje kadrovskog potencijala službenika IT zaštite, u okviru integrisanih službi zaštite i spašavanja, koje kroz programe različitih specijalističkih edukacija, primjenu IT alata i kontinuirane treninge, možemo osposobiti i dodatno ojačati za izazove i adekvatne odgovore u procesu integrisane zaštite evropske, regionalne i nacionalne kritične infrastrukture.

5. LITERATURA

Publikacije

1. Protecting Energy Critical Infrastructure a Key Challenge for DHS**,** February 16. 2019**.,** Chuck Brooks
2. Energetska sigurnost i zaštita kritične infrastrukture: utjecaj na politike nacionalne sigurnosti, Talović Siniša
3. National critical infrastructure protection - regional perspective / Zoran Keković, Denis Ćaleta, Želimir Kešetović, Zoran Jeftić - Beograd : University of Belgrade - Faculty of Security Studies, 2013.
4. Čemerin, D., Trut, D., Kriteriji za određivanje hrvatske kritične infrastrukture, Zbornik radova "Hrvatska platforma za smanjenje rizika od katastrofa", Državna uprava za zaštitu i spašavanje, Zagreb, str. 33, 2010.
5. Stručni rad: Norme informacijske sigurnosti ISO/IEC 27K, Javor Bogati, Ministarstvo obrane Republike Hrvatske
6. "Inovacioni pristup za upravljanje rizicima korištenjem programskih alata GIS i BIM" Garaplija, E., Strugar, V., Međunarodna konferencija „CIBEK 2018“

Internet

1. Direktiva za zaštitu kritične infrastrukture 2008/114 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008L0114&from=EN
2. Regulativa za upravljanje podacima 2016/679 EC, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (18.07.19.)
3. ISO standardi za zaštitu podatakahttp://www.27000.org/
4. US Department of Homeland Security Seal - https://www.dhs.gov/cisa/critical-infrastructure-sectors (31.05.19)
5. Izvještaj za period 2002/2012 osiguravajuće kuće Munich RE
6. “Cyber napadi” na medijskoj mreži Al Jazeera, http://balkans.aljazeera.net/tema/cyber-napadi (18.07.19.)
7. ENISA - https://europa.eu/european-union/about-eu/agencies/enisa_hr (pristup 18.07.19.)
8. https://inzagis17.maps.arcgis.com/apps/webappviewer/index.html?id=c161bac5370542a5aba10f25bd5c2de9 (19.07.19.)
9. Autodesk Handbook, „Strategic industry foresight – The digitalization of Infrastructure“