H. Hamidović*

ZAŠTITA OD POŽARA IKT CENTARA

UDK 004.3:614.841
PRIMLJENO: 5.1.2015.
PRIHVAĆENO: 4.1.2016.

SAŽETAK: Organizacije u kojima se upotrebljavaju računala i mreže za podršku vitalnim poslovnim procesima trebaju osigurati odgovarajuće radno okruženje za njih. Ne učine li to, mogu dovesti do povećanja troškova poslovanja uzrokovanog čestim zastojima. Od vremena njihovog nastanka, IKT centri suočeni su s univerzalnom prijetnjom - požarima. Opsežna uporaba sustava za zaštitu od požara u IKT centrima ne proizlazi iz visoke vjerojatnosti pojave požara, niti od značajne opasnosti za život ljudi, već prije svega zbog mogućih poslovnih šteta uzrokovanih požarom. Stoga je nužno razmotriti potencijal i posljedice prekida u poslovanju neovisno o potencijalu za materijalnu štetu uzrokovanu požarom u IKT centrima. Ovaj rad predstavlja problematiku zaštite od požara IKT centara i zakonske obveze u Federaciji Bosne i Hercegovine.

Ključne riječi: *IKT centri, zaštita od požara, informacijska sigurnost, zakonske obveze*

UVOD

Tijekom godina, informacijsko-komunikacijske tehnologije (IKT) postale su sastavni dio mnogih aktivnosti koje su elementi kritične infrastrukture u svim organizacijskim sektorima, bilo javnim, privatnim ili dobrovoljnim. Širenje interneta i drugih elektroničkih mrežnih usluga, te današnje mogućnosti sustava i aplikacija, čine da organizacije postaju sve više ovisne o pouzdanim i sigurnim IKT infrastrukturama i uslugama. Poremećaj IKT-a može predstavljati strateški rizik za ugled organizacije i njezinu sposobnost za izvršavanje poslovnih operacija.

Elementarne nepogode, djela terorizma, tehnološke nesreće i ekološki incidenti jasno su pokazali da ni javni niti privatni sektor nisu imuni od kriza, bilo namjerno ili nenamjerno izazvanih. Posljedice incidenata se razlikuju i mogu biti dalekosežne. Ove posljedice mogu uključivati ljudske žrtve, gubitak imovine ili prihoda ili nemogućnost isporuke proizvoda i usluga o kojima može ovisiti strategija, ugled ili čak opstanak organizacije. Kako ovisnost o informacijsko-komunikacijskim tehnologijama nastavlja rasti, za očekivati je da će IKT objekti postati primarne mete za sabotaže i paljevine *(NFPA 75, 2013.)*.

Požari u IKT centrima i drugim kritičnim objekatima koji sadrže elektroničku opremu češći su nego bilo tko shvaća ili je spreman da ih prizna u kritičnu infrastrukturu industrije. Većina požara su malog intenziteta, riješeni od lokalnog osoblja, i ne prijavljuju se nadležnim tijelima. Među profesionalcima za zaštitu od požara smatra se da se samo oko 40 % požarnih incidenata prijavljuje, dok je preostalih 60 % požara neregistrirano *(Treyger, 2012.)*.

Ovaj rad predstavlja problematiku zaštite od požara IKT centara i zakonske obveze u Federaciji Bosne i Hercegovine.

*Dr. sc. Haris Hamidović (haris.hamidovic@eki.ba), MKF EKI Sarajevo, Džemala Bijedića bb (do 133), 71000 Sarajevo, Bosna i Hercegovina.

OPĆA OPASNOST

Požar predstavlja opću opasnost, a može se pojaviti u svim mjestima i prostorima u kojima ljudi žive i rade i u kojima se nalaze materijalna i druga dobra i imovina. Požar je opasnost koja je postojala u svim razdobljima ljudske povijesti i postojat će dok postoji ljudska civilizacija. Takva sudbina požara zasnovana je na činjenici što ne postoje sredstva i mjere koje mogu eliminirati mogućnost nastanka požara za sva vremena. To nije moguće iz razloga što postoje razni uzroci nastanka požara, kao što su djelovanje čovjeka, razne vrste tehnoloških procesa u gospodarstvu, proizvodnim i drugim djelatnostima, uporaba raznih izvora topline u svim društvenim subjektima i kućanstvima, kao i određene prirodne pojave, kao što su grom i slično.

Da bi se društvo moglo na organiziran i planski način učinkovito boriti protiv požara, bilo je nužno da se ovo područje pravno uredi. Pravno uređivanje je nužno iz razloga što se u borbi protiv požara moraju angažirati svi društveni faktori (i privatni i javni sektor), jer pojedinačna angažiranja ne mogu riješiti ovaj problem. Upravo ti razlozi nametnuli su potrebu da se ovo područje regulira zakonom, jer se samo zakonom za sve društvene faktore mogu utvrditi prava i obveze za sudjelovanje u borbi protiv požara i da se odredi način tog sudjelovanja. Zbog toga je na razini Federacije Bosne i Hercegovine donesen poseban propis za ovo područje, a to je Zakon o zaštiti od požara i vatrogastvu (u daljnjem tekstu: Zakon o požaru).

Zaštita od požara predstavlja preventivu, jer je njezina osnovna funkcija da sprečava nastanak požara. Da bi se mogao ostvariti taj cilj, Zakon o požaru utvrdio je dvije vrste mjera zaštite, i to: opće mjere i posebne mjere zaštite. Zadatak tih mjera sastoji se u tome da se one moraju provoditi unaprijed, tj. prije nastanka požara. To znači da se kod svake vrste imovine moraju provoditi propisane mjere zaštite za sprečavanje izbijanja požara na imovini za koju su predviđene preventivne mjere.

Zakon o požaru nije propisao sve vrste mjera zaštite od požara koje se mogu provoditi, već su utvrđene samo one mjere koje su važne za ukupan sustav zaštite od požara. To znači da je zakon ostavio dovoljno prostora da svaki subjekt zaštite od požara odredi i druge mjere zaštite od požara koje su prema procjeni subjekta zaštite potrebne za zaštitu njihovih građevina i drugih materijalnih dobara i imovine. Vlastite mjere zaštite od požara svaki subjekt određuje na osnovi svoje procjene ugroženosti od požara. Ta procjena mora pokazati koje sve mjere zaštite od požara treba provoditi da bi se zaštitila njihova imovina. Na taj način svaki subjekt zaštite od požara ima obvezu da primjenjuje mjere zaštite od požara regulirane zakonom, ali i vlastite mjere zaštite koje subjekt zaštite odredi na osnovi vrste izvora opasnosti za izbijanje požara u građevinama i drugim objektima pravnih osoba *(Lepušina, 2014.).*

UZROCI POŽARA U IKT CENTRIMA

Američka Savezna komisija za komunikacije (Federal Communications Commission - FCC) provela je istraživanje o uzrocima požara u telekomunikacijskoj industriji, te identificirala sljedećih sedam osnovnih uzroka požara u telekomunikacijskim objektima *(Federal Communications Commission Network Reliability Council, 1993.)*:

- požari inicirani unutar telekomunikacijske i periferne opreme
- požari koji uključuju elektroenergetsku opremu
- vendor/izvođač pokrenuti požari (npr. zavarivanje)
- telekomunikacijsko osoblje uzrokovalo požar (npr. pušenje)
- prirodni uzroci (npr. oluje)
- uzrok izvan telekomunikacijske građevine (npr. zapaljenje smeća)
- požari unutar građevinskog sustava (npr. dizala).

Prema istraživanju američke Nacionalne agencije za zaštitu od požara (National Fire Protection Association - NFPA), najviše požara unutar IKT centara uzrokovano je u elektronaponskom sustavu – u 46 % slučajeva. Drugi česti uzročnici požara u IKT centrima su elektronička

oprema (33 %) te rashladni i ventilacijski sustavi (15%); *(Hall, 2012.).*

Električna postrojenja (uređaji, vodiči, elementi električnog kruga i sl.) mogu prouzročiti požar na tri načina, i to zbog oslobađanja topline, iskrenja ili električnog luka. Pri svim transformacijama jedne vrste energije u drugu, za što služe električni uređaji, oslobađa se toplina kao gubitak energije koja predstavlja potencijalnu požarnu opasnost u okruženju zapaljivih tvari. Ako je električni vodič nedovljno dimenzioniran, može se pregrijavati prilikom protjecanja struje. Pregrijavanje vodiča može biti tako intezivno da pored uništenja električne izolacije, ako je to izolirani vodič, može izazvati i paljenje. Greške i kvarovi, kao naprimjer, kratki spojevi i zemljospojevi mogu, također, izazvati požare. Ovdje pored topline mogu nastati iskre i električni lukovi *(Nikolić, Petrović, 1979.).*

Bitno je napomenuti da se na temelju člana 34. Zakona o požaru za električne instalacije i uređaje utvrđuje obveza projektiranja, izrađivanja, postavljanja, uporabe i održavanja tako da opasnost od požara ili eksplozije bude svedena na najmanju moguću mjeru dosljednom i pravilnom primjenom odgovarajućih mjera propisanih zakonom, tehničkim normativima i standardima koji se odnose na ta pitanja, kao i uputama proizvođača. Pod odgovarajućim mjerama podrazumijevaju se mjere koje se direktno ili indirektno mogu dovesti u vezu sa zaštitom od požara i sprečavanjem izazivanja ili širenja požara ili eksplozija, a što je u funkciji zaštite ljudi i materijalnih dobara.

PODLOŽNOST ELEKTRONIČKE OPREME OŠTEĆENJU

Robin *(2010.)* identificira tri ključna uzročnika oštećenja elektroničke opreme kao posljedice požara:

1) Toplinsko oštećenje

- Oštećenje informacijsko-komunikacijske opreme može započeti pri duljoj izloženosti opreme okolišnoj temperaturi od 79,4 °C, s povećanjem stupnja oštećenja daljnjim povišenjem okolišne temperature i vremena izloženosti.
- Oštećenja na magnetskim trakama, fleksibilnim diskovima i sličnim medijima mogu započeti pri duljoj izloženosti temperaturi iznad 37,8 °C. Štete koje se pojave pri temeparturama između 37,8 °C i 48,9 °C općenito se mogu uspješno sanirati, dok se šanse za uspješno saniranje šteta ubrzano smanjuju s trajnijom izloženosti okolišnoj temperaturi iznad 48,9 °C.
- Oštećenja na diskovima mogu započeti s duljom izloženosti okolišnoj temperaturi iznad 65,6 °C, s porastom stupnja oštećenja s daljnjim povišenjem okolišne temperature.

2) Netermalno oštećenje uzrokovano produktima izgaranja

Uz oslobađanje topline u požaru se razvijaju i velike količine dima koji je najčešći uzrok stradavanja zatečenih osoba (u 80 % slučajeva) i oštećenja komunikacijske opreme (u 95 % slučajeva). Istraživanja i terenska iskustva pokazala su odnos između akumulacije cink klorida (produkta izgaranja) na elektroničkim komponentama i oštećenja telekomunikacijske opreme. Troškovi restauracije telekomunikacijske opreme uz nakupinu cink klorida iznad 600 µg/in2 prelaze cijenu same telekomunikacijske opreme, bez jamstva dugoročne pouzdanosti.

Najvažnija informacijsko-komunikacijska imovina koja treba biti sačuvana nakon požara su korporativni mediji (organizacijske baze podataka). Ozbiljno oštećenje diskovnih čitaj/piši glava i mehanizma pogona trake je vjerojatno ako se pokušava raditi s medijima koji nisu čisti. "Head-crash" uzrokovan česticama na površini diska neće oštetiti samo pogon, već dovesti i do gubitka podataka.

3) Netermalno oštećenje uzrokovano djelovanjem sredstva za gašenje požara

Agensi za gašenje požara ne bi trebali uzrokovati teška oštećenja informacijsko-komunikacijske opreme. Iskustva sudskih vještaka pokazuju da su i u Federaciji Bosne i Hercegovine evidentirani slučajevi kada je slučajno oslobađanje pojedinih agensa za gašenje požara uzrokovalo teško oštećenje informacijsko-komunika-

cijske opreme. U tri predmetna slučaja radilo se o agensima koji su smjernicom BS 6266:2011 eksplicitno označeni kao sredstva koja imaju potencijal za oštećenje osjetljive elektroničke opreme i kao takva nisu preporučena za uporabu u IKT centrima.

NFPA 76 smjernice navode da se agensi za gašenje požara kao što su oni koje sadrže suhe kemijske tvari ili korozivne vlažne agense ne bi trebali upotrebljavati u bilo kojem području koje sadrži vrijednu komunikacijsku opremu, kao i da se ugradnja automatskih sustava za gašenje požara preporučuje samo ako nije moguće postići visoku razinu gradnje, uporabe, održavanja i upravljanja telekomunikacijskim objektom u smislu odgovarajućih preporuka NFPA 76 norme.

PROCJENA UGROŽENOSTI OD POŽARA

Procjena ugroženosti od požara predstavlja posebnu djelatnost (misaono razmatranje) u kojem se analiziraju i procjenjuju četiri vrste pitanja, i to:

- prvo pitanje odnosi se na određivanje i analizu svih izvora opasnosti koji mogu dovesti do nastanka požara,
- drugo pitanje odnosi se na određivanje mjera zaštite od požara koje treba poduzimati zbog sprečavanja nastanka požara i njegovog širenja u odnosu na označene izvore opasnosti za nastanak požara (preventivna zaštita),
- treće pitanje odnosi se na određivanje mjera zaštite od požara koje treba poduzimati na gašenju požara i spašavanju ljudi i materijalnih dobara ugroženih požarom (operativna zaštita),
- četvrto pitanje odnosi se na mjere zaštite koje treba provoditi na sanaciju posljedica koje nastaju od požara.

Pravna osnova za izradu procjene ugroženosti od požara u Federaciji Bosne i Hercegovine jest Metodologija za izradu procjene ugroženosti od požara objavljena u Službenim novinama Federacije BiH.

Metodologija upućuje na primjenu u svijetu prihvaćenih numeričkih metoda, kao što su: TRVB 100, Euralarm, Gretener, DOW Index i slične. Numeričke metode služe za izračunavanje rizika od požara i požarne ugroženosti za pretpostavljene požare na području lokaliteta na kojem se nalaze građevine i prostori u kojima pravna osoba obavlja svoju djelatnost. Numerička analiza požarne ugroženosti treba pokazati stupanj ugroženosti određenog lokaliteta od požara kako bi se prema toj činjenici planirale i provodile odgovarajuće mjere zaštite od požara koje imaju preventivnu ulogu.

U nastavku se raščlanjuju temeljne značajke metode Euralarm – metodologijom preporučene brojčane metode za analizu požarne ugroženosti u poslovnim i pretežito poslovnim građevinama.

Temeljne značajke metode Euralarm

Metodom Euralarm utvrđuju se posebne mjere zaštite od požara koje treba provesti u analiziranim požarnim sektorima, a posebno se ukazuje na potrebu ugradnje stabilnog automatskog uređaja za gašenje požara.

Euralarm temelji se na dvjema pretpostavkama:

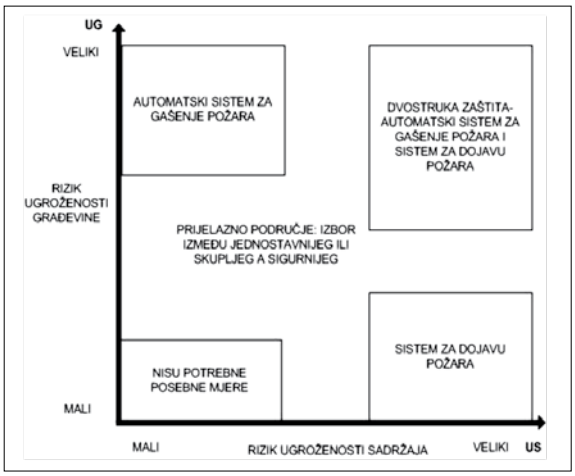
- da požar može ugroziti građevinu, te
- da požar može ugroziti sadržaj u građevini.

Koja od tih dviju pretpostavki dominira ili su, pak, moguće obje, ovisi i koje će se posebne mjere zaštite od požara provoditi. Kada se radi o ugroženosti građevine, tada valja raščlaniti dva glavna učinka koji su međusobno suprotni:

- intenzitet i moguće trajanje požara, te
- otpornost na vatru glavnih i nosivih konstrukcija objekta.

Kada se govori o ugroženosti sadržaja građevine, misli se na to da je u građevinu smještena skupa oprema, odnosno da požar može ugroziti ljude koji stalno ili povremeno borave u njoj. Zato se ukupna požarna ugroženost izračunava za dvije vrijednosti koje zajedno predstavljaju zajedničku ugroženost: za građevinu (ugroženost građevine - UG) i za sadržaj (ugroženost sadržaja - US). Na temelju izračuna ugroženosti određuju se posebne mjere zaštite od požara.

Kada su izračunate vrijednosti za UG i US, unose se kao ordinata, odnosno apscisa u dijagram protupožarnih mjera. Svakoj kombinaciji između UG i US odgovara jedna točka u određenom polju dijagrama, čiji pojednostavljeni prikaz je predstavljen na slici 1 *(Purt, 1972.).*



Slika 1. Dijagram protupožarnih mjera

Figure 1. Diagram showing fire protection measures

Raščlanjenost dijagrama protupožarnih mjera temelji se na iskustvenoj prosudbi u određivanju mjera za smanjenje požarne ugroženosti, a osim toga postupak je praktički provjeren na većem broju primjera.

Za procjenu glede provedbe posebnih protupožarnih mjera, požarna ugroženost sadržaja smatra se prilično nezavisnom od požarne ugroženosti građevine. Izračun požarne ugroženosti sadržaja jednostavniji je od izračuna požarne ugroženosti građevine i dobiva se uglavnom ako se odgovori na sljedeća pitanja:

- Kolika je kod nastanka požara neposredna opasnost za ljude koji se eventualno zadržavaju u građevini?
- Kolika je neposredna opasnost kod nastanka požara za imovinu koja je jako vrijedna, nenadoknadiva ili izričito osjetljiva na sredstva za gašenje?
- Koliko se za oboje još povećava opasnost zbog eventualnog zadimljenja?

Dobivena vrijednost ugroženosti sadržaja, na temelju Euralarm metode, značajno utječe na odluku o izboru automatskih sustava za dojavu požara, dok se izbor automatskih sustava za gašenje požara može smatrati funkcijom dominantno ovisnom o parametru ugroženosti građevine.

MJERE ZAŠTITE OD POŽARA IKT CENTARA

Prilikom donošenja odluke o izboru mjera protupožarne zaštite IKT centara, posebice ugradnje stabilnog automatskog uređaja za gašenje požara, potrebno je dodatno slijediti smjernice za procjenu rizika predstavljene normom BS 6266:2011 *Fire protection for electronic equipment installations,* uzevši u obzir da je odluka o izboru automatskog sustava za gašenje požara u ovim okruženjima funkcija vrijednosti opreme, ali i potencijala za prekid poslovanja koji se ne razmatra Euralarm metodom.

Kritičnost područja IKT centara kategorizira se na temelju norme BS 6266:2011 pomoću ovih elemenata:

- redundantnost opreme i dostupnost zamjene
- planovi kontinuiteta poslovanja
- razine tolerancije prekida u radu
- okolišni operativni zahtjevi specifični za pojedine sustave.

IKT centri mogu se generalno svrstati u 4 kategorije ugroženosti od požara: niska, umjerena, visoka i kritična. Njihove značajke su sljedeće:

a) Umjerena
   - Oprema je standardna i ne može se odmah zamijeniti.
   - Poslovne operacije mogu se prenijeti na drugu lokaciju.
   - Prekid poslovnih operacija može se tolerirati u srednjoročnom razdoblju.

b) Visoka
   - Oprema nije standardna i ne može se zamijeniti u kratkom razdoblju.
   - Poslovne operacije ne mogu se prenijeti na drugu lokaciju bez robusnog plana oporavka.
   - Prekid poslovnih operacija može se tolerirati kratko razdoblje.

c) Kritična
   - Oprema je vrlo skupa, namjenski izrađena i nije lako zamjenjiva.
   - Poslovne operacije ne mogu se lako prenijeti na drugu lokaciju.
   - Prekid poslovnih operacija će najvjerojatnije imati značajne negativne posljedice.

Ako brze akcije gašenja požara nisu vjerojatne, izbor automatskog sustava za gašenje požara je obvezan za IKT centre iz umjerene kategorije ugroženosti. Za IKT centre iz visoke kategorije ugroženosti automatski sustav za gašenje požara je obvezan ako ne postoji robustan plan oporavka od katastrofa, dok je za IKT centre iz kritične kategorije ugroženosti automatski sustav za gašenje požara uvijek obvezan.

Bitno je napomenuti da, za razliku od britanske norme BS 6266, američka NFPA 75 norma propisuje obveznu upotrebu sustava aktivne zaštite u IKT centrima na način da:

- IKT centri smješteni u objektima za koje se zahtijevaju sprinkler sustavi moraju biti opremljeni automatskim sprinkler sustavima.
- IKT centri koji se nalaze u objektima za koje se ne zahtijevaju sprinkler sustavi moraju biti opremljeni automatskim sprinkler sustavima ili sustavima sa clean agentom, ili sa oba.
- Tamo gdje postoji kritična potreba za zaštitu podataka u procesu, smanjenje oštećenja opreme i olakšavanje povratka servisa, treba razmotriti uporabu clean agent sustava u IKT centrima, bez obzira je li se unutar građevine zahtijevaju ili ne zahtijevaju sprinkler sustavi.

Automatski uređaji za detekciju požara moraju biti instalirani u IKT centrima u skladu sa obje navedene norme - BS 6266, NFPA 75. To je i opravdano s obzirom na terenska iskustva koja pokazuju da je direktna materijalna šteta uzrokovana požarima u IKT centrima u prosjeku bila niža za oko 60 % ako su na lokaciji bili instalirani uređaji za detekciju požara *(Hall, 2012.)*.

AUTOMATSKI SUSTAVI ZA GAŠENJE POŽARA

Razvoj stabilnih sustava za gašenje požara s automatskim djelovanjem u uskoj je vezi s općim tehnološkim razvojem u kojem su se znatno povećale opasnosti od požara, čije gašenje je često neizvedivo bez upotrebe takvih stabilnih sustava.

Mnoge prednosti koje ovi sustavi imaju jesu u postupku gašenja (neovisnost o ljudskom faktoru, brzo započinjanje gašenja, učinkovito gašenje bez opasnosti za ljudske živote, odsutnost panike kod nastanka požara i sl.). Dokazana djelotvornost tih sustava koja se temelji na jednom od osnovnih načela za uspješno gašenje požara, a to je pravodobno započinjanje akcije gašenja, ima za posljedicu višu razinu zaštite ljudskih života i materijalnih dobara.

Ovisno o vrsti dobara koja se štite i različitih klasa požara koji mogu nastati, za gašenje požara primjenjuju se različiti stabilni sustavi.

Protupožarna zaštita IKT centara ima za cilj zaštitu ljudskih života, ali i zaštitu vrijednih informacija, imovine, te omogućavanje kontinuiteta poslovanja. Iz tog razloga se normom NFPA 75 preporučuje posebna pozornost prilikom izbora sredstva za gašenje koje bi trebalo biti neškodljivo za ljude i opremu, te da ne ostavlja nikakav trag na površinama prostora u kojem je izvršeno gašenje – upotreba tzv. „clean agent" sredstava.

Loša strana ovih sredstava je u tome što su za učinkovito gašenje potrebne dosta precizne koncentracije, što proračun sustava čini vrlo složenim u nekim okolnostima pa zbog toga proizvođači sustava vode poseban nadzor nad projektantima sustava, a po potrebi provjeravaju projekt i sami projektiraju sustave *(Carević, Jukić, Sertić, Šimara, 2002.)*.

Osim toga, „clean agent" sustavi su "one-shot" dizajn sustavi, tj. ako požar ne bude ugašen prilikom inicijalnog djelovanja sustava, ne postoji druga šansa. Ovaj sustav ne može se upotrebljavati dok se ponovo ne napuni ili poveže s back-up izvorom. Zbog toga se u po-

sebno osjetljivim situacijama preporučuje kombiniranje „clean agent" sustava i „pre-action" sustava za gašenje vodom koji bi se aktivirao ako se djelovanjem „clean agenta" požar ne stavi pod kontrolu. Sustavi za gašenje vodom mogu nastaviti gasiti vatru dok požar ne bude doveden pod kontrolu. Iako je vrlo vjerojatno da će se na taj način oštetiti elektronička oprema, ovo je više siguran način zaštite građevinske strukture.

ZAKLJUČAK

Donošenje Zakona o zaštiti od požara i vatrogastvu pridonijelo je u određenoj mjeri unapređenju i poboljšanju ukupnog stanja zaštite od požara u Federaciji Bosne i Hercegovine. Međutim, analize su pokazale da je i dalje prisutno neshvaćanje značaja i uloge zaštite od požara u suvremenim uvjetima privređivanja.

U odnosu na mjere zaštite od požara postoji veliki broj različitih propisa, tehničkih standarda i normativa. Kadrovi koji se na bilo koji način bave poslovima zaštite od požara moraju se upoznati sa svim propisima, standardima i normativima u kojima su regulirane mjere zaštite od požara za koje su oni nadležni. Samo se na takav način može pravilno postupati u planiranju i provođenju odgovarajućih mjera zaštite od požara.

Požarno preventivne mjere moraju se provoditi od faze projektiranja do faze puštanja u eksploataciju svakog tehnološkog sustava i procesa vezanog uz pojedine grane djelatnosti. Isto tako i za vrijeme eksploatacijskog vijeka istih, preventivnim održavanjem i ispitivanjem.

Organizacije u kojima se upotrebljavaju računala i mreže za podršku vitalnim poslovnim procesima trebaju osigurati odgovarajuće radno okruženja za njih. Ne učine li to, mogu povećati troškove poslovanja uzrokovane čestim zastojima.

Od vremena njihovog nastanka, IKT centri suočeni su s univerzalnom prijetnjom - požarima. Opsežna upotreba sustava za zaštitu od požara u IKT centrima ne proizlazi samo iz visoke vjerojatnosti pojave požara, niti od značajne opasnosti za život ljudi, već prije svega zbog mogućih poslovnih šteta uzrokovanih požarom. Stoga je nužno razmotriti potencijal i posljedice prekida u poslovanju neovisno o potencijalu za materijalnu štetu uzrokovanu požarom u IKT centrima. Međunarodne norme NFPA 75 i BS 6266 pružaju smjernice u vezi s protupožarnom zaštitom IKT centara, uzimajući u obzir specifična obilježja ovih okruženja.

LITERATURA

BS 6266:2011, Fire protection for electronic equipment installations. Code of practice, British Standards Institution (BSI), London, 2011.

Carević, M., Jukić, P., Sertić, Z., Šimara, B.: *Tehnički priručnik za zaštitu od požara (drugo izdanje),* Zagrebinspekt, Zagreb, 2002.

Hall, Jr. J. R.: *Computer rooms and other electronic equipment areas,* National Fire Protection Association Fire Analysis and Research Division, Quincy, 2012.

Lepušina, M.: *Priručnik za organizovanje zaštite od požara i vatrogastva u pravnim licima Federacije Bosne i Hercegovine,* Privredna štampa Sarajevo, Sarajevo, 2014.

Metodologija za izradu procjene ugroženosti od požara, Službene novine Federacije BiH, br. 8/11.

Network Reliability: A Report to the Nation; Fire Prevention in Telecommunications Facilities, Federal Communications Commission Network Reliability Council, 1993. referencirano u Robin M. L., Shaw B., Stilwell B.: Summary of Ongoing Class C Fire Research for the Purpose of Identifying and Evaluating Class C Fire Risks and Suppression Needs in Modern Data Centers, Internet Service Providers and Telecommunications Facilities, **Proc. 2008 Suppression and Detection Research and Applications Conference (SUPDET 2008)**, Orlando, FL, March 11-13, 2008.

NFPA 75: Standard for the Fire Protection of Information Technology Equipment, National Fire Protection Association (NFPA), Quincy, 2013.

NFPA 76: Standard for the Fire Protection of Telecommunications Facilities, National Fire Protection Association (NFPA), Quincy, 2012.

Nikolić, N. Lj., Petrović, M. V.: *Opasnost i zaštita od električne struje,* Institut za dokumentaciju zaštite na radu, Niš, 1979.

Purt, G. A.: The evaluation of the fire risk as a basis for planning automatic fire protection systems, *Fire Technology,* 8, 1972., 4, 291-300.

Robin, M. L.: Fire protection for electronic equipment, *SFPE-SAC Conference,* October 16-20 Al-Khobar, Saudi Arabia, 2010.

Treyger, B.: Protecting Your Most Valuable Assets, *The Data Center Journal,* October 11, 2012.

Zakon o zaštiti od požara i vatrogastvu, Službene novine Federacije BiH, br. 64, 2009.

FIRE PROTECTION IN ICT CENTRES

SUMMARY: Organizations that use computers and networks to support their vital business processes should provide adequate working environment for them. Failure to do so may lead to an increase in operating costs caused by frequent interruptions. From the time of their creation, ICT centres face a universal threat - fire. Extensive use of the fire protection system in ICT centres does not derive from a high probability of fire occurrence or from significant danger to human life, but it is primarily intended to curb potential damage to the business that may be caused by fire. It is therefore necessary to discuss the likelihood and consequences of the business interruption, independently of the potential damages that may be caused by fire in ICT centres. This paper presents the key issues in fire protection in ICT centres and the relevant legal obligations in force in the Federation of Bosnia and Herzegovina.

Key words: *ICT centres, fire protection, information security, legal obligations*

Professional paper
Received: 2015-01-05
Accepted: 2016-01-04