*Bjelajac Đ. Željko*[*]
*Vesić Lj. Slavimir*[**]

**UDK: 004.056:007**
Pregledni rad
DOI 10.5937/ptp2002063B
Primljen: 20.03.2020.
Odobren: 06.04.2020.
Strana: 63–76

# BEZBEDNOST INFORMACIONIH SISTEMA

**REZIME:** U savremenim uslovima poslovanja organizacije ostvaruju svoje misije, vizije i ciljeve upotrebom informacionih sistema. Oni im omogućavaju razmenu podataka, informacija i znanja sa promenljivim okruženjem, nesmetano obavljanje dnevnih aktivnosti, kao i stvaranje osnove za donošenje strateških odluka. Kako se novi modaliteti ugrožavanja bezbednosti informacionih sistema pojavljuju usled promenljivog nebezbednog okruženja i pretnji koje vrebaju iz sajber prostora, potrebno je obratiti pažnju na iste i adekvatno reagovati, pošto nije više u pitanju samo ranjivost informatičko-komunikacione infrastrukture i informacija, već i ljudskog života. U samoj bezbednosti informacionih sistema, pored tehnički mera zaštite koje se sprovode u skladu sa definisanom politikom bezbednosti, potrebno je obratiti pažnju i na ljudski faktor i svest o bezbednosti, kao najslabiju kariku i delovati kako bi se pretnje svele na najmanju moguću meru.

***Ključne reči:*** *informacioni sistemi, bezbednost, sajber bezbednost, ljudski faktor*

[*] Prof. dr, Pravni fakultet za privredu i pravosuđe, Univerzitet Privredna akademija u Novom Sadu, e-mail: zdjbjelajac@gmail.com
[**] Doktorand, Fakultet za ekonomiju i inženjerski menadžment, Univerziteta Privredna akademija u Novom Sadu, e-mail: vesic.slavimir.@gmail.com

## Uvod

Savremeno poslovno okruženje u kojem organizacije ostvaruju svoje ciljeve, odlikuje se velikim brojem interakcija među učesnicima. Glavni faktori okruženja koji utiču na organizaciju mogu se grupisati u tri međusobno povezane celine:[1] specifično okruženje koga čine odnosi sa zaposlenim, trenutnim i budućim, odnosi sa kupcima i dobavljačima, kao i konkurencija, opšte okruženje kojeg čine ekonomski faktori, tehnologija, pravni okvir i javno mnjenje i fizičko okruženje koga čine lokacija i vreme.

Informacioni sistemi kao modeli stvarnih sistema imaju za cilj da sa takvim okruženjem omoguće organizaciji da održi veze putem razmene podataka, informacija i znanja, uz nesmetano obavljanje dnevnih operacija, kao i da omoguće dovoljno dobru osnovu za donošenje strateških odluka. Samo okruženje u kojem organizacija ostvaruje pomenute interakcije je nebezbedno, a pri tome postoje i mogućnosti internih pretnji, a sve to zajedno dovodi do toga da se problem bezbednosti jedne organizacije projektuje i na njen model, tj. informacioni sistem. Zbog toga je i potrebno sprovesti odgovarajući pristup po pitanju bezbednosti informacionog sistema organizacije, i time stvoriti mogućnost za ostvarenje njene misije, vizije i ciljeva. Takođe, potrebno je reći da taj proces nije jednokratan, već se kontinuirano odvija iz razloga što mnogi ranije pomenuti elementi okruženja organizacije, a time i njenog informacionog sistema se neprekidno menjaju, pa time i dinamika i nivoi pretnji kojim su izloženi.

Računarski zasnovan informacioni sistem čine hardver, softver, baze podataka, mreže, ljudi i procedure, podešeni za skupljanje, manipulisanje, skladištenje i procesiranje podataka u informacije.[2] Svi ovi elementi informacionog sistema imaju svoje ranjivosti pa je potrebno na sistematičan način pristupiti njihovoj zaštiti i prema pristupu grupe autora definisati zahteve u pogledu informacione sigurnosti, koja se može razmotriti sa tri aspekta: sigurnosni napad, sigurnosni mehanizam i sigurnosna usluga.[3]

Sa napretkom tehnologije i potrebe za sve većom efikasnošću, umrežavanjem i interakcijom sa okolinom određeni sistemi, su prevazišli granice pojedinačnog sistema i ukrupnjavaju se u veće sisteme što dovodi do toga da imamo značajno drugačije interne i eksterne odnose u tom novom tzv. sistemu

[1] Bocij, P., Greasley, A., Hickie, S. (2015). Business Information Systems, 5th ed, Pearson, p. 17.
[2] Stair, R., Reynolds, G. (2017). Principles of Information Systems, Cengage Learning, p. 6.
[3] Pleskonjić, D. et al., (2006). Sigurnost računarskih mreža. Beograd, Viša elektrotehnička škola u Beogradu, str. 2.

sistema (*engl. System of Systems, SOS*). Prema ISO/IEC/IEEE 21839:2019 sistem sistema je skup sistema ili sistemskih elemenata koji međusobno interaguju da bi obezbedili jedinstvenu sposobnost, koju ni jedan od sistema koji ga čini ne može samostalno da izvrši.[4] Sastavni sistemi mogu biti deo jednog ili više SOS, gde je svaki od njih sistem za sebe sa svojim razvojem, ciljevima, resursima i upravljanjem, a pri tome i sarađuje da bi omogućio jedinstvene sposobnosti SOS. Oni su deo današnje Industrije 4.0 oličene u velikom broju sajber-fizičkih sistema (*engl. cyber-physical systems*) i internetu stvari (*engl. Internet of things, IoT*). Obzirom da su pomenuti sistemi i tehnologije često deo kritične infrastrukture, jasno je da se bezbednost informacionih sistema značajno menja, proširuje i komplikuje u skladu sa pomenutim napretkom i da se ona prostire od nivoa pojedinca do zajednice i države.

## Definisanje pojma bezbednosti informacionih sistema

Pojam bezbednosti informacionih sistema, nije jednostavno jednoznačno definisati, prvenstveno zbog mnogih višestrukih odnosa između bezbednosti i njemu sličnih pojmova, kao i sve većoj složenošću promenljivog okruženja u kojem jedan informacioni sistem organizacije deluje. U različitim jezicima koristi se jedan ili više različitih pojmova za bezbednost. Tako npr. Đukić[5] navodi da se u engleskom jeziku koriste pojmovi: *security* i *safety*. *Security* se više upotrebljava u kontekstima vezanim za nacionalnu bezbednost (*engl. national security*), dok je *safety* „sposobnost delovanja kako ne bi došlo do nepoželjne situacije“. Na osnovu sprovedene sematičko-leksikografske analize, Ilić[6] zaključuje da se bezbednost u srpskom jeziku upotrebljava da označi stanje nekog subjekta (pojedinca, grupe ljudi, zajednice, institucije) koje je obeleženo odsustvom nevolja, briga, nesreća, opasnosti i drugih zala i da je njemu najsličniji pojam sigurnosti, ali da nije potpun sinonim.

U kontekstu sigurnosti računarskih mreža, Pleskonjić[7] i ostali ukazuju da je bezbednost apstraktan model, dok je sigurnost aktuelna implementacija. Pri tome, siguran sistem korespondira modelu koji je bezbedan u odnosu na sva prava, ali model bezbedan u odnosu na sva prava ne garantuje siguran sistem.

[4] Henshaw, M., Dahmann, J., Lawson, B. (2019). Systems of Systems (SoS). Preuzeto sa: https://www.sebokwiki.org/wiki/Systems_of_Systems_(SoS).

[5] Đukić, S. (2017). Osnove i sistem bezbednosti u strategiji nacionalne bezbednosti. *Vojno delo, 69* (7), str. 105.

[6] Ilić, P. (2011). Semantičko-leksikografski aspekti pojma bezbednosti. *Vojno delo, 63* (3), 85-99.

[7] Pleskonjić, D. et al., op. cit. str. 29.

Prema Bourgeois[8] fundamentalni koncepti bezbednosti informacionih sistema su vezani za informacionu bezbednost[9] (*engl. information security*), koja je opisana preko tri karakteristike: poverljivost (*engl. confidentiality),* integritet (*engl. integrity*) i rapoloživost (*engl. availability*) koje se nazivaju „trougao" ili „trojstvo" ili „trijada" sigurnosti. Prilikom zaštite informacije, želimo da ograničimo pristup onima kojima je dozvoljeno da informaciju vide, a svima ostalima da onemogućimo njen sadržaj i to je suštuna poverljivosti. Integritet osigurava da informacija stvarno predstavlja njeno nameravano značenje i da nije izmenjena, slučajno ili namerno. Raspoloživost označava da se informaciji može pristupiti i da se ona može izmeniti od strane bilo koga koji je autorizovan da to uradi u odgovarajućem vremenskom okviru.

U cilju da jasno definiše pojam sajber bezbednosti, von Solms[10] ukazuje na razlike koje postoje u pojmovima informacione bezbednosti (*engl. information security*), bezbednosti informacionih i komunikacionih tehnologija (*engl. information and communication technology security*), skraćeno ICT bezbednost i sajber bezbednosti (*engl. cyber security*). Prema međunarodnom standardu ISO/IEC 27002, informaciona bezbednost je opisana preko tri pomenute karakteristike, označene kao „trojstvo", bez obzira koju formu ta informacija uzima: papir, elektronski oblik, pošta, film, razgovor itd. Kod ICT sistema bezbednost informacije se ne može posmatrati izolovano od resursa i procesa sa kojima se ona suočava. ICT bezbednost, prema standardu ISO/IEC 13335-1[11], pojmove poverljivosti, integriteta i raspoloživosti proširuje neporicanjem, odgovornošću, autentičnošću i pouzdanošću, a svi zajedno zajedno čine bezbednosne usluge, tj. servise. Neporicanje (*engl. non-repudation*) je sposobnost da se dokaže radnja ili događaj koji su se dogodili, tako da ova radnja ili događaj kasnije ne mogu da budu odbačeni. Odgovornost (*engl. accountability*) je svojstvo koje osigurava da se radnje entiteta mogu jedinstveno pratiti u odnosu na entitet. Autentičnost (*engl. authenticity*) je svojstvo koje osigurava da je identitet subjekta ili resursa onaj koji tvrdi da jeste. Odnosi se na korisnike, procese, sisteme i informacije. Pouzdanost (*engl. reliability*) je svojstvo konzistentnog nameravanog ponašanja i rezultata.

Sajber bezbednost uključuje i pretnje koje nisu deo formalnog definisanog obima druge dve vrste bezbednosti. Neki od tih scenarija su sajber

[8] Bourgeois, D. (2014). Information Systems for Business and Beyond, Saylor Foundation, pp.64-65.

[9] Koristi se i termin InfoSec.

[10] Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. 38, 97-102.

[11] ISO/IEC. (2004). International standard 13335-1. Preuzeto sa: https://www.sis.se/api/document/preview/905483/

maltretiranje[12] (*engl. cyber bullying*) koje prouzrokuje sramotu, uznemiravanje i nasilje nanoseći psihološku štetu. Tu ne dolazi do gubitka poverljivosti, integriteta ili dostupnosti informacija, već je rezultat direktna šteta učinjena osobi koja se maltretira. Još jedan primer je sajber terorizam (*engl. cyber terrorism)*, gde gubitak ne podrazumeva samo integritet ili dostupnost informacionih resursa, već i pristup takvim kritičnim servisima. Iz pomenutih primera naglašava se specifičnost i razlika pojma sajber bezbednosti u odnosu na njemu slične pojmove i zbog rizika koji dolazi iz sajber prostora potrebno je štititi i interese osoba, društva i nacije, uključujući i njihove sredstva koja nisu deo informatičke osnove. Odnosi između pomenutih pojmova se mogu prikazati u tabeli 1.

**Tabela 1.** Odnos vrsta bezbednosti

| | Pretnje | Ranjivosti | Sredstva (vrednosti) |
|---|---|---|---|
| Informaciona bezbednost | Razne | ICT itd. | Informacije |
| Bezbednost informaciono komunikacionih tehnologija | Razne | Razne | ICT |
| Sajber bezbednost | Razne | ICT, Informacije itd. | Ljudi i njihovi interesi |

Dakle, sajber bezbednost se može definisati kao zaštita samog sajber prostora, elektronskih informacija, ICT-a koji podržava prostor i korisnika sajber prostora u njihovom ličnom, društvenom i nacionalnom kapacitetu, uključujući bilo koji njihov interes, merljiv ili nemerljiv, koji je ranjiv u odnosi na napade potekle iz sajber prostora.[13]

## Tehnike zaštite

U ostvarenju poverljivosti, integriteta i raspoloživosti, sprovode se tehnike ili mere zaštite, koje su potrebne da bi umanjile ranjivost sistema ili da ga svedu na privatljivu meru sa jedne strane, a sa druge je potrebno da budu osmišljene na način da ne utiču negativno na produktivnosti. Pored toga, potrebno je imati u vidu da je komunikacija unutar računarskih mreža složen problem, i da bi se efikasno rešio potrebno bilo je primeniti princip apstrakcije. Kontrolisano uvođenje složenosti dovelo je do toga da imamo višeslojne referentne modele mrežne komunikacije koji se danas koriste, pri čemu su

[12] Kod nas se upotrebljava i pojam digitalno nasilje.
[13] Von Solms, R., Van Niekerk, J., op. cit. p. 101.

najpoznatiji ISO/OSI model i TCP/IP model. Pomenuti modeli imaju arhitekturu organizovanu u slojevima (*engl. layers*), gde se svaki sloj može posmatrati kao usluga (*engl. service*) koja se nudi sloju iznad sebe. Na svakom sloju postoje komunikacioni protokoli putem kojih se definiše format i redosled poruka, razmenjenih između najmanje dve strane koje učestvuju u komunikaciji, kao i postupci koji se preduzimaju posle slanja i/ili prijema poruka ili nekog drugog događaja.[14] Način na koji funkcionišu komunikacioni protokoli i računarske mreže, pa time i internet, daje mogućnosti zlonamernim akterima da naruše poverljivost, integritet i raspoloživost, upotrebom opštepoznatih mehanizama samih računarskih mreža. Dakle, tehnologija koliko sa jedne strane daje mogućnosti, sa druge donosi pretnje i rizike koje je potrebno sagledati i adekvatno upravljati njima.

Napadači koriste mnogo različitih metoda i alata, često i u kombinaciji, da bi kompromitovali poverljivost.[15] Opisaćemo neke od njih. Jedan od alata, koji je široko u upotrebi je softver za hvatanje i analizu mrežnih paketa (*engl. packet sniffer*) putem kojeg se komunikacija preseca i snima, a nakon toga se vrši analiza sadržaja paketa. Ukoliko postoji neki osetljiv sadržaj, lozinka ili broj kartice prikazan u obliku čistog teksta on se može pročitati. Suština napada na šifru (*engl. password attacks*) jeste da se dobije pristup sistemu, putem nekog naloga. Napad putem rečnika (*engl. dictionary attack)* je vrsta napada gde napadač pokušava da pogodi šifru upotrebom reči iz rečnika ili često korišćenih i poznatih šifri. Pored toga napadač može da pokuša da pogodi šifru sprovodeći svaku moguću kombinaciju, što je poznato kao napad sirovom snagom (*engl. brute-force attack)*. Skeniranje portova (*engl. port scanning*) je tehnika koja se koristi da bi se utvrdilo koji su portovi otvoreni na računaru, pri čemu se za popularne protokole obično zna koje portove koriste. Uobičajeno se koristi da se utvrdi da se sazna nešto o konfiguraciji sistema, potencijalne slabe tačke i da li postoji neki sigurnosni mehanizmi koji kontrolišu mrežni saobraćaj, kao npr. mrežne barijere (*engl. firewalls*). *Phishing* napad je forma napada gde se najčešće putem elektronske pošte, prosleđuje email korisniku koji svojim izgledom i sadržinom veoma podseća na email njemu važnog pošiljaoca, npr. banke, koji navodi primaoca na odavanje poverljivih informacija kao što je broj kartice ili lozinke. *Phishing* je jedna od formi socijalnog inženjeringa (*engl. social engineering*) kao vida psihološke

[14] Kurose, J., Ross, K. (2009). Umrežavanje računara: Od vrha ka dnu (4. izd.). Računarski fakultet, str. 9.

[15] Types of Network Attacks against Confidentiality, Integrity and Avilability. Preuzeto sa: https://www.omnisecu.com/ccna-security/types-of-network-attacks.php.

manipulacije koja se koristi da obmane korisnike u cilju odavanja poverljivih informacija.

Neke od mera koje se mogu primeniti u obezbeđivanju poverljivosti su pre svega, adekvatno upravljanje korisničkim nalozima i lozinkama. Pored toga, jedan od bitnih procesa je autentifikacija (*engl. authentication*) u kome korisnik dokazuje da je ono za šta se predstavlja. Kada korisnik pokušava da pristupi sistemu, sprovodi se utvrđivanje njegovog identiteta. Pored toga, sprovodi se i proces autorizacije (*engl. authorization*) kojom se određuje da li korisnik ima pravo da pristupi određenom resursu. Autorizacija se sprovodi nakon procesa autentifikacije i određuje čemu korisnik može ili ne može da pristupi. Elementi koji određuju način ka koji će biti sprovedena autentifikacija se nazivaju autentifikacioni faktori. Uobičajeno jeste da se oni klasifikuju u odnosu na to da: korisnik nešto zna (kao što su npr. lozinka, PIN, odgovor na pitanje itd.), korisnik nešto ima (kao što su npr. kartica, token, mobilni telefon itd.) i korisnik nešto jeste (kao što su npr. otisak prsta, rožnjača oka, glas, obrazac hodanja itd.). U cilju poboljšanja poverljivosti preporučuje se najmanje dvofaktorska autentifikacija, npr. ako posedujete karticu, potrebno je da znate PIN. Jedan od važnih koncepata koji se primenjuje jeste tehnika šifrovanja (*engl. encryption).* Otvoreni tekst (*engl. plain text)* putem šifrovanja postaje tekst sa prikrivenim sadržajem, tzv. šifrat (*engl. ciphertext*). Dešifrovanje (*engl. decryption*) je obrnuti proces od šifrovanja, gde se od šifrata dobija izvorni otvoren tekst. Svi pomenuti koncepti su deo kriptografije (*engl. cryptography*) - nauke i umetnosti čuvanja bezbednosti poruka.[16] Kriptografski algoritam (*engl. cryptographic algorithm*) je matematička funkcija koja se koristi za šifrovanje i dešifrovanje. Obzirom da postoje ograničenja kada su kriptografski algoritmi zasnovani na tajnosti načina na koji algoritam radi, savremena kriptografija je to prevazišla uvodeći koncept ključa (*engl. key*). Prilikom šifrovanja i dešifrovanja koriste se ključevi, a sama sigurnost algoritma se zasniva na ključevima, a ne na algoritmu koji je javno poznat. Dakle, Kerkohovo pravilo da se tajnost u celosti mora biti zasnovano na ključu, se primenjuje, a koncept držanja algoritma u tajnosti (*engl. security by obscurity*) nikada ne dovodi do rezultata. Osnovna dva tipa algoritma su: simetrični algoritmi - gde se jedan ključ koristi i za šifrovanje i za dešifrovanje i asimetrični algoritmi - koji imaju dva ključa, gde se jedan koristi za šifrovanje i naziva se javni ključ (*engl. public key*), dok se drugi koristi za dešifrovanje i naziva se tajni ključ (*engl. private key*). Neki simetrični kriptogrfski algoritmi su: AES, Triple-DES itd. Primeri asimetričnih kriptografskih algoritama su:

[16] Šnajer, B. (2007). Primenjena kriptografija, prevod drugog izdanja. Beograd, Mikro knjiga. str. 1-3.

RSA, DSA itd. Asimetrični algoritmi se primenjuju u infrastrukturi javnih ključeva (*engl. public key infrastructure*), čime se obezbeđuje kriptovanje na Web-u primenom TLS (*engl. transport layer security*) protokola i ostvaruje sigurnija komunikacija. Pored toga, oni se koriste i u obezbeđivanju digitalnog potpisa (*engl. digital signature*) koji je skup podataka u elektronskom obliku koji su dodati ili logički pridruženi elektronskim porukama ili dokumentima i služe kao metod za identifikaciju potpisnika.[17]

Neki primeri kršenja integriteta će biti opisani. Salama napad (*engl. salami attack*) je forma napada koji se ponavlja više puta, a najčešće je vezan za dobavljanje finansijske koristi, gde se maliciozni program koristi da ukrade veoma mali deo iznosa, koji se ne primećuje jednostavno. Kada se mnogo puta program izvrši, ta suma naraste. Ovaj napad je težak za detekciju i njegova detekcija u velikoj meri zavisi od svesti zaposlenih. Napad sa posrednikom (*engl. man-in-the-middle attack*), je specifična vrsta napada gde se napadač nalazi između dve strane koje komuniciraju i prisluškuje komunikaciju presretanjem poruka i pri tome menja sadržaj tih poruka, pri čemu učesnici komunikacije nisu svesni posrednika. Ova vrsta napada može imati nekoliko formi, a jedan od njih je preuzimanje sesije (*engl. session hijacking attack*), trovanje ARP keša (engl. *ARP cache poisoning*) ili DNS *Spoofing*, koji otvaraju prostor za sprovođenje drugih napada.

Integritet je vezan za očuvanja konzistentnosti, tačnosti i pouzdanosti podataka tokom celokupnog ciklusa. Podaci ne mogu da budu promenjeni u prenosu i podaci ne smeju da budu izmenjeni od strane neautorizovanih ljudi. Dosta tehnika koje se koriste i za očuvanje poverljivosti, koriste se i za očuvanje integriteta. Pored toga, važno je istaći i kontrolu pristupa (*engl. access control*), gde se u poslovnim sistemima uobičajeno koristi model zasnovan na ulogama (*engl. role-based access control*). Takođe, primenjuju se i mehanizmi koji proveravaju integritet. Pored toga, uobičajeno je da se prave rezerve podatka (*engl. backup*).

Opisaćemo neke napade koji se odnose na kompromitaciju raspoloživosti. Odbijanje usluge (*engl. denial of service attack*) je tip napada u kome se usled velikog broja zahteva ka nekom serveru ili servisu dogodi da on postane nedostupan jer ne može da procesira pomenute zahteve. Specijalna forma tog napada je distribuirano odbijanje usluge (*engl. distributed denial of dervice attack*) koje dolazi iz više različitih izvora i blokiranjem jednog izvora napad se ne može zaustaviti. Jedan od pristupa jeste da napadač programira mrežu računara, poznatiju kao botnet koji preplave server zahtevima i dovedu ga

[17] Digatalni potpis. Preuzeto sa: http://ca.mup.gov.rs/digitalni-potpis-lat.html.

u stanje da on padne i postane nedostupan. Jedna vrsta prethodno opisanog napada je *SYN flood* napad. Obzirom da na transportnom sloju može da se koristi TCP protokol, koji je i u osnovi internet protokol steka, napadač može da iskorišćava način na koji funkcioniše njegov mehanizam pod nazivom TCP trostruko rukovanje (*engl. TCP three-way handshake*). *SYN flood* napad funkcioniše tako što napadač ne odgovori serveru na očekivani ACK kod, jer je uobičajeno poslao zahtev sa lažne IP adrese. Obzirom da server čuva red neisporučenih poruka, u memoriji vremenom dolazi do njegovog zatrpavanja, pogotovo kada je broj zahteva veći.

Mere koje je potrebno sprovoditi u cilju raspoloživosti, koja je u snažnoj sprezi sa druga dva principa, jeste da su podaci dostupni unutar svih sistema i da može da se podnese odgovarajuće mrežno opterećenje. Samim tim, je potrebno hardver držati ažurnim, nadgledati upotrebu mrežnog opsega i obezbediti mogućnosti oporavka i oporavaka od katastrofe (*engl. disaster recovery*) ukoliko do toga dođe. Sve opisane tehnike zaštite su deo šifre strategije bezbednosti.[18] Prvi korak te strategije jeste definisati politiku bezbednosti. Sa jedne strane ona može biti jedan neformalan dokument koji opisuje željeno ponašanje sistema, dok sa druge to može biti dokument koji sadrži pravila i prakse, koje organizacija primenjuje da bi obezbedila bezbednosne servise. Uobičajeno se navodi: vrednost sredstava koja se štite, ranjivosti sistema i potencijalne pretnje i verovatnoće napada. Zatim sledi proces implementacije koji sadrži sledeće komplementarne aktivnosti: prevencija, detekcija, odgovor i oporavak. Nakon toga slede radnje u vezi osiguravanja i procene. Osiguravanje je atribut informacionog sistema koji je osnova u poverenje da sistem radi u skladu sa primenjenim politikama. Evaluacija je proces utvrđivanja da li je sistem ispunio odgovarajuće propisane kriterijume.

U organizacijama je uobičajeno da imaju timove koji su posvećeni problemu bezbednosti, koji sprovode celokupnu strategiju bezbednosti, koja je u skladu sa poslovanjem. Neke organizacije se odlučuju da za bezbednosne servise, kao i kompletno upravljanje njima angažuju specijalizovanu organizaciju, koja će za njih to obavljati u potpunosti ili služiti u cilju poboljšanja postojećih bezbedonosnih servisa.[19] Te organizacije se nazivaju dobavljači bezbednosnih usluga (*engl. managed security service provider*) i najčešće su nastali kao proširenje aktivnosti dobavljača internet usluga (*engl. Internet*

[18] Stallings, W., Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson. pp. 46-48

[19] Eight major benefits of having a Managed Security Services Provider (MSSP). Preuzeto sa: https://www.infradata.co.uk/news-blog/8-major-benefits-of-having-a-managed-security-services-provider-mssp/

*service provider*). Pomenute organizacije obavljaju poslovne stalnog monitoringa, upravljanje sistemima za detekciju upada (*engl. intrusion detection systems*), upravljanje zaštitnim barijerama (*engl. firewalls)*, nadgledanje nadoradnje softvera na nove verzije, kao i odgovarajuće bezbednosne procene, revizije i odgovore na hitne slučajeve, kao i razne konsultantske usluge. Uobičajeno nude svoje usluge upotrebom platforme računarstva u oblaku (*engl. cloud computing*) po modelu softvera kao usluge (*engl. software-as-a-service*). Pored toga, što pomenuti način uvećava bezbednost servisa oranizacije, on se može pokazati kao i finansijski isplativ.

## Ljudski faktor

U praksi je čest slučaj da i pored toga što su adekvatno sprovedene sve mere tehničke i tehnološke prirode koje se tiču politike bezbednosti i organizacije imaju bezbedonosne probleme usled toga što zasposleni ne poštuju propisane politike u adekvatnoj meri. Pomenuti problem je deo šireg problema vezanog za izgradnju i uspostavljanje informaciono-bezbednosne kulture, gde je jedan od glavnih aspekata podizanje svesti korisnika informacionih tehnologija.[20] Bezbedonosna kultura se ogleda u prepoznavanju opasnosti, reagovanju na njih izbegavanjem opasnosti, otklanjanju opasnosti ili upućivanju na one subjekte koji će profesionalno reagovati i sačuvati ugrožene vrednosti.[21]

Određena istraživanja pokazuju da organizacije koje obraćaju pažnju pored tehničkih i na netehnička sredstva u zaštiti svojih informacionih sistema, imaju najbolje rezultate u očuvanju sredstava. Ifinedo[22] je sproveo istraživanje koje je imalo za cilj da pokaže uticaj teorije planiranog ponašanja (*engl. theory of planned behavior*) i motivacione teorije zaštite (*engl. protection motivation theory*) na ispunjenje politike bezbednosti informacionih sistema (*engl. information systems security policy compliance*). Motivacija za zaštitu proizilazi iz ocene pretnje i ocene suočavanja. Ocena pretnje se sastoji iz percipirane ranjivosti, tj. ocene pojedinca o verovatnosti pretećeg događaja i percipirane jačine posledice tih togađaja. Ocena suočavanja se

[20] Milanović, Z., Radovanović, R. (2015). Informaciono-bezbedonosna kultura - imperativ savremenog društva. *NBP. Nauka, bezbednost, policija, 20*(3), str. 55.

[21] Bjelajac, Ž., Jovanović, M. (2013). Pojedini aspekti bezbedonosne kulture na internetu. *Kultura Polisa, 10*(21), str. 102.

[22] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

sastoji iz samoefikasnosti kao procene sposobnosti pojedinca da izvede preporučeno ponašanje, efikasnosti odgovora kao verovanja o koristima akcije koja je preduzeta i troška odgovora kojim se naglašava uočeni oportunitetni trošak u pojmovima novca, vremena, uloženog napora u usvajanju određenog ponašanja. Teorija planiranog ponašanja u pomenutom istraživanju koristi tri činioca, a to su da je ponašanje definisano kao pozitivno ili negativno osećanje pojedinca usmereno ka angažovanju u određenom ponašanju (u ovom slučaju to je stav ka ispunjenju politike bezbednosti informacionog sistema), subjektivna norma koja opisuje percepciju pojedinca o tome šta ljudi, koji su važni za njih, misle o datom ponašanju i samoefikasnost koja se odnosi se na percipiranu lakoću ili poteškoću u izvođenju ili olakšavanju određenog ponašanja. Istraživanje je sprovedeno na 124 ispitanika različitih demografskih karakteristika i pokazalo se da su na poželjno ponašanje u kontekstu ispunjenja politike bezbednosti informacionih sistema uticali faktori kao što su samoefikasnost, efikasnost odgovora, odnos prema saglasnosti, uočena ranjivost i subjektivne norme.

## Zaključak

Bezbednost informacionih sistema je izuzetno važna za ostvarivanje misije, vizije i ciljeve svake organizacije, koja svoje poslovanje organizuje upotrebom računarski zasnovanih informacionih sistema, a danas to su gotovo sve organizacije. Konstantne promene u okruženju, deluju na organizaciju i na njen informacioni sistem pa je potrebno sprovesti odovarajući bezbedonosni menadžment, da bi se stare i izmenjene, a neke i novonastale pretnje svele na prihvatljivu meru. Pokazuje se da iako sprovedene mere tehničke i tehnološke prirode mogu da budu na visokom nivou, to ne garantuje eliminisanje pretnji, jer one su često deo ljudske prirode i da najbolje rezultate imaju one organizacije koje primenjuju i tehnološke i netehnološke mere. U cilju podizanja svesti o bezbednosti u organizaciji, često je potrebno da menadžeri izvrše uticaje na zaposlene i time deluju na ispunjenje politike bezbednosti informacionog sistema.

***Bjelajac Đ. Željko, LLD***
The Faculty of Law for Commerce and Judiciary, The University of Business Academy in Novi Sad

***Vesić Lj. Slavimir***
Doctoral candidate, The Faculty of Economics and Engineering Management, The University of Business Academy in Novi Sad

# SECURITY OF INFORMATION SYSTEMS

***A b s t r a c t***

In modern business conditions, organizations have achieved their missions, visions and goals of using information systems. They enable them to share data, information and knowledge with a changing environment, to carry out daily activities smoothly, and to create the basis for strategic decisions. As new modalities for compromising information systems security emerge due to the changing unsafe environment and threats that lurk from cyberspace, it is necessary to pay attention to them and to respond appropriately, since it is no longer only a question of vulnerability of information and communication infrastructure and information, but also of human life. In the security of information systems itself, in addition to the technical security measures implemented following the defined security policy, it's necessary to pay attention to the human factor and security awareness, as the weakest link, and to act to minimize threats.

***Key words:*** *information systems, security, cyber security, human factor*

## *Literatura*


1. Bjelajac, Ž., Jovanović, M. (2013). Pojedini aspekti bezbedonosne kulture na Internetu. *Kultura Polisa, 10* (21), str. 99-114
2. Bocij, P., Greasley, A., Hickie, S. (2015). Business Information Systems (5th ed.). Harlow, United Kingdom, Pearson
3. Bourgeois, D. (2014). Information Systems for Business and Beyond. Saylor Foundation. Preuzeto sa: https://resources.saylor.org/wwwresources/archived/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf
4. Đukić, S. (2017). Osnove i sistem bezbednosti u strategiji nacionalne bezbednosti. *Vojno delo, 69* (7), str. 100-121
5. Eight major benefits of having a Managed Security Services Provider (MSSP). Preuzeto sa: https://www.infradata.co.uk/news-blog/8-major-benefits-of-having-a-managed-security-services-provider-mssp/
6. Henshaw, M., Dahmann, J., Lawson, B. (2019). *Systems of Systems (SoS)*. Preuzetosa:https://www.sebokwiki.org/wiki/Systems_of_Systems_(SoS)
7. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), str. 83-95
8. Ilić, P. (2011). Semantičko-leksikografski aspekti pojma bezbednosti. *Vojno delo, 63*(3), str. 85-99
9. ISO/IEC. (2004). International standard 13335-1. Preuzeto sa: https://www.sis.se/api/document/preview/905483/
10. Kurose, J., Ross, K. (2009). Umrežavanje računara - Od vrha ka dnu (4. izd.). Beograd, Srbija: Računarski fakultet
11. Milanović, Z., Radovanović, R. (2015). Informaciono-bezbedonosna kultura - imperativ savremenog društva. *NBP. Nauka, bezbednost, policija, 20*(3), str. 45-65
12. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M. (2006). Sigurnost računarskih mreža. Beograd, Srbija, Viša elektrotehnička škola u Beogradu
13. Šnajer, B. (2007). Primenjena kriptografija - prevod drugog izdanja. Beograd, Mikro knjiga.
14. Digitalni potpis. Preuzeto sa: http://ca.mup.gov.rs/digitalni-potpis-lat.html
15. Stair, R., Reynolds, G. (2017). Principles of Information Systems (13th ed.). Boston, Massachusetts, USA: Cengage Learning
16. Stallings, W., Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Harlow, United Kingdom: Pearson

17. Types of Network Attacks against Confidentiality, Integrity and Avilability. Preuzeto sa: https://www.omnisecu.com/ccna-security/types-of-network-attacks.php
18. Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. *38*, str. 97-102