UDK: 004.738.5:339 | DOI: 10.5937/etp/1904065Č
Datum prijema rada: 11.11.2019.
Datum korekcije rada: 29.11.2019.
Datum prihvatanja rada: 12.12. 2019.

STRUČNI RAD

EKONOMIJA
TEORIJA I PRAKSA
Godina XII • broj 4
str. 61–81

BEZBEDNOSNE IMPLIKACIJE DIGITALNOG POSLOVANJA

Čelik Petar [1]

Sažetak: *U novije vreme, digitalna transformacija poslovanja i sajber bezbednost izazivaju veliko interesovanje ne samo poslovnih i političkih krugova već i naučno-istraživačkog sektora. Digitalna tehnologija je poslednjih godina ubrzanim tempom dramatično promenila, redizajnirala i ubrzala način poslovanja, obrazovanja, zabave, javnog sektora, kao i drugih društvenih segmenata. Konfiguracija i obim promena, uz neizbežnu disrupciju odvijaju se na tri nivoa: individualnom, organizacionom i društvenom nivou. Digitalna transformacija je, svojim neposrednim uticajem na svest, ideje, ponašanje i promenu paradigme, fokusa i načina poslovanja, nesumnjivo dovela do stvaranja i ekspanzije digitalne ekonomije, kao potpuno novog i do tada nepoznatog modela tržišnog poslovanja. Paralelno sa razvojem novih poslovnih modela i načina privređivanja, disruptivne tehnologije su u kompleksnom globalnom okruženju postale veliki izazov i svojevrsna pretnja i samom modelu digitalnog poslovanja, zbog neograničenih mogućnosti zloupotrebe tehnologija i njihovih slabih strana i tako nastalog disbalansa između veoma brzog razvoja tehnoloških inovacija i njihove implementacije, sa jedne, i pratećih mehanizama zaštite i bezbednosnih izazova, sa druge strane.*

Ključne reči: *digitalna transformacija poslovanja / digitalna ekonomija / disruptivne inovacije / digitalizacija / sajber bezbednost.*

[1] Visoka strukovna škola za preduzetništvo, Majke Jevrosime 15 Beograd, tel:+381 63 442 009, e-mail: petarcelik@sbb.rs

UVOD

U terminološkom smislu, digitalna transformacija postoji više od 15 godina. Sa protokom vremena, digitalna transformacija se terminološki sve češće koristi da objasni ili opiše opsežne društvene promene koje se odvijaju pod uticajem novih tehnologija, ujedno sa tim i kako te promene kao celina ostvaruju uticaj na poslovanje kompanija i rad javnih servisa.

Kako je digitalna transformacija po svom značenju nezaokružen termin, samim tim ovaj vid transformacije se različito i definiše. To je doprinelo da danas ne postoji jedno opšteprihvaćeno ili univerzalno određenje ovog pojma, već se najčešće pod ovim terminom podrazumeva potpuno nov način poslovanja diktiran tržišnim uslovima, a zasniva se na primeni savremenih tehnologija i disruptivnih inovacija. Prema nekim autorima, digitalna transformacija predstavlja korišćenje novih tehnologija, pri čemu tehnologija nije ključna, već se radi o uvođenju novih digitalnih biznis modela u poslovanje i prilagođavanje svog poslovanja novim digitalnim trendovima.

Ovaj rad akcenat stavlja na pojmove kao što su digitalna transformacija, disruptivne tehnologije i inovacije, digitalizaciju ekonomije, a isti se obrađuju stavljaju u kontekst pojma bezbednosti informacionih sistema sa osvrtom na poverljivost, integritet i dostupnost informacija, kao i bezbednost Cloud-a kao neizostavnog segmenta modernog poslovnog konteksta. Rad se zaokružuje osvrtom na prednosti i vrednosti digitalnog poslovanja i kao takav čini kontekstiranu osnovu za dalja naučna istraživanja.

Na globalnom nivou, digitalna transformacija najbrže je rastući poslovni trend u oblasti informacionih tehnologija. Polazeći od toga da digitalna transformacija nije samo tehnološki trend, već da se nalazi u samom centru poslovnih strategija gotovo svih industrijskih segmenata i tržišta, autori kao što su Westermann i dr. preciziraju digitalnu transformaciju kao kontinuirani proces kojim se preduzeća prilagođavaju ili pokreću disruptivne promene kod svojih klijenata ili na tržištima, iskorišćavajući digitalne kompetencije za noveliranje poslovnih modela, proizvoda i servisa koji bešavno spajaju digitalno, fizičko, poslovno i korisničko iskustvo, istovremeno unapređujći operativnu efikasnost i performanse postojeće organizacije (Westerman et. al. 2012).

Nakon što su ubrzale protok informacija i povećale kapacitet komunikacijske umreženosti i značajno pojednostavile i olakšale proces

proizvodnje i pružanja usluga, informacione i digitalne tehnologije ulaze u svoju poslednju ili završnu fazu – digitalizaciju stvari (Jovković, Čelik, 2017).

Osnovni činilac digitalne transformacije je sama informacija. S obzirom na količinu i protok informacija, informacija se zapravo ispostavila kao najvažniji i najtraženiji resurs modernog poslovnog konteksta. Pogrešno je uverenje da postoji univerzalna formula sprovođenja digitalne transformacije (Internet ogledalo, 2016). Digitalna transformacija sa sobom nosi nov način razmišljanja, nov organizacioni dizajn i pristup rešavanju problema (Petković, M. 2013).

U izvornom smislu, disruptivne tehnologije i inovacije najčešće su dolazile u talasima. Međutim, za kratko vreme, svet digitalnih trendova pokazao je i svoju drugu stranu. Četvrta industrijska revolucija, tj. Industrija 4.0, bar za sada, ima skoro nesagledivu dubinu i širinu. Takav trend razvoja Industrije 4.0 svakodnevno aktuelizuje brojne pretnje i rizike u oblasti digitalnog poslovanja, koji kao takvi pretenduju na često veoma zahtevno i prilično obuhvatno redefinisanje uspostavljenih strateških agendi, a sa tim i promenu u dizajnu operativnih zaštitnih mehanizama, i to ne samo u sferi digitalne ekonomije, već i u sferi cele države i njenog aparata (Schwab, K. 2016). Na ovaj način, digitalna transformacija poslovanja izvršila je opsežan uticaj na svest svih njenih činilaca i aktera. Digitalna transformacija nije samo promenila ideale, već i ponašanje i paradigme, usled čega je redefinisala fokus i načine poslovanja, stvarajući tako novi, nedovršeni i još uvek nezaokruženi tržišno-poslovni model.

Disruptivne tehnologije, kada se posmatraju kao deo kompleksnog globalnog okruženja, ispostavile su se i svojevrsnom pretnjom digitalnom poslovanju kao modelu, obzirom da neograničene mogućnosti tehnologije obrnuto proporcionalno daju i neograničene mogućnosti tehnološki zasnovanih zloupoteba slabih strana digitalno-tehnološkog poslovnog modela, što je postalo stalna pretnja koja izaziva disbalans na relaciji tehnoloških inovacija i njihove primene sa jedne strane i pratećih zaštitnih mehanizama i bezbednosnih izazova sa druge strane.

Prema zvaničnim podacima briselske administracije i procenama novijih studija, Evropski sektor IKT predstavlja oko 4% BDP i zapošljava više od 6 miliona ljudi, što ga čini važnim delom privrede. Digitalizacija proizvoda i usluga industrijskom sektoru će u Evropi sledećih 5 godina

doneti više od 110 milijardi evra prihoda godišnje. Očekuje se da će u razdoblju od 10 godina dalja digitalizacija industrije samo u Nemačkoj dovesti do povećanja produktivnosti do 8% i rast prihoda od 30 milijardi evra godišnje (Boston Consulting Group, 2015).

Nivo digitalizacije pojedinih ekonomija ili sektora različit je, i na tom planu postoje ogromne diskrepance. Većina evropskih kompanija svrstane su u dve kategorije – „digitalne istraživače“ i „digitalne igrače“. Najkraće rečeno, kompanije često priznaju potrebu za digitalnom transformacijom, ali su u ranoj fazi transformacije postojećeg (klasičnog) poslovnog modela u digitalni.

Kada se posmatraju u širem kontekstu, transformacione ideje i inicijative ili konkretni napori, najčešće se fokusiraju na optimizovanje postojećih poslovnih procesa, a manje na razvoj digitalnih proizvoda ili razvijanje novog dublje profilisanog digitalnog poslovnog modela. Kompanije koje posluju po ovom modelu nazivaju se „digitalnim otpornicima“, s obzirom da nemaju strategiju digitalne transformacije, a moguće inicijative su na strateškom nivou nedovoljno usklađene.

Sa druge strane, digitalni transformatori su one kompanije koje isporučuju digitalne proizvode, usluge ili iskustva, dok su digitalni remetioci „disruptori“ vrlo agresivni u primeni novih digitalnih tehnologija i poslovnih modela za obnavljanje i stvaranje novih tržišta. (Dell Technologies, 2016)

Stručnjaci iz oblasti tehnologije i biznisa, slažu se da je danas, obzirom na opseg primene i dostupnost, digitalna transformacija ključ opstanka i razvoja svake kompanije, a da je aplikacija okosnica te transformacije.

U cilju iskorišćavanja digitalnih mogućnosti i inovativnih potencijala, Evropska komisija je 2016. godine usvojila strateško viziju industrijske politike u komunikaciji, pod nazivom "Digitalizacija evropske industrije – iskorišćavanja prednosti jedinstvenog digitalnog tržišta".

Nova strateška vizija i uspostava jedinstvenog digitalnog tržišta fokus stavlja na četiri glavne teme: 1. tehnologije i platforme; 2. norme i referetne arhitekture; 3. geografsku koheziju koju predstavlja mreža regionalnih inovacijskih čvorišta; 4. veštine na svim nivoima (Evropska komisija, 2016).

DIZAJNIRANJE I KONTEKST INFORMACIONE BEZBEDNOSTI U DIGITALNOM POSLOVANJU

Sve veća učestalost napada na informacione sisteme i informacionu infrastrukturu, bilo kompanija ili institucija čiji rad podrazumeva posedovanje poverljivih sadržaja, kao što su lični podaci korisnika, korisnička imena i lozinke, dokumenti poverljivog sadržaja, itd., iznedrili su potrebu za bližim uređenjem pravila koja bi trebalo zaštititi i materijalne i intelektualno-svojinske vrednosti takvih organizacija. Imajući u vidu činjenicu da napade nije moguće ni sa sigurnošću predvideti, a često ni sprečiti, to ne umanjuje potrebu za preduzimanjem svih raspoloživih mera predostrožnosti kako bi se šteta koju bi sajber napad prouzrokovao, smanjila na najmanju moguću, tj. razumnu meru.

Činjenica je takođe, da je najčešći motiv sajber napada sticanje protivpravne finansijske koristi. Međutim, činjenica je i da je u velikom broju slučajeva u kojima su sajber napadi izvršeni, finansijska šteta bila manja od one koja je određenom sistemu naneta otkrivanjem u njemu poverljivih informacija. Ovakav činjenični korpus, na temelju iznetog, zahteva dizajniranje i definisanje prefinjene kontekste informacione bezbednosti u digitalnom poslovanju.

Da bi to bilo moguće, neophodno je izvršiti jasno definisanje rizika i sigurnosnih pravila koja su u stanju obuhvatiti celokupni područni kontekst poslovnih segmenata podložnih nekim vrstama napada. Ta pravila nazivamo sigurnosnom, odnosno bezbednosnom politikom. Cilj takve politike je da uredi dizajn i kontekst pravila ponašanja i suštinski uredi odgovornosti u odnosu na određeni informacioni sistem, kako bi na tim temeljima došlo do minimiziranja svih potencijalnih šteta i posledica koje tako mogu nastati, bilo putem namernih ili nenamernih radnji ili delovanja.

Prema Mijalkoviću i Keseroviću (2010.), rizik je verovatnoća nastupanja štetne posledice u slučaju izlaganja opasnostima, dok Milutinović (2013.) precizira da je bezbednosni rizik zapravo kalkulisana prognoza nastajanja negativnih događaja (opasnosti) koji uzrokuju gubitke i štete, odnosno kalkulisana prognoza nastajanja pozitivnih događaja (prilika/šansi) koje nam donose koristi.

Visok nivo zaštite informacionog sistema podrazumeva se u svim slučajevima, a posebno kada određena organizacija ima definisanu i u

upotrebu formalno uvedenu bezbednosnu politiku, dok bezbednosna politika kao pristup ima ulogu podizanja nivoa svesti zaposlenih o važnosti informacione bezbednosti, te kontinuirane edukacije o njoj i prepoznavanju mogućih rizika i posledica bezbednosnih incidenata. Bezbednosna politika je, stoga, skup pravila, smernica i postupaka koji definišu na koji se način informacioni sistem može učiniti bezbednim i kako moraju štititi njegove tehnološke i pohranjene informacione vrednosti.

Bezbednosna politika služi da korisnike uputi na ono što im je dozvoljeno, odnosno nedozvoljeno činiti, kao i kakve su konsekvence u slučaju odstupanja od ovih pravila. Samim tim, bezbednosnom politikom se ne određuje način zaštite informacionog dobra, već samo šta je predmet zaštite. Ovo je važno, jer svakodnevni intenzivni razvoj tehnologija otkriva i sve novije metode kojima je moguće ugroziti štićeni sistem. Uopšteno definisanje bezbednosne politike za informacione sisteme i dobra nije moguće, obzirom da bezbednosna politika mora biti proaktivno postavljena, pa se kao takva mora redovno preispitivati, menjati i dopunjavati. Ipak, bezbednosna politika obuhvata široka područja bezbednosnih mera, ali razloženo prema potrebama određenih grupa korisnika. Primera radi, zaposleni koji koriste sistem ne moraju poznavati i deo bezbednosne politike koji se odnosi na parametre tehničke opreme ili onaj deo politike bezbednosti namenjen spoljnim korisnicima ili saradnicima, što samim tim preporučuje projektovanje bezbednosne politike iz više delova (Kovačević, 2008. str.3).

ODREĐENJE POJMA I SADRŽAJA INFORMACIONE BEZBEDNOSTI

Pojam informacione bezbednosti nastao je u SAD na osnovu teorije informacionog ratovanja ili izvorno „Information Warfare“-a. Prema Danielu Vulfu, 60-ih godina XX veka pojavio se i termin komunikacione bezbednosti ili izvorno „COMSEC- Communication Security“.

Sa značajnijom pojavom i primenom računara, 70-ih godina XX veka, nastala je i kompjuterska bezbednost ili izvorno „COMPUSEC – Computer Security“. Do kraja 80-ih godina, usled ekspanzije računarstva, COMSEC i COMPUSEC objedinjeni su u Informacionu bezbednost ili izvorno „INFOSEC – Information Security“, čime je učinjen pokušaj da se integrišu ove ranije potpuno odvojene discipline, kao što su bezbednost osoblja, kompjuterska, odnosno računarska bezbednost sa komunikacionom i operativnom bezbednošću (Wolf, 2003).

Akcenat na kome je nastao „INFOSEC“ već na samom početku stavljen je na sprečavanje neovlašćenog pristupa informacionim sistemima i njihovim resursima. Tada je takođe došlo do razmatranja temeljnih postavki bezbednosti u smislu poverljivosti, integriteta i raspoloživosti informacija.

Dalji razvoj računarstva koji je doveo do nastanka umrežavanja i pojava mreža LAN i WAN, a pre svega Internet-a, dovodi do proširenja liste informacionih svojstava pred koja se postavljaju bezbednosni zahtevi, a to su autentičnost i neporecivost.

Prema savremenim shvatanjima pojma nacionalne bezbednosti, informaciona bezbednost predstavlja jednu od osnovnih komponenti nacionalne bezbednosti, što ovu problematiku čini krajnje i trajno aktuelnom (Sinkovski, 2005:31-81).

Prema odredbama Zakona o informacionoj bezbednosti Republike Srbije, član 2, stav 1 tačka 3, „informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica“.

Reformisano zakonodavstvo o zaštiti podataka pruža stoga brojne mehanizme za nesmetan međunarodni prenos podataka. Osnovna svrha tih pravila i mehanizama, ne samo na nivou nacionalnih država, već i na nivou EU pledira da osigura da lični podaci evropljana budu zaštićeni u svakom trenutku njihovog prenosa u inostranstvo. U posebnom dokumentu Evropske Komisije predstavljen je sveobuhvatan i pojednostavljen okvir EU za razmenu i zaštitu ličnih podataka u globalnom okruženju. (Pejanović, Komarčević, Čelik, 2017)

Poverljivost

Poverljivost čini zaštitu informacija na nivou sprečavanja njihovog otkrivanja od strane neovlašćenih lica ili sistema. Ukoliko se dogodi da se štićenim, odnosno poverljivim informacijama ne rukuje na pravilan način, može doći do povrede njihove poverljivosti, a time i nedozvoljenog otkrivanja ovih informacija, bilo da je to učinjeno usmenim putem, njihovim štampanjem, kopiranjem, slanjem elektronskom poštom, itd.

(Zakon o tajnosti podataka, Sl. Glasnik RS br.104/2009).

U smislu toga, za najčešće pretnje poverljivim informacijama smatraju se:

- Napadači – koji zloupotrebom bezbednosnih propusta pokušavaju otkriti i pribaviti štićene informacije, bilo radi sopstvene koristi ili radi zloupotrebe tih informacija i njihovog objavljivanja na internetu;
- Lažno predstavljanje – radi dobijanja mogućnosti pristupa poverljivim informacijama, zloupotrebom lozinke drugog korisnika;
- Neovlašćena aktivnost – kada korisnik sistema podatke menja, briše, kopira i sl., suprotno svojim ovlašćenjina;
- Kopiranje podataka na nezaštićene lokacije – kada se ugrožavanje poverljivosti podataka vrši njihovim kopiranjem na sisteme sa nedovoljnim nivoom zaštite;
- Zlonamerni programi – u pitanju su programi kojima je moguće ostvariti neovlašćen pristup sistemu koji sadrži poverljive podatke, radi njihovog neovlašćenog otuđenja.

Integritet

Prilikom rukovanja podacima, od izuzetne je važnosti očuvanje njihovog punog integriteta koji se postiže time što korisnik nema mogućnost da izmeni podatke bez odobrenja, pa integritet podataka znači da su podaci o kojima je reč, potpuni i ispravni i jednoznačni, tj. u skladu sa svojim izvorom (Kovačević, 2008., str. 5).

Važan segment zaštite je i sprečavanje mogućnosti u kojima se može dogoditi, bilo nameran ili nenameran slučaj narušavanja integriteta podataka. Na ovaj način osigurava se puna tačnost i ispravnost podataka pohranjenih u velikim informacionim sistemima, a to se postiže nekom od vrsta autentifikacije korisnika putem utvrđivanja njegovog identiteta, za šta se najčešće koriste jednokratne lozinke, pametne kartice, biometrijski čitači i sl.

Nakon eliminisanja mogućnosti neželjenih namernih izmena poverljivih podataka, veoma je važno održati oprez koji će u najvećoj meri garantovati da se neće dogoditi ni slučajne izmene u domenu poverljivih podataka. Ovaj efekat može se postići organizovanjem strogo poverljivog i profesionalnog radnog okruženja, koje će postati garant da neće doći ni do namernih, ni nenamernih izmena podataka, međutim, tu ne treba

izostaviti ni institucionalne okvire koji treba da podrže ovakve kontekste, imajući u vidu da kontekst digitalnog poslovanja sam po sebi ima globalni, tj. prekogranični karakter u kome se sudaraju pravni okviri država i njihovi digitalno/poslovno/bezbednosni interesi.

Prema izmenjenoj uredbi usvojenoj od strane Evropskog parlamenta i Veća Evrope i Europol dobija nove, uz proširenje postojećih zadataka (Evropski parlament, 2016):

- prikupljanje, skladištenje, obrada, analiza i razmena informacija, uključujući kriminalističke obaveštajne podatke,
- obaveštava države članice bez odlaganja o svim važnim informacijama,
- obavlja koordinaciju, organizaciju i sprovođenje istražnih i operativnih radnji,
- učestvuje u zajedničkim istražnim timovima i predlaže njihovo osnivanje,
- pruža informacije i analitičku podršku državama članicama u vezi sa međunarodnim događajima,
- priprema procenu opasnosti, strateški i operativnih analiza i izveštaja o opštem stanju bezbednosti,
- podela i unapređenje stručnog znanja o metodama sprečavanja kriminala, istražnim postupcima, tehničkim i forenzičkim istragama i dr. (Pejanović, Komarčević, Čelik, 2017)

Dostupnost

Svrha informacionog sistema jeste da informacije sadržane u njemu učini uvek i u svakom trenutku dostupnim njihovim korisnicima. Da bi to bilo moguće, potrebno je u svakom trenutku osigurati njegov rad. Da bi se to ostvarilo, neophodno je u punom formatu vršiti održavanje sistema za unos i obradu informacija, sistema za zaštitu, komunikacionih kanala i infrastrukture putem kojih se pristupa pohranjenim informacijama i sistemu.

U praksi, do nedostupnosti informacija najčešće dolazi zbog DoS (Denial of Service) napada, odnosno prestanka mogućnosti obrade podataka od strane servera. Kada je u pitanju DoS napad, pod njim se smatra svaka vrsta napada na server koji ima za cilj onemogućavanje njegovog rada u odnosu na ovlašćena lica i korisnike. Mehanizam ove vrste napada je

takav da napadač organizuje napad na informacioni sistem, tako što sa velikog broja računara ili Bot Net mreže IoT istovremeno šalje ogroman broj zahteva, koji prevazilazi meru koju ovaj sistem usled tehničkih ograničenja može podneti, što samim tim dovodi do toga da informacioni sistem prestane primati i obrađivati sve dalje zahteve, čime ovlašćenim licima i korisnicima onemogućava dalji pristup podacima i onemogućava svaki rad.

Da bi se DoS napad sproveo, potrebno je da napadač, najpre korišćenjem bezbednosnih propusta u sistemima, uspostavi kontakt sa takvim računarima i sistemima, nakon čega na teret tih propusta preuzima kontrolu nad tim računarima, od njih organizuje Bot Net mrežu i usmerava resurse ovako stvorene mreže, tj. ogromni saobraćaj na server koji se napada, a koji usled takvog enormnog saobraćaja nije više u mogućnosti da funkcioniše, usled čega počinje da odbija sve pristigle zahteve, bilo spolja, bilo od ovlašćenih korisnika iznutra.

Ipak, do gubitka mogućnosti za obradu podataka u informacionom sistemu ne dolazi samo iz ovih razloga, već se to može dogoditi i kao posledica prirodnih katastrofa, ali i zlonamernih, nesavesnih ili nestručnih aktivnosti ljudi u odnosu na informacioni sistem. Samim tim, i prirodne katastrofe (zemljotresi, požari, poplave i sl.) mogu biti jednak uzrok prestanka normalnog rada sistema, kao i ljudsko delovanje, bilo ono namerno ili nenamerno, čime ova vrsta delovanja, bez razlike, može izazvati jednako ozbiljnu štetu i posledice.

U ovakvim slučajevima, preduzimaju se odgovarajuće mere čiji je zadatak da obezbede stalnu dostupnost podataka i resursa informacionog sistema. Najpre, tu treba pomenuti fizičke mere bezbednosti, kojima se postiže fizičko-tehničko sprečavanje neovlašćenog pristupa informacionom sistemu i njegovim delovima, a time i ostalim sistemima koji bi mogli dovesti do bilo koje neplanirane ili nedopuštene promene u poslovnom okruženju.

Uporedo sa tim, preduzimaju se i druge tehničke mere, kao vrsta mera čiji je zadatak da obezbede ispravnost i funkcionisanje, kako informacionog sistema, tako i svih njegovih delova. Najčešće, to se postiže tzv. mirroring-om, koji obezbeđuje da se istovremeno sadržaj nosašča podataka višestruko iskopira, pa ukoliko bi se dogodilo da se neki od nosača pokvari ili iz drugog razloga prestane sa radom, naredni nosač sa identičnim sadržajem preuzeće njegovu funkciju i obezbediti efekat visoke redundantnosti ovako koncipiranog informacionog

sistema.

Pored ovakvih hardverskih, preduzimaju se i odgovarajuće softversko-tehničke mere kojima se vrši stalno testiranje ispravnosti rada softvera uz obaveznu izradu bezbednosnih kopija, čak i za slučaj u kome bi došlo i do prestanka napajanja sistema električnom energijom.

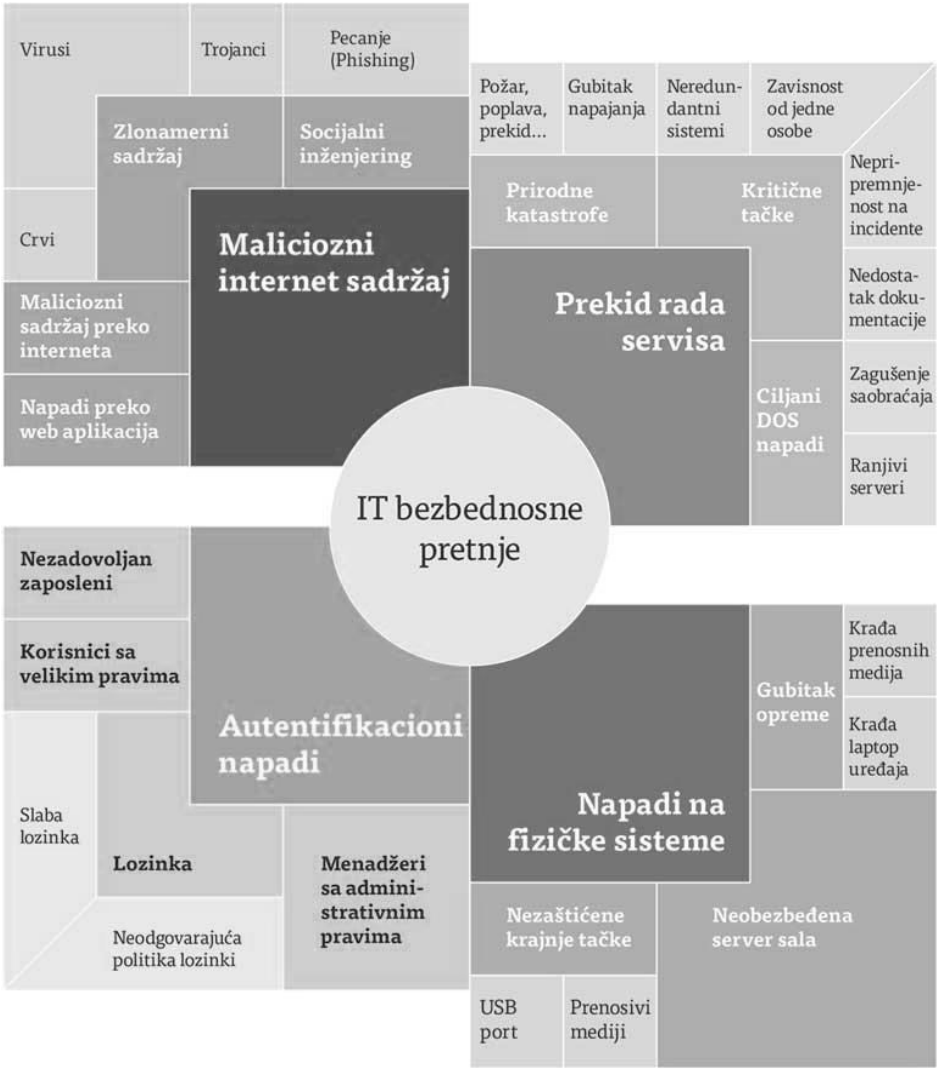
Da bi se uspostavili svi bezbednosni standardi, potrebno je uspostaviti poštovanje bezbednosne politike postojeće organizacije, kako bi se doslovno i bez izuzetka primenjivali svi propisani standardi iz domena bezbednosti informacionog sistema. Takav način rada dalje obezbeđuje upravljanje bezbednosnom politikom prema jasnim standardima, kako bi se na taj način najpre obezbedili svi aspekti zaštite informacionog sistema, i u sklopu toga, uspostavio puni kvalitet primenjenih mera bezbednosti (Kovačević, 2008. str.7).

BEZBEDNOST CLOUD-A

U proteklom periodu, naročito u poslednjoj deceniji, bezbednost podataka iz domena poslovanja predstavlja krucijelni element postojanja kompanija. Uporedo sa tim, element zaštite od pretnje i rizika po ovaj segment, zahteva i angažovanje brojnih resursa koji su potrebni za ostvarivanje ove zaštite.

Problem u ovoj oblasti postoji i zato što veliki broj kompanija na tržištu i dalje nema razvijenu poslovno-bezbednosnu svest iz ovog domena, usled čega se ispostavlja da, ukoliko postoji takva konstelacija u organizaciji, čak ni najveći poslovni sistemi nisu u stanju držati korak, kako sa agresivnim konkurentskim okruženjem, tako ni sa rizičnim okruženjem koje se nadvija iz sajber prostora nad svakom organizacijom.

Slika - *IT bezbednosne pretnje*



Izvor: https://coming.rs/bezbednost/

Da bi kompanija postala cloud provajder, ona prethodno mora ispuniti određene međunarodne standarde, kao što je na primer ISO standard za zaštitu informacija 27001. Uporedo sa tim, poslovna praksa uspostavila je i obavezu potpisivanja NDA ugovora (Non Disclosure Agreement), koji zakonski u potpunosti štite korisnika i privatnost njegovih podataka, a taj segment je dodatno pojačan od stupanja na snagu uredbe GDPR Evropske Unije (General Data Protection Regulation). Samim tim, cloud

provajder, iako se podaci korisnika nalaze na infrastrukturi koja mu pripada, kao pružalac cloud usluge nema pravo da pristupi podacima korisnika bez obezbeđivanja pisanog pristanka njihovog vlasnika.

U određenim tehnološkim krugovima, cloud tehnologija se često predstavlja i za tehnologiju štednje. Ipak, zabrinutost kompanija za svoje poslovne tajne i bezbednost podataka i dokumenata, ne prestaje, s obzirom na značajan nedostatak referenci cloud provajdera, što čini da kompanije koje bi se možda i odlučile za prelazak na ovu tehnologiju i vid usluga, nisu spremne na to da se poslovni podaci iz njihovog poseda presele na tuđe servere i infrastrukturu i tako postanu deo za njih nekontrolisanog okruženja.

Mnoge kompanije, kada se pomene cloud tehnologija i dalje pristaju da plaćaju veću cenu poslovanja, kako ne bi izgubili sopstvenu autonomiju nad podacima i tehnologijom obrade koju koriste, tj. kako ne bi došle u situaciju da se izlože rizicima koji nastaju sa curenjem, tj. narušavanjem poverljivih podataka, koje bi moglo dovesti do gubljenja poverenja klijenata, i time drugih pravnih i finansijskih posledica povezanih sa tim, o čemu je već bilo reči.

Sa druge strane, postoje kompanije koje posluju na globalnom nivou, usled čega njihova poslovna politika onemogućava čuvanje poslovnih podataka na sistemima koji su u tuđem vlasništvu. Takve kompanije su napravile poslovni kompromis koji zadovoljava ove potrebe (i racionalnu i bezbednosnu), usled čega su uspostavile određenu vrstu privatnog računarskog oblaka, koji kao takav svakako ima svojih nezanemarljivih prednosti.

Ipak, kada je reč o malim i srednjim preduzećima, odnosno biznisima u razvoju koji nemaju potencijal kakav imaju velike organizacije, čini se da je za njih računarstvo u oblaku, odnosno Cloud computing, idealno poslovno i bezbednosno rešenje.

S obzirom da cloud provajder ne može biti bilo ko, već samo onaj ko zadovoljava, pored tehničkih kriterijuma, naročito i one bezbednosne, to je mnoge kompanije usmerilo prema tom rešenju. Tako, kada se donosi poslovna odluka kompanije o prelasku na cloud servise, tu se suštinski radi o opredeljenju kompanije da primeni principe autsorsinga, tj. eksternalizacije određenih poslovnih funkcija. Eksternalizacija vitalnih poslovnih funkcija, odnosno poveravanje istih spoljnim saradnicima i partnerima, svakako mora podrazumevati primenu svih poslovnih i bezbednosnih standarda koje kompanija inicijalno ispunjava, ili su joj

potrebni za rad i funkcionisanje, a te uslove i zahteve i eksterni provajder mora zadovoljiti ili u toj meri u kojoj to čini sama kompanija, ili u meri koja prevazilazi ova očekivanja i pretpostavke.

Kada kompanija sve svoje poslovne aktivnosti zasniva na sopstvenoj IT infrastrukturi, sudeći po sadašnjim uzusima poslovanja, ona sebe izlaže troškovima, eksternim rizicima i pretnjama, a time i mogućim napadima koji suštinski mogu biti svakodnevni, s tim što rizici za poslovanje ne podrazumevaju samo eksternost, imajući u vidu da je praksa pokazala da štete i gubici veoma često nastaju i na temeljima internih rizika, bilo da su oni izazvani slučajno ili namerno od strane internih faktora.

Stoga, sve takve kompanije moraju primenjivati mere bezbednosti i prema unutra, i prema spolja, ali i u skladu sa tim merama primenjivati i odgovarajuća antivirusna i firewall rešenja, koja, naravno, imaju svoju cenu i stepen opterećivanja poslovanja u celini.

Kupovina i održavanje ovakvih proizvoda ima svoju cenu, koja neretko, ako se pribegava ozbiljnim rešenjima, prevazilazi projektovane vrednosti i očekivanja. Samim tim, trošak po ovom osnovu stalno raste, počev od segmenta kupovine i održavanja proizvoda, a onda i obnavljanja licenci, a tek iza toga i troškova u vidu organizovanja odgovarajućih infrastrukturnih i ljudskih resursa koji će biti odgovorni za uspostavljanje i održavanje ovog sistema, a na način koji treba da garantuje maksimalnu bezbednost i podataka i infrastrukture.

Sa druge strane, Cloud computing kao rešenje, tj. kao višeznačni servis, daje mogućnost kompaniji da kompletnu brigu u oblasti poslovne informatike, uključujući i bezbednost iste, prepusti cloud provajderu i njegovim profesionalnim i visokospecijalizovanim kadrovima, kako bi na taj način svoj poslovni problem i profesionalizovala i eksternalizovala, bez daljeg rasipanja resursa ili potrebe za investiranjem u ovu visoko osetljivu oblast.

Vremenom je nizom standarda, polisa, regulativa i tehnologija uređena i zaokružena kontrola i sigurnost podataka, njihovog prenosa i skladištenja, a profilisan je i tretman čitave infrastrukture primenjene u računarskom oblaku. Sve je više i preduzeća koja su implementirala sisteme upravljanja identitetom i njima regulisala pristup informacijama i primenjenoj računarskoj opremi. Takođe, ovaj mehanizam i standard neretko su primenjivani i na infrastrukturu računarskog oblaka, a posebno ukoliko klijent, odnosno korisnik istakne takav zahtev sa ciljem

da obezbedi da je pristup podacima i infrastrukturi moguć samo autorizovanim korisnicima i to na način što je svaki pristup podacima i infrastrukturi u svakom trenutku i bez izuzetka na odgovarajući način dokumentovan.

Ipak, ovakav vid racionalizacije poslovanja ne podrazumeva u celosti i prelazak odgovornosti za štete i posledice po korisnike kompanije u slučaju narušavanja bezbednosti podataka, s obzirom da korisnike objektivno ne zanimaju pozadinski potencijali kompanije kojoj je poverena saradnja, ili pozadinski problemi kompanije od koje kupuju proizvode i usluge, već ih isključivo zanima bezbednost njihovih podataka i ono što u svakom trenutku dobijaju za svoj novac.

U ovim okolnostima, odgovornost pružalaca usluga u cloud industriji raste, iz kog razloga cloud provajderi moraju da, imajući u vidu da je to njihova primarna delatnost, nivo bezbednosti i kvaliteta pružanja usluga kontinuirano održavaju na najvišem nivou, iz kog razloga su pojedini stručnjaci skloni tome da kažu da su podaci na cloud-u daleko bezbedniji, nego kada se nalaze na informacionoj infrastrukturi same kompanije, posebno kada se osvrnu na činjenicu da je to nekoj kompaniji prateća poslovna aktivnost, dok je cloud provajderu primarna i jedina.

Treba zato istaći da sve veći broj stručnjaka smatra da Cloud tehnologija kao poslovni izbor u domenu pružanja IT usluga ne predstavlja više pitanje da li će, već samo kada će tradicionalni IT gurnuti u prošlost, a da će tržište i pritisak konkurencije učiniti svoje u korist cloud rešenja i njegove poslovne sveprisutnosti.

Međutim, tendencija savremenog poslovanja već duže vreme podrazumeva i to da su komunikacioni kanali veoma često oni koji se zasnivaju na bežičnim i mobilnim mrežama, čime se prilikom komuniciranja od mesta inicijalnog zahteva do odredišta zapravo koristi tuđa IKT infrastruktura, pa je u tom smislu nastala i obaveza kompanija da uspostave i razvijaju odgovarajuće sisteme upravljanja bezbednošću informacija, kako bi i protok i manipulacija informacijama bili obavljeni jednostavno, brzo i efikasno, ali i na način koji uliva puno poverenje, kako među IT poslovnim partnerima, tako i među korisnicima na tržištu (Tepšić, Tanjga, 2011).

U tom smislu, neophodno je organizovati proaktivan pristup bezbednosti koji podrazumeva pravovremenu identifikaciju rizika radi obezbeđivanja bezbednog i sigurnog elektronskog poslovanja, negovanja dobre poslovne prakse, dostupnost informacija u zaštićenom i bezbednom

okruženju, efektivniji i efikasniji rad informacionih sistema, negovanje i produbljenje poverenja kompanije i njenih klijenata i partnera, poboljšanje tržišnog kredibiliteta i ugleda kompanije, efikasnije korišćenje informatičkih resursa neophodnih za čuvanje i razmenu podataka i istovremeno jasno uređivanje uloge i odgovornosti učesnika u svim ovim poslovnim procesima, što bi sve zajedno, kao pristup, ustanovilo potrebne preduslove za ostvarivanje jasno odredive konkurentske prednosti kompanije.

Zaštita i bezbednost informacija kompanije suštinski znači i zaštitu bezbednosti i za njen know-how. Iz ovih razloga, upravljanje rizikom na nivou definisanom međunarodno priznatim standardima i uz poštovanje principa dobrog upravljanja, u velikoj meri smanjuje mogućnost i verovatnoću nastanka nepredviđenih situacija. Ovakva organizacija, odnosno organizacija koja funkcioniše na ovim principima, nesumnjivo ima odgovarajuće preduslove da ostvari kompetitivnu prednost na tržištu.

Digitalna transformacija poslovanja, kao lice, u svom naličju ima brojne bezbednosne implikacije. Što je izraženiji informaciono-komunikacioni progres u oblasti digitalne transformacije poslovanja, utoliko dolazi i do većeg stepena usložnjavanja bezbednosnih tendencija i faktora. Jedan od ključnih razloga za to jeste što digitalna transformacija nije samo primena novih tehnologija u poslovanju, već jedna sveobuhvatna disruptivna transformacija bezmalo svih postojećih modela poslovanja, kako uopšte, tako i u načinima komunikacije i povezivanja svakog modernog preduzeća sa njegovim kupcima i dobavljačima, uključujući u to i državnu administraciju kao javni servis.

Ovakav „disruptivno-razarački“ model tradicionalnog poslovnog koncepta ne samo da zahteva već i podrazumeva novi sistem vrednosti, kreiranje novih poslovno-komunikacionih lanaca, a u skladu sa tim i sprovođenje promena u domenu marketinga, menadžmenta, zapošljavanja i radnih odnosa, tržišnog pristupa, interpersonalnih odnosa, kako unutar svake kompanije, tako i u relacijama svake kompanije sa njenim opštim i digitalnim okruženjem.

PREDNOSTI I VREDNOSTI KOJE STVARA DIGITALNO POSLOVANJE

Sve češće se u stručnim krugovima i diskursu govori o tzv. digitalnom rascepu, tj. digitalnom jazu i digitalnom usponu. Digitalizacija u najširem

smislu, tj. primena savremene IK tehnologije, bilo u državnoj upravi ili ekonomiji, kako pokazuju rezultati, dovodi do povećanja produktivnosti i konkurentnosti. U uslovima rastućih kompetitivnih pritisaka globalizovane ekonomije, ta dva elementa ne dovode samo do povećanja društvenog proizvoda ili blagostanja nacije, već se radi o imperativu zadržavanja priključka u odnosu na zemlje digitalne lidere, koje kao takve faktički predvode aktuelni, ali i budući tehnološki, a time i ekonomski razvoj.

Prednosti primene IK tehnologija su „ogromne i brojne:

- brža i učestalija pojava inoviranih usluga i proizvoda višeg nivoa kvaliteta sa nižom cenom;
- efikasnije upravljanje poslovnim i partnerskim procesima radi stvaranja vrednosnih lanaca;
- proširivanje tržišta i lakše sprovođenje vertikalne i horizontalne integracije preduzeća;
- smanjenje troškova elektronskih transakcija i brži povraćaj sredstava uloženih u e-poslovanje;
- povećanje brzine, efikasnosti i ekonomičnosti rada;
- nove poslovne mogućnosti bez obzira na lokaciju sedišta kompanije;
- dvadesetčetvoročasovno radno vreme, 365 dana u godini;
- povećanje zadovoljstva kupaca i korisnika usluga;
- velika prilagodljivost i brzina odgovora na zahteve kupaca;
- ogromne uštede u vremenu i opipljivim resursima; i
- povećanje ekonomičnosti, produktivnosti i rentabilnosti poslovanja“. (Miletić et. al., 2014:977)

Sveprisutnost novih tehnologija predstavlja ključni motor inovacija za budućnost digitalne ekonomije, najpre time što podržava savremene vizije budućnosti, kako sektora energetike, saobraćaja, zdravstva, itd., tako i transformaciju drugih sektora kreativne industrije, proizvodnje i sektora finansijskih usluga.

Kompanije koje su odabrale stratešku opciju primene savremenih tehnologija radi podizanja konkurentske prednosti ostvaruju povećan profit i više su usmerene ka korisničkim potrebama, što za rezultat ima

osnaživanje njihove tržišne pozicije i stvaranje poslovnog prestiža u konkurentskom okruženju.

ZAKLJUČAK

Primena disruptivnih tehnologija, moglo bi se reći, na tek donekle kontrolisani način utiče na ekonomske i opšte društvene procese, odnose i socijalna dešavanja. Samim tim, brzina promena korisničkog ponašanja, usled sticanja novih znanja i iskustava na tržištu, jasno dovodi do brze evolucije u korisničkim očekivanjima i načinu interakcije. Zato, bezmalo svakodnevo, „nad glavom" ekonomije stoji „mač" koji forsira kontinuiranu transformaciju svih ekonomskih sektora, jer se promene moraju dešavati na svim poljima, od poljoprivrede do infrastrukture, pa ove promene čak disrupuju i tradicionalne industrije poput transporta i proizvodnje.

Iznalaženje odgovora na pitanja u kom pravcu će se dalje odvijati tehnološki razvoj, koje tehnologije će izmeniti način proizvodnje, kakve će biti komunikacije i uopšte ponašanje ljudi u budućnosti, odnosno kakvi će tehnološki trendovi dominirati na globalnom, regionalnom ili lokalnom nivou, zahteva sveobuhvatnu projekciju inovativnih rešenja baziranih pre svega na korisničkim iskustvima, te brojnim istraživačkim i naučnim naporima usmerenim na rešavanje konkretnih društvenih, ekonomskih, egzistencijalnih i drugih pitanja i problema koji danas opterećuju gotovo sve zemlje, nezavisno od njihovog razvojnog ili tehnološkog statusa.

Rezimiranje ovakve situacije, kristalno jasno ispoljava da transformacija poslovanja u digitalno, u vreme u kome živimo, više nije stvar izbora. Ako neko želi da postoji i opstane, da se tržišno pozicionira na turbulentnom konkurentskom tržištu, onda on mora da zna da je digitalna transformacija poslovanja imperativ tog i takvog modela postojanja.

Poslovanje na digitalnom tržištu za koje više ne postoje geografske i teritorijalne odrednice, već nesagledivo širok i dubok sajber prostor u kome je svako od svakog na „klik" daleko i prostor u kome svako ko ima internet vezu i pametni uređaj može postati digitalni ponuđač i proizvođač, daje jednu široku iznijansiranu lepezu poslovnoj disrupciji i neizvesnosti.

Jasno je da su liderske kompanije shvatile ovaj izazov, pa su u tom pravcu inovirale načine komuniciranja sa svojim partnerima, uspostavile nove

modele saradnje sa potrošačima i javnom upravom, redizajnirale ključne poslovne procese itd., što je iziskivalo uspostavljanje i sasvim novih modela organizovanja.

Pritisak transformativne moći digitalnog poslovnog modela zahteva i nove načine upravljanja, kako horizontalno, tako i vertikalno, sve kako bi se stvorilo neophodno prostranstvo za unapređenje poslovne efikasnosti. Takva poslovna efikasnost podrazumeva istovremeno smanjenje troškova poslovanja, ali i maksimizaciju i racionalizaciju upotrebe postojećih i dostupnih resursa.

Ipak, pomenute prednosti i perspektive same digitalne transformacije, iznova daju ogromne pretnje i rizike. Prikupljena i analizirana iskustva jasno pokazuju da kompanije, bez obzira na svoju spremnost i obazrivost, veoma često nisu u stanju da prate tempo razvoja modernih tehnologija, a posebno ne bez toga da se izlože znanim i neznanim rizicima, dok sa druge strane ni same države ne uspevaju da pravovremeno i adekvatno pravnom regulativom obuhvate sve tehnološke promene i inovacije i odrede okvir za sankcionisanje njihovih bogato iznijansiranih zloupotreba.

Ovakvo „novo digitalno vreme“, pred istraživače je postavilo zahtev da oni razmišljaju kao inovatori sa jedne strane, a istovremeno i kao preduzetnici sa druge strane, jer svaka nova ideja i rešenje moraju biti prepoznati, imajući u vidu da će oni, bilo delimično, ili u potpunosti promeniti ili zameniti prethodnu tehnologiju ili neko primenjeno rešenje.

Digitalna ekonomija, a time i transformacija, svojom dinamikom su naprosto obrisale sve prethodno uspostavljene granice između tradicionalne materijalne i savremene (nove) digitalne ekonomije. Tako je došlo do razdvajanja resursno zasnovane ekonomije od ekonomije znanja, ili savremeno rečeno, ekonomije zasnovane na bitovima i bajtovima, tj. ekonomije čiju dodatnu vrednost generišu nove tehnologije, informacije i podaci, kao i njihova temeljna analiza i znanje stečeno na osnovu toga.

Ipak, dosadašnji razvoj digitalne ekonomije izdiferencirao je i neke svoje ključne komponente uz uvažavanje svih bezbednosnih izazova i rizika koji su na tom razvojnom polju stalno prisutni. U te komponente spadaju vlada, pravna regulativa, širok dijapazon politika, internet, www, telekomunikaciona industrija, provajderi digitalnih usluga, elektronsko poslovanje i elektronska trgovina, tehnološki generisane informacije, veštačka inteligencija i mašinsko učenje, sistemi za kreiranje i upravljanje znanjem, prava iz domena intelektualne svojine, ljudski

kapital i njegova primenjiva znanja, stalno istraživanje i razvoj i na tome nastale nove tehnologije i rešenja i njihove bezbednosne implikacije. Uzimajući u obzir sve ove elemente i pretpostavke, ovaj rad postavlja osnove za dalja istraživanja i usmerava buduća istraživanja i istraživače na trendove proporcionalnosti razvoja digitalne ekonomije i njenih bezbednosnih implikacija.

LITERATURA:

1. Boston Consulting Group., PwC, Opportunities and Challenges of the industrial internet. 2015. The future of productivity and growth in manufacturing industries, Preuzeto sa: https://www.zvw.de/media.media.72e472fb-1698-4a15-8858-344351c8902f.original.pdf
2. Bezbednost u računarskom obliku. Preuzeto sa: https://coming.rs/business-and-it/business-and-it-broj-4/bezbednost-u-racunarskom-oblaku/
3. Digital Transformation Index, (2016)., Dell Technologies EMC
4. Evropska komisija, (2016). *Digitalizacija evropske industrije: iskorišćavanje svih prednosti jedinstvenog digitalnog tržišta.* COM 180 final. Brisel
5. Internet ogledalo, (2016). *Četvrta industrijska revolucija.* Business & Technologies Magazine. Beograd, 61
6. Jovković S., Čelik P., (2017). „Dometi i ograničenja digitalizacije pravosuđa u Republici Srbiji“ – „Benefits and Limitations of Digitization of the Judiciary in Serbia“, XIV Međunarodni naučni skup, “Pravnički dani – prof. dr Slavko Carić“, Novi Sad,
7. Kovačević, D. (2008). Sigurnosna politika, Diplomski zadatak, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, 3-7
8. Mijalković, S., & Keserović, D. (2010). *Osnovi bezbednosti.* FBZ Banja Luka.
9. Miletić, Lj., Ničić, M., Ćurčić, R., (2014). *Uticaj informacionih tehnologija na lanac vrednosti i podizanje konkurentnosti preduzeća*, Međunarodna konferencija Univerziteta Union, Sinteza 2014, 977
10. Milutinović, M. (2013). *Izazovi savremenog društva u bezbednosti.* Zbornik radova 1 Pravo i bezbednost. IV Međunarodni naučni skup: Multikulturalnost i savremeno društvo. USEE. Pravne i poslovne akademska studije dr Lazar Vrkatić. Novi Sad.
11. Pejanović Lj., Komarčević M., Čelik P. (2017). *Centralizacija i militarizacija područja bezbednosti u Evropskoj Uniji,* Crisis Management Days, 10th International Scientific Conference,Velika Gorica
12. Petković, M. (2013). Uticaj infromacione tehnologije na dizajn organizacije: primer organizacije u zdravstvu. *Sociologija.* (3), Beograd

13. Schwab, K. (2016). *The Fourth Industrial Revolution.* World Economic Forum. Geneva, Switzerland
14. Sinkovski S., (2005). *Informaciona bezbednost – komponenta nacionalne bezbednosti,* Vojno delo, 2/2005, 31-81
15. Tepšić, M., Tanjga, R. (2011). Zaštita informacionih sistema, Banja Luka College i Besjeda
16. Westerman, G., Tannou, M., Bonnet, D., Ferraris, P., & McAfee, A. (2012). *The Digital Advantage: How Digital Leaders Outperform their Peers in Every Industry,* MIT Center for Digital Business and Capgemini Consulting
17. Wolf, D. (2003). Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development, Nacional Security Agency US, July 22, 2003
18. Zakon o tajnosti podataka, Službeni glasnik RS br.104/2009

SECURITY IMPLICATIONS OF DIGITAL BUSINESS

Čelik Petar

Abstract: *Digital transformation of business and cyber security have recently caused great interest, not only in business and political circles, but also among scientists and researchers. In recent years digital technology has dramatically changed, redesigned and accelerated the way of doing business, education, entertainment, public sector, and other segments of society. Configuration and scope of changes, along with inevitable disruption, take place at three levels: individual, organizational and social level. With its direct impact on the consciousness, ideas, behavior and change of paradigm, focus and the manner of business, digital transformation has undoubtedly led to the creation and expansion of digital economy, as a brand new and unknown model of business. With the development of new business models and modes of business, disruptive technologies have become a great challenge and a kind of threat to the digital business model itself in the complex global environment. This is due to the unlimited possibilities of abuse of technologies and their weaknesses. More precisely, there is an obvious imbalance between the very rapid development of technological innovations and their implementation, on the one hand, and accompanying protection and security challenges, on the other.*

Keywords: *digital transformation of busines / digital economy / disruptive innovations / digitization /cyber security*