# ZNAČAJ ISO 27001 STANDARDA ZA INFORMACIONU SIGURNOST / IMPORTANCE OF ISO 27001 STANDARD FOR INFORMATION SECURITY

Edin Alić[1], Azra Ahmić[1], Muhamed Ćosić[1], Venan Hadžiselimović[2]
[1]Internacionalni univerzitet Travnik, Bosna i Hercegovina
[2]HIFA-OIL d.o.o. Tešanj, Bosna i Hercegovina
e-mail: alicedin@hotmail.com, azraahmic30@gmail.com, drmuhamedcosic@gmail.com, venanh@hifaoil.ba

***Pregledni članak***
**UDK / UDC 004.056.5:005.1**

**Sažetak**
*Informaciona sigurnost postaje ključna komponenta za savremeno poslovanje zbog sve veće zavisnosti od digitalnih tehnologija. Ciljevi informacionih sistema obuhvataju očuvanje povjerljivosti, integriteta i dostupnosti podataka, što je ključno za efikasnost i zaštitu organizacija. Ulaganje u informacioni sistem omogućava bolje donošenje odluka, upravljanje poslovanjem i unapređenje odnosa sa klijentima. S razvojem tehnologije javljaju se prijetnje poput zlonamjernog softvera, phishing napada i tehničkih ranjivosti. Da bi se smanjio rizik, potrebno je koristiti enkripciju, dvofaktorsku autentifikaciju i redovne sigurnosne provjere, uz kontinuirano obrazovanje zaposlenih. ISO 27001 standard omogućava sistemski pristup upravljanju sigurnošću informacija, što doprinosi stabilnosti i jačanju povjerenja klijenata. Implementacijom ovog standarda, organizacije smanjuju sigurnosne prijetnje, identifikuju ranjivosti i razvijaju strategije za smanjenje rizika gdje ostvaruju konkurentsku prednost i dugoročnu efikasnost.*

***Ključne riječi:*** *Informaciona sigurnost, rizici, prijetnje, strateško upravljanje i organizacija, zaštita podataka.*
JEL *klasiikacija*: L86

**Abstract**
*Information security is becoming a key component for modern business due to the increasing dependence on digital technologies. The goals of information systems include the preservation of confidentiality, integrity and availability of data, which is crucial for the efficiency and protection of organizations. Investing in an information system enables better decision-making, business management and improvement of relations with clients. As technology evolves, do to threats such as malware, phishing attacks, and technical vulnerabilities. To reduce the risk, it is necessary to use encryption, two-factor authentication and regular security checks, along with continuous employee education. The ISO 27001 standard enables a systematic approach to information security management, which contributes to stability and strengthening client trust. By implementing this standard, organizations reduce security threats, identify vulnerabilities and develop risk reduction strategies where they achieve competitive advantage and long-term efficiency.*

***Keywords:*** *Information security, risks, threats, strategic management and organization, data protection.*
JEL *classification*: L86

# UVOD

Informaciona sigurnost je ključni poslovni proces u zaštiti povjerljivih poslovnih podataka i očuvanja stabilnosti i integriteta poslovanja. Sistem upravljanja sigurnošću informacija (ISMS) je neophodan jer prijetnje dostupnosti, integritetu i povjerljivosti informacija organizacije su velike i stalno rastu.[226] Razumijevanje, implementacija i održavanje visokih standarda informacione sigurnosti postaju strateški proces za organizacije. Upravljanje informacionom sigurnosti igra važnu ulogu u sposobnosti organizacije da efikasno upravlja sigurnosnim pitanjima u svim poslovnim aktivnostima. Održavanje sigurnosti informacionih sistema i zaštita osjetljivih podataka predstavljaju izazove za organizacije, ali su neophodni za očuvanje kontinuiteta poslovnih operacija i reputacije. Cilj informacionog sistema (IS) je osigurati pravovremenu, tačnu i relevantnu informaciju na odgovarajućem mjestu uz minimalne troškove. Međutim, postizanje tog cilja u praksi nije jednostavno. Samo poslovni sistemi koji ulažu dovoljno u razvoj informacionih sistema mogu se uspješno nositi sa izazovima složenih uslova globalnog tržišta i konkurencije. Danas je nemoguće zamisliti da menadžeri mogu uspješno upravljati organizacijama na čijem su čelu bez dobro organizovanog i efikasnog informacionog sistema. Upravljanje organizacijom je sve više zavisno od kvaliteta informacija koje informacioni sistem pruža. Informacioni sistemi direktno utiču na procese donošenja odluka, planiranje i upravljanje zaposlenicima, dok sve više postaju ključan faktor u određivanju prioriteta i vremenskog rasporeda odluka.

Ključne uloge informacionih sistema u organizacijama uključuju:

- **Pomoć pri donošenju odluka**: Informacioni sistemi omogućavaju menadžmentu donošenje informisanih odluka kroz analize, izvještaje i prediktivnu analizu.
- **Povećanje efikasnosti i produktivnosti**: Automatizuju zadatke, ubrzavaju razmjenu podataka i omogućavaju lakši pristup informacijama, što poboljšava produktivnost.
- **Podrška poslovnim aktivnostima**: Integracijom funkcija omogućavaju bolje upravljanje resursima i identifikaciju oblasti za unapređenje.
- **Komunikacija**: Omogućavaju internu saradnju putem alata za komunikaciju, bez obzira na lokaciju.
- **Unapređenje odnosa sa klijentima**: Kroz CRM sisteme pomažu u personalizovanoj komunikaciji i izgradnji dugoročnih veza. **Podsticanje inovacija**: Pružaju pristup informacijama za identifikaciju poslovnih prilika i razvoj novih proizvoda i usluga.

Upotreba savremenih informacionih sistema omogućava organizaciji da se izdvoji na tržištu, nudeći bolje, pouzdanije i kvalitetnije usluge ili proizvode. Kombinovanjem ovih elemenata, IS postaje ključan faktor za uspješno poslovanje kako na lokalnom tako i na globalnom planu. U današnjem poslovnom okruženju, informacije su postale ključni resurs savremenog poslovanja. One nisu samo podaci, već dragocjeni resurs sa ogromnim potencijalom za transformaciju i konkurentsku prednost za organizacije. Prvo i najvažnije, informacije su temelj za donošenje informisanih odluka. Kvalitetne informacije omogućavaju menadžerima da sagledaju tržišne uslove, preferencije potrošača, strategije konkurencije i unutrašnje operacije.

[226] Calder, A, Watkins, S. (2015) An international guide to data security and ISO27001/ISO27002, IT Governance 6th edition: Kogan Page Publishers, str. 9.

Na osnovu dobivenih podataka, menadžeri mogu donositi odluke koje su u skladu sa ciljevima i planovima organizacije te doprinose njenom dugoročnom uspjehu. Organizacije koje efikasno prikupljaju, analiziraju i primjenjuju relevantne informacije često su uspešnije od konkurencije. Razumjevanje tržišta i potrošača omogućava organizacijama da razvijaju proizvode i usluge koje bolje zadovoljavaju potrebe klijenata, čime stvaraju održivu prednost na tržištu. Inovacije su ključno područje u kojem informacije igraju presudnu ulogu. Analizom podataka o trendovima, potrebama kupaca i novim tehnologijama, organizacije mogu prepoznati prilike za razvoj novih proizvoda ili usluga. Ova sposobnost predviđanja i inovativnog reagovanja ključna je za dugoročni uspjeh u dinamičnom poslovnom okruženju. Upravljanje rizicima u poslovanju takođe zavisi od tačnih i pravovremenih informacija koje omogućavaju identifikaciju i smanjenje potencijalnih rizika, čime se pomaže u kontroli finansijskih rizika, sajber bezbjednosti i usklađenosti sa zakonima. Informacije su važan resurs za izgradnju i održavanje odnosa s kupcima. Razumijevanje njihovih potreba i povratnih informacija omogućava organizacijama da pruže personalizovane usluge i izgrade lojalnost što doprinosi dugoročnom uspjehu.

# 1. INFORMACIONA SIGURNOST

Tehnološki napredak i novi uređaji povećavaju oslanjanje na informacione sisteme, ali i zabrinutost zbog prijetnji kao što su hakeri i krađa podataka. Organizacije prikupljaju i skladište osjetljive informacije o zaposlenima, klijentima i proizvodima, što zahtijeva ozbiljan pristup zaštiti sistema. Budući da vrijednost organizacije često zavisi od vrijednosti njenih informacija, zaštita tih podataka postaje od strateškog značaja. Sigurnost informacionih sistema obuhvata metode koje osiguravaju zaštitu podataka i sistema od neovlaštenog pristupa, manipulacije i uništenja, što je od strateškog značaja za vrijednost organizacije[227].

**Tri glavna područja koja čine osnovu informacione sigurnosti su:**
**Povjerljivost** ( eng. Confidentiality ), osigurava da samo ovlaštene osobe imaju pristup informacijama i sistemima. Procedure za održavanje povjerljivosti moraju biti temeljito implementirane. Ključni aspekti povjerljivosti uključuju korisničku identifikaciju i autentifikaciju. Uspješna identifikacija je ključna kako bi se osigurala djelotvornost politika koje određuju koji korisnici imaju ovlasti pristupa određenim podacima. Povjerljivost može biti kompromitirana na različite načine.

**Najčešće prijetnje povjerljivosti su:**

- Nepoštivanje sigurnosnih procedura i politika od strane zaposlenika.
- Neovlašten pristup ili krađa identiteta.
- Napadi hakera i krađa podataka putem računarskih mreža.
- Fizički gubitak ili krađa uređaja koji sadrže osjetljive informacije.
- Društveno inženjerstvo i prevare putem lažnog predstavljanja.
- Slabe kontrole pristupa i nedostatak autentifikacije.
- Nedostatak obuke i svijesti o sigurnosnim praksama među zaposlenicima.
- Propusti u sigurnosti dobavljača i vanjskih partnera.

[227] Michael E. Whitman & Herbert J. Mattord (2021) Principles of Information Security, Cengage Learning, poglavlja 2 i 3.

**Integritet** ( eng. Integrity ) - osigurava da podaci ostanu ispravni i cjeloviti, te da nisu podložni neovlaštenim promjenama.Važno je osigurati da podaci kojima pristupaju ovlašteni korisnici ostanu cjeloviti. Sigurnosne mjere ne mogu jamčiti tačnost podataka koje korisnici unose u sistem, ali mogu pomoći u osiguranju ispravnosti promjena nad podacima. Integritet se može ugroziti putem hakiranja, prikrivanja, neovlaštene korisničke aktivnosti, nezaštićenog preuzimanja datoteka, lokalnih mreža, trojanskih konja i slično.

**Tri su temeljna principa uspostave kontrola integriteta:**

- Dodjela samo određenih prava pristupa (eng. Need-to-know basis). Korisnicima treba dodijeliti pravo pristupa samo na one datoteke i programe koji su im potrebni da bi obavljali svoju poslovnu funkciju u organizaciji.
- Razdvajanje dužnosti (eng. Separation of duties). Potrebno je osigurati da nijedan zaposlenik nema kontrolu nad informacijom od početka do kraja.
- Rotacija dužnosti (eng. Rotation of duties). Periodično mijenjanje poslovnih zadataka može otežati zlonamjerno preuzimanje kontrole nad sistemom. Ovaj princip pokazuje učinkovitost kada se koristi zajedno sa odvajanjem dužnosti. Međutim, organizacije koje imaju manjak zaposlenih ili zaposlenika sa manje iskustva teško provode rotaciju dužnosti.

**Raspoloživost** ( eng. Availability ). Osigurava da ovlaštene osobe imaju pravovremen i neprekidan pristup informacijama i sistemima.

**Dva su najvažnija aspekta raspoloživosti:**

- Uskraćivanje usluge (eng. Denial of service). Distribuirano uskraćivanje usluge (eng. Distributed Denial of Service - DDoS) je vrsta napada u kojoj se namjerno generiše velika količina mrežnog prometa kako bi se zagušili mrežna oprema i poslužitelji. Kada su opterećeni, oni postaju nesposobni obraditi ispravan zahtjev za izvršenje usluge.
- Gubitak sposobnosti procesiranja podataka kao rezultat prirodnih katastrofa (npr:poplave, potresi, požari) ili ljudskih akcija (teroristički napadi, štrajkovi).

Planiranje nepredviđenih situacija, koje može uključivati planiranje oporavka od katastrofe (eng. Disaster recovery planning), planiranje obnove poslovnih procesa (eng. Business resumption planning) i slično, pruža alternativne načine procesiranja podataka odnosno osiguranje raspoloživosti

Ranjivost predstavlja nedostatak ili slabost u sigurnosnim procedurama, dizajnu, implementaciji ili unutrašnjim kontrolama informacionog sistema. Takva ranjivost može biti slučajno aktivirana ili namjerno iskorištena od strane zaposlenih ili napadača, što može ugroziti sigurnost sistema i dovesti do kršenja sigurnosne politike. Prijetnje informacionom sistemu uključuju aktivnosti koje narušavaju integritet, poverljivost i dostupnost podataka i resursa, bilo kroz tehničke ili fizičke napade ili kroz nenamjerne ili namjerne ljudske aktivnosti. Zaštita informacionih sistema zavisi od uvođenja i primjene informacionih kontrola, koje služe smanjenju ili ublažavanju rizika. Ove kontrole obuhvataju preventivne, detektivne i korektivne mjere koje sprečavaju, otkrivaju i ispravljaju neželjene događaje, omogućavajući tako nesmetano funkcionisanje sistema. Efikasne kontrole smanjuju vjerovatnoću da informacioni sistem bude izložen prijetnjama i da neželjeni događaji postanu poslovni rizici.

# 2. ISO / IEC 27001 STANDARD

Međunarodni standard ISO/IEC 27001 je ISMS skup zahtjeva za uspostavljanje, implementaciju, implementaciju, praćenje, pregled, održavanje, ažuriranje i poboljšanje dokumentovanog ISMS-a u odnosu na sveukupne poslovne rizike i mogućnosti organizacije.[228] Standard ISO 27001 ima za cilj zaštitu poverljivosti, integriteta i dostupnosti informacija za sve zainteresovane strane kroz uspostavljanje odgovarajućih mehanizama kontrole zaštite i pristupa informacijama. U tehnološkom razvoju informacionih tehnologija, informacije su postale dostupne svim zainteresiranim stranama, ali i sigurnosno veoma ranjive. Informacije predstavljaju resurs koji poput drugih poslovnih sredstava ima značaj za organizaciju i potrebno je da budu adekvatno zaštićene. Implementacija međunarodnih standarda i pravila za informacionu sigurnost je imperativ za organizacije koje žele opstati u poslovnom okruženju sa brzim tehnološkim napretkom. Korištenje ISO 27001 standarda postaje strateški cilj za organizacije koje žele osigurati visoku razinu kvalitete i sigurnosti u svojim aktivnostima. Standard je posvećen bezbjednosti informacija i daje okvir na koji način organizacije treba da pristupe zaštiti informacija. On je značajan za sve organizacije koje imaju potrebu za kontrolom pristupa informacijama, bez obzira čime se bave, to jeste da li posluju u oblasti informacionih tehnologija, proizvodnjom ili pružanjem usluga.

U uslovima visoke konkurentnosti, tačna i blagovremena informacija predstavlja novac (kapital), opstanak i prednost na tržištu. Podatak koji je ažuriran i pravovremeno dostavljen do korisnika postaje informacija. ISO 27001 standard se primjenjuje u raznim oblastima kako bi identificirao različite procese u organizaciji povezane sa upravljanjem informacionom sigurnosti. Ovi procesi obuhvataju: politiku sigurnosti, kontrolu i klasifikaciju resursa, sigurnost zaposlenih, zaštitu poslovnih sredstava, strateško upravljanje i komunikaciju, kontrolu pristupa, razvoj i održavanje informacionih sistema, kao i upravljanje kontinuitetom poslovanja.

Prednosti implementiranog ISMS-a prema zahtjevima standarda ISO 27001 mogu se podjeliti u dva dijela:

- Zaštita i sigurnost informacija i **know-how** organizacije postiže se sistematskim pristupom za identifikaciju i dovođenje pod kontrolu različite potencijalne rizike sa kojima je organizacija izložena. Upravljanje rizicima po bezbjednost informacija značajno smanjuje vjerovatnoću pojave nekontrolisanih situacija u poslovnim aktivnostima.
- Zaštita podataka i informacija klijenata sa kojima organizacija dolazi u kontakt tokom instalacije opreme, obuke, projektovanja i montaže je ključna. Certifikat o implementiranom ISMS-u prema zahtjevima standarda ISO 27001 dokazuje da su informacije klijenata i partnera sigurni i zaštićeni od različitih zloupotreba. Takav sistem daje organizaciji konkurentsku prednost.

Standard koristi procesni pristup za uspostavljanje, implementaciju, rad, praćenje, kontrolu, održavanje i unapređivanje ISMS-a u organizaciji. Kako bi organizacija funkcionisala efikasno, potrebno je da upravlja sa brojnim aktivnostima. Aktivnosti koje koriste poslovne resurse i u kojima se vrši transformacija ulaznih elemenata u izlazne naziva se procesom. Procesni pristup podrazumijeva primjenu sistema procesa unutar same organizacije, uključujući identifikaciju, međusobno djelovanje i njihovo upravljanje.

[228] Humphreys, Edward. (2016) Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, str. 22.

# 3. REZULTATI ISTRAŽIVANJA

Cilj provedenog istraživanja bio je da se dobiju podaci o percepciji uposlenika o aspekatima informacione sigurnosti u organizacijama. Kroz ovo istraživanje analizirani su stavovi, znanje i praksa zaposlenika u vezi s različitim komponentama informacione sigurnosti. Fokus je bio trenutnoj svijesti zaposlenika o sigurnosnim protokolima i procedurama unutar organizacija. Istraživanje je provedeno kroz anketiranje kompanija male, srednje i velike veličine, različitih djelatnosti i vlasničke strukture (privatne i državne), na uzorcima 305 zaposlenika. Anketirane kompanije iz naftnog, proizvodnog, trgovačkog, finansijskog, građevinskog i informatičkog sektora. Ukupan broj kompanija na kojima je napravljeno istraživanje jeste 115 privatnih i 35 državne kompanije. Sve kompanije u kojima je provedeno istraživanje nalaze se u Republici Bosni i Hercegovini.

Grafikon 1 prikazuje rezultate anketnog istraživanja o stanju informatičke sigurnosti u organizaciji na osnovu uzorka od 305 zaposlenika, koristeći pie chart.

**Opis rezultata prikazanih na grafikonu:**

- Ovaj segment čini najveći dio grafikona, što znači da je najveći broj zaposlenika ocijenio stanje informatičke sigurnosti kao "Vrlo dobro" (45,5%).
- Značajan broj zaposlenika ocijenio stanje informatičke sigurnosti kao "Dobro" (32,5%).
- Ovaj segment prikazuje manji broj zaposlenika koji su ocijenili stanje kao "Izvrsno" (15,1%).
- Vrlo mali broj zaposlenika ocijenio stanje kao "Loše" (4,6%).

Ovaj segment je najmanji, što znači da je najmanji broj zaposlenika odgovorio s "Ne znam" (2,3%).

Grafikon jasno prikazuje kako su zaposlenici ocijenili informatičku sigurnost u njihovoj organizaciji, sa većinom ocjena u pozitivnom spektru ("Vrlo dobro" i "Dobro").


Izvor: Istraživanje autora rada

Grafikon 1: Kakvo je prema Vašem mišljenju stanje informatičke sigurnosti u Vašoj organizaciji?

| PONUĐENI ODGOVORI | ODGOVOR | |
|---|---|---|
| | Broj | % |
| Loše | 14 | 4,6 |
| Dobro | 99 | 32,5 |
| Vrlo dobro | 139 | 45,5 |
| Izvrsno | 46 | 15,1 |
| Ne znam | 7 | 2,3 |
| **UKUPNO** | **305** | **100 %** |

Izvor: Istraživanje autora rada

Tabela 1: Kakvo je prema Vašem mišljenju stanje informatičke sigurnosti u Vašoj organizaciji?

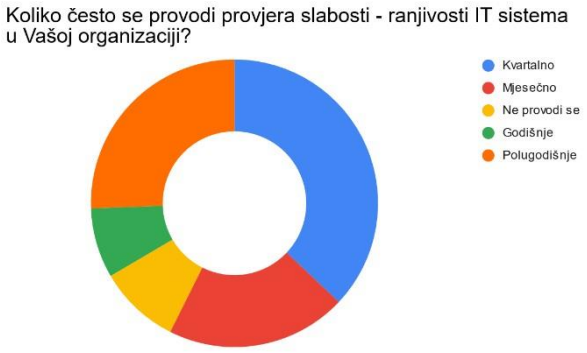
Ovi podaci predstavljaju rezultate anketnog istraživanja u kojem su zaposlenici ocjenjivali stanje informatičke sigurnosti u organizaciji na skali od "Loše" do "Izvrsno". Rezultati su prikazani brojčano sa postotcima za svaku ocjenu.

Grafikon 2 prikazuje učestalost provjere slabosti - ranjivosti IT sistema u organizacijama na osnovu uzorka od 305 zaposlenika, koristeći pie chart.

**Opis rezultata prikazanih na grafikonu:**

- Ovaj segment čini najveći dio grafikona, što znači da je najveći broj zaposlenika odgovorio da se provjere vrše "Kvartalno" (37%).
- Određeni broj zaposlenika je odgovorio je da se provjere vrše "Mjesečno" (20,3%).
- Značajan broj zaposlenika odgovorio je da se provjere vrše "Polugodišnje" (25,6%).
- Ovaj segmentt prikazuje broj zaposlenika koji su odgovorili da "Ne provode se"provjere slabosti – ranjivosti IT sistema (9,2%).
- Ovaj segment je najmanji, što znači da je najmanji broj zaposlenika odgovorio da se provjere vrše "Godišnje" (7,9%).

Prema grafikonu, najveći broj organizacija vrši provjere kvartalno, zatim mjesečno, pa godišnje, dok pojedine organizacije ne provode provjere nikako dok mali broj organizacija vrši provjere polugodišnje.




Izvor: Istraživanje autora rada

Grafikon 2: Koliko često se provodi provjera slabosti – ranjivosti IT sistema u Vašoj organizaciji?

| PONUĐENI ODGOVORI | ODGOVOR | |
|---|---|---|
| | Broj | % |
| Mjesečno | 62 | 20,3 |
| Kvartalno | 113 | 37 |
| Polugodišnje | 78 | 25,6 |
| Godišnje | 24 | 7,9 |
| Ne provodi se | 28 | 9,2 |
| **UKUPNO** | **305** | **100 %** |

Izvor: istraživanje autora rada

Tabela 2: Koliko često se provodi provjera slabosti – ranjivosti IT sistema u Vašoj organizaciji?

Ovi podaci predstavljaju rezultate anketnog istraživanja u kojem su zaposlenici ocjenjivali koliko često se provodi provjera slabosti – ranjivosti IT sistema u organizaciji. Rezultati su prikazani brojčano sa postotcima za svaku ocjenu.

Grafikon 3 prikazuje najveće opasnosti za sigurnost u organizacijama na osnovu uzorka od 305 zaposlenika, koristeći pie chart.

**Opis rezultata prikazanih na grafikonu:**

 Ponašanje zaposlenika predstavlja manju opasnost (11,5%).

- Napad na IT sistem predstavlja najveću opasnost (59,7%).
- Stanje IT infrastrukture je predstavlja značajnu opasnost (5,9%).
- Napadi na zaposlenike putem ucjena i drugih vrsta elektronskih prevara su opasnost, koje pored napada na IT sistem zauzimanju najveći dio grafikona (21,6%).  Ponašanje uprave organizacije predstavlja najmanju opasnost (1,3%).

Iz grafikona se može zaključiti da većina zaposlenika smatra da su napadi na IT sistem najveća opasnost za sigurnost u organizaciji, dok je ponašanje zaposlenika najmanje zabrinjavajuće.


Izvor: Istraživanje autora rada

Grafikon 3: Koja je najveća opasnost za sigurnost Vaše organizacije?

| PONUĐENI ODGOVORI | ODGOVOR | |
|---|---|---|
| | **Broj** | **%** |
| Napad na IT sistem | 182 | 59,7 |
| Napad na zaposlene - ucjene i druge vrste elektronskih prevara | 66 | 21,6 |
| Ponašanje zaposlenika | 35 | 11,5 |
| Ponašanje uprave organizacije | 4 | 1,3 |
| Stanje IT infrastrukture | 18 | 5,9 |
| **UKUPNO** | **305** | **100 %** |

Izvor: istraživanje autora rada

Tabela 3: Koja je najveća opasnost za sigurnost Vaše organizacije?

Ovi podaci pokazuju da je **napad na IT sistem** glavni razlog za zabrinutost među zaposlenicima, dok su ponašanje zaposlenika i uprave najmanje zabrinjavajući faktor. Rezultati su prikazani brojčano sa postotcima za svaku ocjenu.

Grafikon 4 prikazuje rezultate ankete o primjeni sigurnosnih politika u organizacijama na osnovu uzorka od 305 zaposlenika, koristeći pie chart.

**Opis rezultata prikazanih na grafikonu:**

- Ovaj segment čini najveći dio grafikona, što znači da je najveći broj zaposlenika odgovorio da je primjena sigurnosnih politika "Zadovoljavajuća" (61,3%). Značajan broj zaposlenika odgovorili su da je primjena sigurnosnih politika "Izvrsna" (26,2%).
- Ovaj segmentt prikazuje broj zaposlenika koji su odgovorili da je primjena sigurnosnih politika " Slaba" (10,5%).
- Najmanji broj zaposlenika odgovorio je da "Ne provodi se" primjena sigurnosih politika (2,0%).

Na rezultata iz grafikona, najveći broj ispitanika smatra da je implementacija sigurnosnih politika zadovoljavajuća dok najmanji broj smatra da je primjena slaba.


Izvor: Istraživanje autora rada

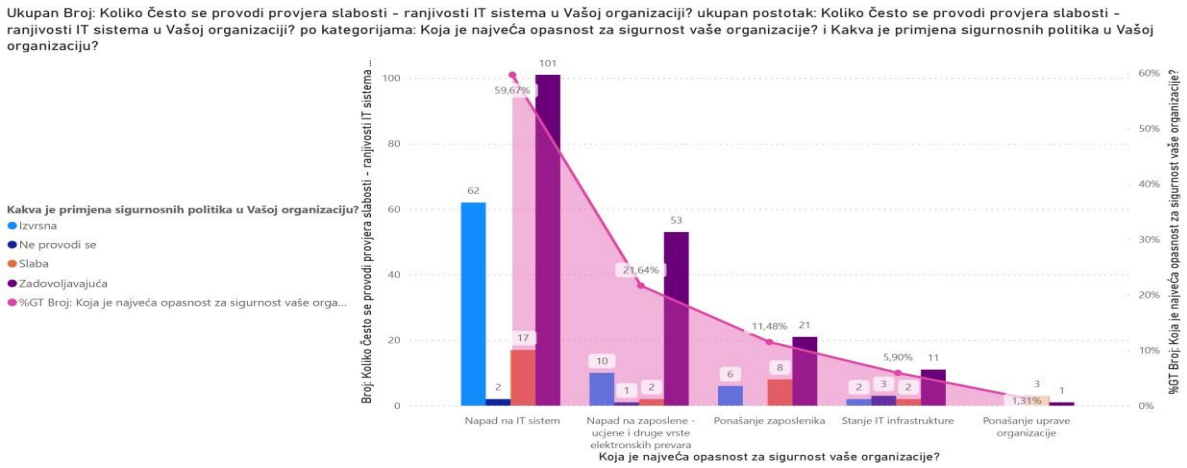
Grafikon 4: Kakva je primjena sigurnosnih politika u Vašoj organizaciji?

| PONUĐENI ODGOVORI | ODGOVOR | |
|---|---|---|
| | **Broj** | **%** |
| Izvrsna | 80 | 26,2 |
| Zadovoljavajuća | 187 | 61,3 |
| Slaba | 32 | 10,5 |
| Ne provodi se | 6 | 2,0 |
| **UKUPNO** | **305** | **100 %** |

Izvor: istraživanje autora rada

Tabela 4: Kakva je primjena sigurnosnih politika u Vašoj organizaciji?

Ovi podaci pokazuju da je primjena sigurnosnih politika u organizacijama zadovoljavajuća. Rezultati su prikazani brojčano sa postotcima za svaku ocjenu.




Izvor: Istraživanje autora rada

Grafikon 5: Učestalost provjere slabosti i ranjivosti IT sistema

Grafikon 5 prikazuje broj odgovora po kategorijama prijetnji i učestalost provjere slabosti i ranjivosti IT sistema. Većina zaposlenika smatra da su napadi na IT sistem najveća prijetnja sigurnosti (55,0%). Slijede nedovoljna edukacija zaposlenika (14,8%), ponašanje zaposlenika (11,8%), stanje IT infrastrukture (5,0%), i nepostojanje opreme za otkrivanje napada (3,1%).
Grafikon također prikazuje učestalost provjere slabosti i ranjivosti IT sistema po kategorijama. Najveći broj odgovora je za redovne provjere (najviše za napade na IT sistem).

# 4. DISKUSIJA

Ovi podaci ukazuju na to da su napadi na IT sistem prepoznati kao najveća prijetnja za organizacije, dok se većina organizacija pridržava zadovoljavajućih sigurnosnih politika. Redovne provjere slabosti i ranjivosti IT sistema su ključne za održavanje sigurnosti. Provedena anketa omogućila je analizu poznavanja osnovnih aspekata informacione sigurnosti u organizacijama među zaposlenicima te je istražila povezanost stepena obrazovanja zaposlenika, godina rada u organizaciji i poznavanje politika i procedura u zaštiti informacionih sistema unutar organizacije. Na osnovu ankete utvrđeno je da su zaposlenici organizacije upoznati sa osnovnim aspektima informacione sigurnosti, a njihov stepen obrazovanja utiče na razinu zaštite informacionih sistema unutar organizacije. Podaci dobiveni istraživanjem su dodatno ukazali na značaj implementacije ISO/IEC 27001 standarda u zaštiti informacione sigurnosti u korporativnom poslovanju. Rezultati istraživanja su potvrdili važnost svijesti o infomacionoj sigurnosti u korporativnom poslovanju i implementacije normi ISO/IEC 27001.
Standard se može implementirati u bilo kojoj organizaciji, bez obzira na njen profitni status, vlasničku strukturu ili veličinu. Standard su razvili vodeći svjetski eksperti za informacionu sigurnost i pruža metodologiju za uvođenje sistema upravljanja informacionom sigurnosti unutar organizacije. Također, omogućava organizacijama sticanje certifikata koji potvrđuje da je nezavisno certifikacijsko tijelo verifikovalo usklađenost organizacije sa ISO/IEC 27001 standardom. U savremenom poslovanju, informacioni sistemi su ključni za uspjeh organizacije, jer omogućuju donošenje odluka i upravljanje podacima neophodnim za funkcionisanje. Oni omogućavaju efikasno upravljanje podacima, automatizaciju poslovnih procesa, poboljšanu komunikaciju i saradnju, bolje upravljanje resursima i pružanje usluga korisnicima.

# ZAKLJUČAK

Porast digitalizacije i modernizacije poslovanja donosi i povećane sigurnosne rizike. Stoga je važno da organizacije prepoznaju opasnosti koje prijete njihovim informacionim sistemima i preduzmu odgovarajuće mjere zaštite. Izazovi sa kojima se suočavaju uključuju krađu intelektualne svojine, hakerske napade, špijunažu i unutrašnje prijetnje od zaposlenih. Posljedice sigurnosnih incidenata mogu biti ozbiljne, uključujući finansijske gubitke, gubitak povjerenja kupaca i partnera te narušavanje ugleda organizacije. Zbog toga je važno redovno provjeravati i unapređivati sigurnost informacionih sistema, implementirajući dodatne sigurnosne kontrole prema preporukama stručnjaka za informacionu sigurnost. Na taj način, organizacije mogu smanjiti rizik od napada i osigurati pouzdanost i sigurnost svojih informacionih sistema. Zahtjevi za posjedovanjem certifikata kao uslova za učestvovanje u javnim konkursima jasno pokazuju da je sistemski pristup i osiguranje informacione sigurnosti prepoznato kao preduslov za poslovanje i ekonomsku saradnju pravnih subjekata na globalnom i lokalnom tržištu.

Standard ISO/IEC 27001 u potpunosti zadovoljava stroge zahtjeve Opšte uredbe o zaštiti podataka (GDPR) i Direktive o sigurnosti mrežnih i informacionih sistema (NIS direktiva), čime se osigurava usklađenost sa većinom zahtjeva ovih zakonskih dokumenata kada organizacija implementira navedenu normu. Certificirani sistem upravljanja informacionom sigurnosti služi kao potvrda organizaciji prema postojećim i potencijalnim klijentima da su preduzeti svi koraci za zaštitu njenog poslovanja, informacija i podataka. Certifikat predstavlja dokaz učinkovite interne sigurnosne prakse, što organizaciji omogućuje sticanje konkurentske prednosti u odnosu na konkurenciju koja ne posjeduje isti certifikat.

Važnost, prihvaćenost i prepoznatljivost norme ISO/IEC 27001 raste u nacionalnim i međunarodnim okvirima, postajući ključni uslov za organizacije koje teže opstanku, razvoju i proširenju na nacionalnom i globalnom tržištu. Implementacija norme ISO/IEC 27001 u poslovanje organizacija stoga nije samo poželjna praksa, već imperativ.

# LITERATURA

1. Calder, A, Watkins, S. (2015) An international guide to data security and ISO27001/ISO27002, IT Governance 6th edition: Kogan Page Publishers, str. 9.
2. Calder, Alan, and Steve Watkins. (2008) A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd.
3. Disterer, Georg. (2013) ISO/IEC 27000, 27001 and 27002 for information security management.
4. Humphreys, Edward. (2016) Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, str. 22.
5. Bogati, J. (2011) Norme informacijske sigurnosti ISO/IEC 27K ,Praktični menadžment, Vol. II, br. 3, str. 112-117.
6. Davis, G.B., Olson, M.H. (1985) Management Information Systems: Conceptual Foundations, Structura and Development, McGraw- Hill, New York, SAD, str. 200-202.
7. Michael E. Whitman & Herbert J. Mattord (2021) Principles of Information Security,Cengage Learning.