INFORMATION PROTECTION STANDARDS AND SECURITY RISKS IN INFORMATION AND COMMUNICATION SYSTEMS: EXPERIENCES FROM THE REPUBLIC OF SERBIA

Nemanja Deretić
Belgrade business school, Higher education institution for applied studies – Belgrade, Republic of Serbia nemanja.deretic@bbs.edu.rs
Dejan Obućinski
Belgrade business school, Higher education institution for applied studies – Belgrade, Republic of Serbia dejan.obucinski@bbs.edu.rs

Abstract: In an area of development and implementation of computer systems, a growing problem is security and protection of information. Networked computer systems increase the vulnerability of business information systems. The consequences of unauthorized access to protected information may be financial, immaterial and combined. In the latest years, more and more business subjects apply information security management system as a part of its risk management strategy. Information security management system is composed of policies, procedures, guidelines and related resources and activities. With this system, the organization wants to protect its information property. In addition, this approach helps in establishment, implementation, execution, monitoring, reviewing, maintaining and improving information security organizations to achieve its business goals. The whole system of information security management is based on the evaluation of risks and levels of the risk acceptance by the organization. The aim of the design is effective treatment and risk management. This paper is aimed at managers and employees in the field of information technologies in companies' organizational units. In addition to that, this paper may be of interest to everyone involved in the process of programming and the design of data protection systems, and the implementation of data protection standards. The paper offers an overview of basic information about the legal regulations on data protection systems in the Republic of Serbia, the standards of electronic data interchange, and the basics of cyber crime. In addition, a section of the paper is concerned with the identification of risks and the definition of the need for information protection. At the end, a review has been given of the information security management system in organizations and of security techniques.
Keywords: data security, standards, information interchange, data management

STANDARDI ZAŠTITE PODATAKA I BEZBEDNOSNI RIZICI U INFORMACIONO-KOMUNIKACIONIM SISTEMIMA: ISKUSTVA IZ REPUBLIKE SRBIJE

Nemanja Deretić, M.Sc
Beogradska poslovna škola, Visoka škola strukovnih studija – Beograd, Republika Srbija
nemanja.deretic@bbs.edu.rs
Dejan Obućinski, M.Sc
Beogradska poslovna škola, Visoka škola strukovnih studija – Beograd, Republika Srbija
dejan.obucinski@bbs.edu.rs

Rezime: U razvoju i primeni računarskih sistema, sve veći problem postaje bezbednost i zaštita informacija. Umrežavanjem računarskih sistema povećava se ranjivost poslovnih informacionih sistema. Posledice neovlašćenog pristupa zaštićenim informacija mogu biti finansijske, nematerijalne i kombinovane. U zadnjih par godina, sve više poslovnih subjekata primenjuje sistem menadžmenta bezbednošću informacija kao deo svoje strategije upravljanja rizikom. Sistem menadžmenta bezbednošću informacija sastoji se od politika, procedura, smernica i sa njima povezanih resursa i aktivnosti. Pomoću ovog sistema, organizacija upravlja kako bi zaštitila svoju informacionu imovinu. Pored toga, navedeni pristup pomaže u uspostavljanju, primeni, izvođenju, praćenju, preispitivanju, održavanju i poboljšavanju bezbednosti informacija organizacije radi postizanja ciljeva poslovanja. Ceo sistem menadžmenta bezbednošću informacija je zasnovan na ocenjivanju rizika i nivoima prihvatanja rizika od strane organizacije. Cilj projektovanja je efektivno postupanje i upravljanje rizicima. Rad je namenjen rukovodiocima i zaposlenima iz oblasti informacionih tehnologija u organizacionim jedinicama

preduzeća. Pored toga, ovaj rad može biti interesantan i svima koji učestvuju u procesu programiranja i projektovanja sistema zaštite podataka i implementacije standarda u oblasti zaštite podataka. U radu je dat pregled osnovnih informacija o zakonskoj regulativi o sistemima zaštite podataka u Republici Srbiji, standardima elektronske razmene podataka i osnovama visokotehnološkog kriminala. Pored toga, poseban deo rada je posvećen identifikaciji rizika i definisanju potrebe zaštite informacija. Na kraju, dat je osvrt na sistem upravljanja bezbednošću informacija u organizacijama i tehnike bezbednosti.
Ključne reči: bezbednost podataka, standardi, razmena informacija, menadžment podataka

1. UVOD

U najširem smislu i najopštijem značenju, pod pojmom tajna se podrazumeva sve ono što je nepoznato. Prema dosadašnjem izučavanjima pojma tajna, moguće je razmatrati dve osnovne vrste tajni: apsolutnu (opštu) tajnu, koja je nepoznata svima i relativnu tajnu, koja predstavlja nepoznanicu samo za nekoga. Pojam tajne se može razmatrati sa sociološkog, filozofskog i krivično-pravnog aspekta.[181] U radu se razmatra pojam tajne sa aspekta zaštite informacija. Ovaj aspekt podrazumeva one podatke o činjenicama, sredstvima i postupcima za čije odavanje je predviđena krivična sankcija protiv učinioca takvog dela.

U današnjem društvu, postaje sve važnije razvijanje svesti o zaštiti informacija. Funkcionisanje državne uprave i raznih korporacija u velikoj meri zavisi od stepena razvijenosti računarske i komunikacione infrastrukture. Pored toga što zainteresovane strane razmenjuju različite informacije, sa druge strane izlažu svoje računarske sisteme raznovrsnim pretnjama. Postoje različite vrste mera, koje se odnose na zaštitu informacija. Prva vrsta su tehničke mere, u koje se mogu ubrojati korisnička imena, šifre pristupa, pravo pristupa, enkripcija, itd. U drugu vrstu spadaju administrativne mere: razni pravilnici, bezbednosne procedure, bezbednosne politike i slično. Treća vrsta je predstavljena sa fizičkim merama: fizička kontrola pristupa, zaštitne mere, radnici obezbeđenja, video nadzor, itd. Da bi računarski sistem bio zaštićen na odgovarajući način potrebno je primenjivati sve tri vrste mera.

Po pravilu, fizička i pravna lica vrše određenu privrednu, vanprivrednu ili stručnu delatnost. Njihov značaj je u tome što zadovoljavaju određene egzistencijalne i druge svakodnevne potrebe stanovništva. Pored toga što se preduzeća staraju o bezbednosti svoje imovine i svojih radnika, potrebno je da se staraju i o zaštiti tajnih podataka.

Bezbednosna kultura u primeni visokih tehnologija pre svega podrazumeva svest o tome da navedene tehnologije mogu imati i negativan uticaj na bezbednost društva, pojedinca, njegove imovine i životne sredine. Iz ovih razloga, neophodno je vršiti stalnu obuku i stručno usavršavanje radnika i predviđati krivičnu odgovornost za nestručan i nesavestan rad.[182]

Internet je jedan od najprovokativnijih sociooloških i psiholoških fenomena. Slobodno druženje i pretraživanje po online prostoru sa sobom vuče i ostavljanje tragova. Svaki korisnik daje podatke o sebi, a to najčešće radi svesno i nesvesno. Prvi način se dešava kada mu se postavlja uslov da bi mogao da pristupi traženim aplikacijama, kada svesno na to pristaje. Drugi način se dešava kada razmenjuje podatke sa drugim učesnicima mreže, nesvestan da mreža sve podatke skladišti, a da podaci ostaju deponovani čak i u slučaju kada uklone svoj profil.[183]

U domenu poslovanja preduzeća, pored materijalnih resursa i informacije se mogu smatrati vidom imovine, koje je potrebno zaštititi na odgovarajući način. Informacije moraju biti zaštićene od neovlašćenog pristupa, bez obzira na način kojim se čuvaju ili skladište. U pogledu zaštite informacija, postoje brojne pretnje sa kojima se susreću preduzeća. Pored kvarova na instalacijama usled požara, poplava ili vandalizma, sve veći udeo uzimaju i različite vrste špijunaže, sabotaže i računarskih prevara.

2. ZAKONSKA REGULATIVA U REPUBLICI SRBIJI

U procesu pridruživanja Evropskoj Uniji, od posebnog interesa je usklađivanje nacionalnog zakonodavstva sa pravnim tekovinama Evropske unije. Pored oblasti unapređenja ljudskih prava i jačanja pravne države, podrazumeva se i uređenje oblasti nacionalne bezbednosti i uspostavljanje jasno definisanih instrumenata zaštite nacionalnih interesa. Na taj način, neophodna reforma sektora bezbednosti podrazumeva i uspostavljanje i primenu jasnih mehanizama zaštite tajnih podataka od nacionalnog i kolektivnog značaja. Ova

[181]Stajić, Lj. (2005). Osnovi bezbednosti. Fakultet civilne odbrane. Izdavačka kuća "Draganić", p.320.
[182]Stajić, Lj., Mijaljković, S., Stanarević, S. (2005). Bezbednosna kultura, drugo izdanje. Izdavačka kuća "Draganić", p.133.
[183]Baltezarević, V., Baltezarević, R. (2015). Sloboda na internetu i njene posledice. Godišnjak Fakulteta za kulturu i medije: komunikacije, mediji, kultura, p.257.

oblast u Republici Srbiji zanemarena je duže od dve decenije.[184] Zakonska regulativa, koja se bavi sistemima zaštite podataka u Republici Srbiji, određena je sledećim zakonima: zakonom o slobodnom pristupu informacijama od javnog značaja, zakonom o zaštiti podataka o ličnosti i zakonom o tajnosti podataka. Kod domaćih ili stranih fizičkih i pravnih lica, zakonom o zaštiti poslovne tajne uređuje se pravna zaštita poslovne tajne od svih radnji nelojalne konkurencije.

Za potrebe ovog rada, posebno je značajan zakon o informacionoj bezbednosti, kojim se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

Rukovanje tajnim podacima u Republici Srbiji predviđeno je u uređenom sistemu. Sistem treba da bude realizovan u skladu sa pravnom regulativom i standardima iz oblasti zaštite tajnih podataka. Tako uređen i sertifikovan sistem, od strane akreditovanog organa, predstavlja registarski sistem i može da bude koncipiran u zavisnosti od potreba određenog organa. Registarski sistem može da bude koncipiran kao centralizovan (jedan Centralni registar, podregistri i tačke za obradu podataka) ili decentralizovan (više centralnih registara i podregistara i slično).[185] Nacionalni organ nadležan za zaštitu tajnih podataka, u Republici Srbiji, je Kancelarija Saveta za nacionalnu bezbednost, koja je osnovana je 16. novembra 2009. godine. Od 1. januara 2010. godine Zakonom o tajnosti podataka promenjen je naziv u Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.[186]

3. KORIŠĆENJE INFORMACIONO-KOMUNIKACIONIH TEHNOLOGIJA U REPUBLICI SRBIJI

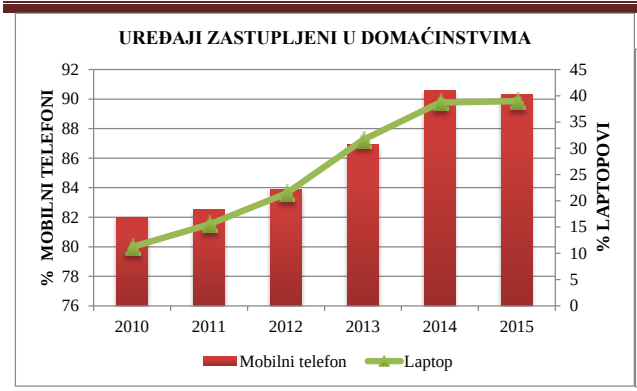
Prema metodologiji Republičkog zavoda za statistiku Republike Srbije (u daljem tekstu RZSRS), statistički podaci o korišćenju informaciono-komunikacionih tehnologija dobijaju se na osnovu rezultata istraživanja o upotrebi:

1. informaciono-komunikacionih tehnologija u domaćinstvima i pojedinačno i
2. informaciono-komunikacionih tehnologija u privrednim društvima i finansijskim institucijama.

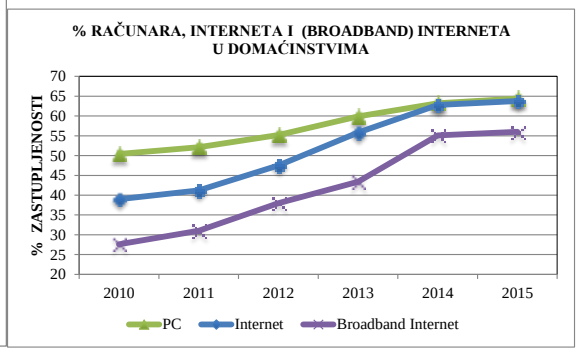
Kod prikupljanja podataka o domaćinstvima i pojedinačnim licima, istraživanje se sprovodi jednom u godini dana, a obavlja se putem telefona. Veličina uzorka u oba slučaja iznosi 2400, odnosno 2400 domaćinstava i 2400 pojedinaca. U izveštajima RZSRS, posebno su prikazani podaci za region Beograda, Vojvodine, Šumadije i Zapadne Srbije i Južne i Istočne Srbije. Jedino nisu prikazani podaci za region Kosovo i Metohija. Kod prikupljanja podataka o privrednim društvima, prethodno je uzorak podeljen po kriterijumima veličina i delatnost. Veličina uzorka iznosi 1400 privrednih subjekata, a istraživanje se takođe sprovodi telefonskim putem.

Kod istraživanja domaćinstava, pojedinačnih lica i privrednih društava, korišćena je metodologija Eurostat[187]. Prema ovoj metodologiji, istražuju se domaćinstva sa najmanje jednim članom koji ima između 16 i 74 godine života, a takođe isti standard važi i za pojedinačna lica. Kod privrednih društava, istražuju se ona koja imaju 10 i više zaposlenih lica iz narednih delatnosti: prerađivačka industrija; građevinarstvo; trgovina na veliko i malo, popravka motornih vozila; hoteli, kampovi i drugi smeštaj za kraći boravak; saobraćaj, skladištenje i veze; poslovi u vezi s nekretninama, iznajmljivanje i poslovne aktivnosti; kinematografske i video aktivnosti, radio i TV aktivnosti. Procenat zastupljenosti uređaja (Slika 1a) i pristupa internetu (Slika 1b) u domaćinstvima Republike Srbije su dati u narednom delu.

[184]Terzić, K., Župac, G. (2015). Značaj normiranja industrijske bezbednosti u Republici Srbiji u postupku usklađivanja sa Odlukom saveta 2013/488/EU. Vojno delo, 67(3), p.178.
[185] Kovačević, N., (2012). Zaštita tajnih podataka, p.3.
[186] Stamenković, B. (2015). Sertifikacija pravnih lica za rad sa tajnim podacima, zakonski okvir , p.4.
[187] http://ec.europa.eu/eurostat



Slika 1a. % zastupljenosti mobilnih telefona i laptopova u domaćistvima

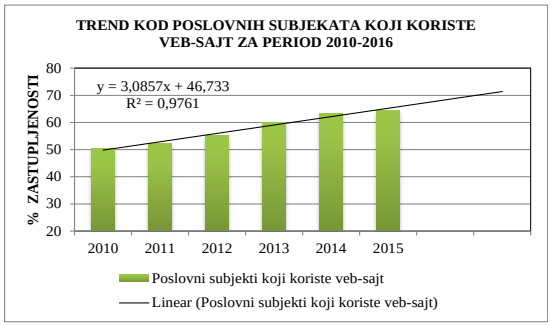


Slika 1b. % korišćenja računara, interneta i širokopojasnog (broadband) interneta u domaćistvima

Izvor podataka: RZSRS, Statistički godišnjak Republike Srbije – Informacione tehnologije, 2016, pp. 5-6.

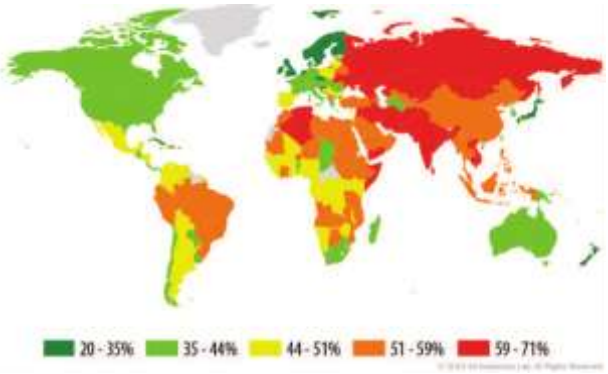
Povećanje procenta korišćenja laptopova prati porast korišćenja mobilnih telefona. U istraživanom periodu raste i korišćenje interneta i širokopojasnog interneta. U periodu od 2010. do 2016. godine prisutan je visok udeo korišćenja računara i interneta u poslovanju poslovnih subjekata, koji su imali internet priključak. Na nivou statističke greške se mogu naći poslovni subjekti koji ne koriste računar ili internet, a imaju internet priključak. Na slici 2 je dat trend u korišćenju veb-sajta za poslovne subjekte za analizirani period od 2010-2016 godine. U posmatranom periodu, korišćenje veb-sajta od strane poslovnih subjekata se povećavalo prosečno za 3,0857 % na godišnjem nivou, a koeficijent determinacije iznosi 97,61%.

Prema izveštaju Kaspersky security bulletin, države iz celog sveta su svrstane u tri kategorije: 1. države sa maksimalnim rizikom (iznad 60%, 22 države), 2. države sa visokim rizikom (41-60%, 98 država) i 3. države sa srednjim rizikom (21-40,99%, 45 država). Republika Srbija je svrstana u drugu grupu zemalja, sa izračunatim nivoom rizika od 50,1% po korisnike personalnih računara.



Slika 2. Trend kod poslovnih subjekata koji koriste veb-sajt za period 2010-2016

Izvor podataka: RZSRS, Statistički godišnjak Republike Srbije – Informacione tehnologije, 2016, p. 8.



Slika 3. Nivo rizika sa kojim se susreću korisnici personalnih računara po državama

Izvor: Kaspersky security bulletin, #KLReport, 2015, p. 69.

4. STANDARDI ELEKTRONSKE RAZMENE DOKUMENATA

Međunarodni standard za razmenu poslovnih dokumenata u digitalnom obliku je EDI[188] (Electronic Data Interchange) i odnosi se na standard za komunikaciju između informacionih sistema. Primenom ovog standarda, uklanja se potreba za ponovnim prekucavanjem dokumenta, slanjem poštom ili putem faksa. Samim tim, eliminišu se problemi i smanjuju se troškovi. Jedan od primera poboljšanja poslovanja je kada jedan poslovni subjekat napravi porudžbinu za drugog poslovnog subjekta, onda se ista porudžbina pojavljuje i u sistemu drugog poslovnog subjekta. Naravno, neophodan preduslov je da poseduju EDI standard. Kompajler (Compiler) za EDI standard koji se najviše koristi je EDIFACT. EDIFACT podržava različite dokumente koji se razmenjuju

[188] http://www.edibasics.com/what-is-edi/

u poslovnoj komunikaciji (porudžbine, otpremnice, cenovnike, izveštaje, itd.) Prema kompaniji Eightbit[189] postoji pet osnovnih prednosti upotrebe EDI standarda u razmeni dokumenata:
1. Maksimalna tačnost između poslatih i primljenih podataka, što isključuje faktor ljudske greške pri prekucavanju;
2. Brzina slanja i prihvata podataka je drastično ubrzana u odnosu na manuelni unos podataka;
3. Uštede u poslovanju (vreme, radna snaga, potrošni materijal);
4. Povećana produktivnost;
5. Unapređeno upravljanje logistikom.

5. SISTEM UPRAVLJANJA BEZBEDNOŠĆU INFORMACIJA U ORGANIZACIJAMA

Svesni činjenica i odlika sadašnjice da se u najvećoj meri koriste informacione tehnologije koje su, prepune rizika po bezbednost informacija, zaključena je i definisana potreba njihove zaštite. Proširenje poslovne politike po tom pitanju oslanja se na sistem organizacionog menadžmenta. Naime, rizik po bezbednost informacija je izražen u toj meri da je ugrožena kako lična, tako i poslovna bezbednost, što znači da nije samo ugrožena konkurentnost preduzeća, već i sama egzistencija. Odgovor na prethodno navedenu pretnju predstavlja prevashodno prihvatanje postojanja rizika, zatim, identifikacija rizika, definisanje potrebe zaštite informacija i na kraju menadžment rizicima. Ova lista aktivnosti čini većinu procesa implementacije zaštite informacija. Rezultat navedenih činjenica je bilo definisanje sistema menadžmenta bezbednošću informacija ISMS (Information Security Management System). Međunarodna organizacija za standardizaciju ISO[190] (International Organization for Standardization) je taj, može se reći, primarni problem održivog poslovanja preduzeća, rasta i razvoja, uzela u obzir definišući standarde. Navedene standarde čini sledeća serija:
- ISO/IEC 27000 (Information technology - Security techniques - Information security management systems - Overview and Vocabulary) predstavlja pregled i rečnik pojmova;
- ISO/IEC 27001 (Information security management – Requirements) predstavlja definisane zahteve standarda;
- ISO/IEC 27002 (Code of practice for information security controls) predstavlja pravila prakse za kontrolu bezbednosti informacija;
- ISO/IEC 27003 (Information security management – guidance) predstavlja smernice za implementaciju;
- ISO/IEC 27004 (Information security management– Monitoring, measurement, analysis and evaluation) odnosi se na merenja;
- ISO/IEC 27005 (Information technology - Security techniques - Information security risk management) odnosi se na upravljanje rizikom;
- ISO/IEC 27006 (Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems) obuhvata zahteve za tela koja obavljaju proveru i sertifikaciju;
- ISO/IEC 27007 (Information technology - Security techniques - Guidelines for information security management systems auditing) predstavlja uputstvo za interne i eksterne provere.

Pored navedenih, postoje i sledeći standardi od kojih je jedan povučen.
- ISO/IEC 27011 (Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations) predstavlja zahteve za sektor telekomunikacija.
- ISO/IEC 27012, standard koji je bio predložen, ali kasnije i povučen zbog nedostatka interesa.
- ISO/IEC 27013 (Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1).
- ISO/IEC 27014 (Information technology - Security techniques - Governance of information security).
- ISO/IEC TR 27016 (Information technology - Security techniques - Information security management - Organizational economics).
- ISO/IEC TR 27019:2013 (Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry).
- ISO 27799 (Health informatics - Information security management in health using ISO/IEC 27002).

Sa druge strane, da je shvaćena ozbiljnost ovakve tematike, govori činjenica preuzimanja i objavljivanja dela standarda od strane Republike Srbije, konkretno Instituta za standardizaciju[191] koji je u međuvremenu

[189] http://www.8bit.rs/edi
[190] http://www.iso.org/iso/home.html
[191] http://www.iss.rs/

postao punopravni član evropskih organizacija za standardizaciju CEN[192] (European Committee for Standardization) i CENELEC[193] (European Committee for Electrotechnical Standardization). Preuzeti standardi su dati u tabeli 1.

ISO 27001 je takođe kompatibilan sa standardom ISO 22301:2012 (u Srbiji zvanično SRPS ISO 22301:2014 - Društvena bezbednost - Sistemi menadžmenta kontinuitetom poslovanja - Zahtevi). Ovaj standard se odnosi na identifikaciju potencijalnih pretnji po sistem i koji kroz uspostavljen sistem upravljanja kontinuitetom poslovanja ima za cilj zaštitu preduzeća od potencijalnih pretnji, smanji verovatnoću prekida poslovanja, pripremi za adekvatno reagovanje ukoliko do toga dođe i obezbedi odgovarajuće planove oporavka. Incidenti koji su obuhvaćeni mogu biti u rangu od iznenadnog prekida IT (Information technology) sistema do prirodnih katastrofa i terorističkih napada.[194]

Tabela 1. Spisak preuzetih standarda Instituta za standardizaciju Republike Srbije

R.br.	**Standardi serije SRPS ISO/IEC 27000**	**Naslov:** Informacione tehnologije
1.	SRPS ISO IEC 27000:2014	Tehnike bezbednosti - Sistemi menadžmenta bezbednošću informacija - Pregled i rečnik
2.	SRPS ISO IEC 27001:2014	Tehnike bezbednosti - Sistemi menadžmenta bezbednošću informacija - Zahtevi
3.	SRPS ISO IEC 27005:2013	Tehnike bezbednosti - Menadžment rizicima po bezbednost informacija
4.	SRPS ISO IEC 27013:2015	Tehnike bezbednosti - Smernice za integrisanu primenu ISO/IEC 27001 i ISO/IEC 20000-1
5.	SRPS ISO IEC 27014:2015	Tehnike bezbednosti - Upravljanje bezbednošću informacija
6.	SRPS ISO IEC 27032:2015	Tehnike bezbednosti - Smernice za sajber bezbednost

Da je moguća povreda privatnosti, odnosno da je javno i eksplicitno pokazan rizik narušavanja bezbednosti informacija, kao i ličnosti na nivou nacije, govori podatak iz 2014. godine, kada se zaključilo da je na sajtu Agencije za privatizaciju Republike Srbije dugi period bio dostupan dokument koji je sadržao lične podatke o 5.190.396 građana Srbije. U tom dokumentu nalazila su se imena i prezimena građana i što je najgore njihov jedinstveni matični broj (JMBG). Ipak nije potvrđeno da su ti podaci nedozvoljeno obrađivani, ali je međutim evidentno da da su bile i da još uvek jesu moguće pravne i ostale zloupotrebe.

6. ZAKLJUČAK

Poverljivost, raspoloživost i integritet predstavljaju tri najvažnija pojma u oblasti bezbednosti informacija. Upravljanje merama bezbednosti na osnovu definisanih standarda osigurava održivost poslovnog uspeha i svodi moguće incidente na najmanju meru. Bezbednost informacija se postiže putem primenljivog skupa kontrola, koje su izabrane kroz proces menadžmenta odabranim rizikom i kojima se upravlja korišćenjem ISMS-a.

Da bi se na pravi način zaštitio informaciono-komunikacioni sistem potrebno je definisati potrebne politike, procese, procedure, organizacione strukture i na odgovarajući način koristiti sofver i hardver. Ove kontrole treba definisati, primeniti, pratiti, preispitivati i poboljšavati onda kada je to neophodno da bi se organizaciji osiguralo ispunjavanje specifičnosti bezbednosti informacija i poslovnih ciljeva. Očekuje se da relevantne kontrole bezbednosti informacija budu potpuno integrisane u poslovne procese organizacije.

LITERATURA

Stajić, Lj., Osnovi bezbednosti, Fakultet civilne odbrane, Izdavačka kuća "Draganić", 2005.

Stajić, Lj., Mijaljković, S., Stanarević, S., Bezbednosna kultura, drugo izdanje, Izdavačka kuća "Draganić", 2005.

Baltezarević, V., Baltezarević, R., Sloboda na internetu i njene posledice, Godišnjak Fakulteta za kulturu i medije: komunikacije, mediji, kultura, vol. 7, pp. 257-272, 2015.

[192] https://www.cen.eu/Pages/default.aspx
[193] https://www.cenelec.eu/
[194] http://www.kvalitet.org.rs/standardi/iso-27001-i-iso-22301

Terzić, K., Župac, G., Značaj normiranja industrijske bezbednosti u Republici Srbiji u postupku usklađivanja sa Odlukom saveta 2013/488/EU, Vojno delo, vol. 67(3), pp. 178-191, 2015.

Zakon o tajnosti podataka. Službeni glasnik Republike Srbije broj 104/2009.

Zakon o zaštiti poslovne tajne. Službeni glasnik Republike Srbije broj 72/2011.

Zakon o slobodnom pristupu informacijama od javnog značaja. Službeni glasnik Republike Srbije broj 120/2004, 54/2007, 104/2009 i 36/2010.

Zakon o zaštiti podataka o ličnosti. Službeni glasnik Republike Srbije broj 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012.

Zakon o informacionoj bezbednosti. Službeni glasnik Republike Srbije broj 6/2016.

Kovačević, N., Zaštita tajnih podataka, Sedmi stručni skup "ARHIV INFO 2012", Primena informacionih tehnologija u oblasti e-poslovanja, arhiviranja i upravljanja dokumentima i podacima, aktuelni trendovi, 2012. Dostupno na: http://www.arhivinfo.org.rs/radovi-2012/radovi/Zastita%20tajnih%20podataka.pdf [05.11.2016]

Stamenković, B. Sertifikacija pravnih lica za rad sa tajnim podacima -zakonski okvir-, 2015. Dostupno na: http://www.pks.rs/SADRZAJ/Files/Centar%20za%20edukaciju/1_%20ZAKONSKI%20OKVIR%20PKS%20-%20%20privreda.pdf. [05.11.2016]

Republički zavod za statistiku, Statistički godišnjak Republike Srbije – Informacione tehnologije, 2016. Dostupno na: webrzs.stat.gov.rs/WebSite/repository/documents/00/02/29/10/17_Informacione_tehnologije.pdf [15.11.2016]

Republički zavod za statistiku, Upotreba informaciono- komunikacionih tehnologija u Republici Srbiji, 2016. - knjiga. Dostupno na: webrzs.stat.gov.rs/WebSite/repository/documents/00/02/25/89/ICT2016s.pdf [15.11.2016]

Kaspersky security bulletin, #KLReport, 2015. Dostupno na: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. [10.11.2016]

SAGA New frontier group, EDI – Elektronska razmena podataka u vašoj firmi. http://www.saga.rs/fileadmin/Content/saga.rs/ECOD_EDI_Elektronska_razmena_podataka_u_firmi_srp.pdf [10.11.2016]

SRPS ISO IEC 27000:2014, Informacione tehnologije - Tehnike bezbednosti - Sistemi menadžmenta bezbednošću informacija - Pregled i rečnik.