

The background of the central section features a stylized, pixelated map of the world in shades of green and yellow, overlaid on a dark blue background with vertical lines and a subtle grid pattern.

“Pokretanje digitalne i održive transformacije u Crnoj Gori kroz ICT i BIM standarde”

ICT Standardi: Temelj digitalne bezbjednosti i interoperabilnosti

ICT Standards: Foundations of Digital Security and Interoperability

Svrha brošure:

Ova brošura je namijenjena svim zainteresovanim stranama koje žele da steknu osnovna saznanja o ICT standardima, njihovoj ulozi u razvoju informaciono-komunikacionih tehnologija i značaju njihove primjene u savremenom digitalnom okruženju.



Ovaj dokument pruža pregled **ICT standarda** kao ključnih pravila i specifikacija koji osiguravaju **bezbjednost, interoperabilnost i kvalitet** u digitalnom svijetu. Tekst objašnjava kako ovi standardi omogućavaju različitim sistemima i uređajima da funkcionišu usklađeno, naglašavajući ulogu vodećih međunarodnih organizacija poput **ISO, IEC i ETSI**. Poseban fokus stavljen je na zaštitu podataka, **sajber bezbjednost** i razvoj savremenih tehnologija kao što su **IoT, 5G mreže i cloud servisi**. Implementacija ovih normi olakšava inovacije i smanjuje troškove, dok istovremeno garantuje stabilnost informacionih sistema u svim sferama društva. Konačno, brošura služi kao vodič za razumijevanje temelja na kojima počiva **pouzdana i moderna digitalna transformacija**.

Značaj ICT standarda

ICT standardi predstavljaju temelj savremenih informaciono-komunikacionih tehnologija. Zahvaljujući radu međunarodnih (ISO, IEC, ITU i IEEE) i evropskih organizacija (ETSI, CENELEC, CEN) omogućena je interoperabilnost sistema, bezbjedna komunikacija i razvoj novih digitalnih tehnologija. Primjena ovih standarda doprinosi kvalitetu, sigurnosti i održivom razvoju digitalnog društva.



ICT standardi (Information and Communication Technology standards) predstavljaju skup pravila, preporuka i tehničkih specifikacija koje omogućavaju da različiti digitalni sistemi, uređaji, mreže i softver rade zajedno na pouzdan, bezbjedan i kompatibilan način.

Standardi imaju veoma široku primjenu i prisutni su u gotovo svim oblastima savremenog društva i to: računarske mreže i internet, informaciona bezbjednost, razvoj softvera, telekomunikacije, cloud tehnologije i data centri, elektronsko poslovanje, zdravstvo, obrazovanje, industrija...

Njihova primjena omogućava:

- **Interoperabilnost** – različiti uređaji i sistemi mogu međusobno da komuniciraju;
- **Kompatibilnost** – softver i hardver različitih proizvođača funkcionišu zajedno;
- **Bezbjednost** – zaštita podataka, mreža i korisnika;
- **Kvalitet usluga** – pouzdan i stabilan rad informacionih sistema;
- **Lakše održavanje i razvoj** – standardizovana rješenja olakšavaju nadogradnje i integracije.

Razvoj ICT standarda



Međunarodne organizacije zadužene za standardizaciju **ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission)** razvijaju veliki broj ICT standarda u okviru zajedničkog tehničkog komiteta ISO/IEC JTC 1 – Informacione tehnologije.



Na evropskom nivou postoje **CEN/CENELEC (European Committee for Standardization / European Committee for Electrotechnical Standardization)** stručna tijela koja se bave standardizacijom u oblasti ICT npr. CEN/CLC/JTC 13.



Pored toga, **ETSI (European Telecommunications Standards Institute)** kao evropska organizacija razvija ICT standarde za sljedeće oblasti: internet stvari (IoT), sajber bezbjednost, vještačku inteligenciju, digitalni identitet, pametne gradove itd.

CENELEC razvija ICT standarde koji se odnose na: Sajber bezbjednost (Cybersecurity), Elektromagnetnu kompatibilnost (EMC), Bezbjednost električne i elektronske opreme, Pametne elektroenergetske mreže, Pametne gradove, IoT, Data centre, Električna vozila, Vještačku inteligenciju i digitalnu transformaciju itd. Preklapanja po pitanju standardizacije kod CENELEC i ETSI su prisutna u sljedećim oblastima: pametne mreže (Koordinaciona grupa CEN-CENELEC-ETSI za pametne energetske mreže), sajber bezbjednost (zajedničke konferencije sa EU agencijom), pametni gradovi i Internet stvari (IoT), električna vozila, data centri...

ICT standardi omogućavaju:

- bezbjednu razmjenu podataka,
- kompatibilnost uređaja različitih proizvođača,
- pouzdan rad informacionih sistema,
- međunarodnu saradnju,
- razvoj inovacija,
- zaštitu korisnika,
- smanjenje troškova razvoja.



Svaka država na nacionalnom nivou usvaja standarde iz svih oblasti pa, naravno, i iz ICT područja i oni moraju biti usklađeni sa međunarodnim i evropskim. U Crnoj Gori to je u nadležnosti Instituta za standardizaciju i njegovih Tehničkih komiteta (ISME/TK E 013 – Informacione tehnologije). Kao proizvod takve hijerarhijske strukture iz ove oblasti su ključni sledeći standardi:

- **MEST EN ISO/IEC 27001:2024*** - Bezbjednost informacija, sajber bezbjednost i zaštita privatnosti – Sistemi menadžmenta bezbjednošću informacija – Zahtjevi
- **MEST EN ISO/IEC 15408-1:2025** - Bezbjednost informacija, sajber bezbjednost i zaštita privatnosti – Kriterijumi za vrednovanje bezbjednosti u IT – Dio 1: Uvod i opšti model
- **MEST EN ISO/IEC 15408-2:2025** - Bezbjednost informacija, sajber bezbjednost i zaštita privatnosti – Kriterijumi za vrednovanje bezbjednosti u IT – Dio 2: Funkcionalne komponente za bezbjednost
- **MEST ISO/IEC 20000-1:2019** - Informacione tehnologije - Upravljanje uslugama - Dio 1: Zahtjevi sistema upravljanja uslugama

U oblasti sajber bezbjednosti ETSI je donio standard koji je na nacionalnom nivou u Crnoj Gori usvojen kao:

- **MEST EN 303 645 V3.1.3:2026** - Sajber-prostor - Sajber-sigurnost za internet stvari koji je namijenjen potrošačima - Osnovni zahtjevi



***Primjer: MEST EN ISO/IEC 27001:2024**

- MEST - Oznaka nacionalnog standarda. Svi crnogorski standardi imaju oznaku MEST.
- EN - Oznaka evropskog standarda. European Norm. Svi evropski standardi imaju oznaku EN.
- ISO/IEC - Oznaka međunarodnog standarda. Svi međunarodni standardi imaju oznaku ISO ili IEC. Ukoliko sadrži obje oznake onda se radi o saradnji međunarodnih organizacija za standardizaciju koje su izdale zajednički standard ISO/IEC.
- 27001 - Brojčana oznaka standarda (projekta).
- 2024 - Godina izdanja standarda. Ukoliko nije navedena, po pravilima standardizacije, misli se na trenutno važeće izdanje.

Primjeri primjene ICT standarda

ICT standardi se često dijele na **osnovne, najčešće zahtijevane i specijalizovane** standarde, u zavisnosti od njihove namjene i oblasti primjene.

Osnovni ICT standardi bi bili:

- **MEST EN ISO/IEC 27001:2024** - Bezbjednost informacija, sajber bezbjednost i zaštita privatnosti – Sistemi menadžmenta bezbjednošću informacija – Zahtjevi
- **MEST ISO/IEC 20000-1:2019** - Informacione tehnologije - Upravljanje uslugama - Dio 1: Zahtjevi sistema upravljanja uslugama
- **MEST ISO/IEC 20000-2:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 2: Uputstvo za primjenu sistema upravljanja uslugama
- **MEST ISO/IEC 20000-3:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 3: Uputstvo za definiciju područja i primjene i primjenjivosti standarda ISO/IEC 20000-1
- **MEST ISO/IEC TR 20000-7:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 7: Smjernice za integraciju i korelaciju ISO/IEC 20000-1: 2018 sa ISO 9001: 2015 i ISO/IEC 27001: 2013
- **MEST EN IEC 62443-2-1:2025** - Bezbjednost sistema za industrijsku automatizaciju i upravljanje – Dio 2-1: Zahtjevi programa bezbjednosti za vlasnike IACS imovine
- **MEST CLC IEC/TS 62443-1-5:2025** - Bezbjednost sistema za industrijsku automatizaciju i upravljanje – Dio 1-5: Šema za IEC 62443 bezbjednosne profile
- **MEST EN IEC 62443-2-4:2025** - Bezbjednost sistema za industrijsku automatizaciju i kontrolu – Dio 2-4: Zahtjevi programa bezbjednosti za provajdere IACS usluga
- **MEST CLC IEC/TS 62443-6-1:2026** - Bezbjednost sistema za industrijsku automatizaciju i upravljanje – Dio 6-1: Metodologija vrednovanja bezbjednosti prema IEC 62443-2-4
- **MEST EN IEC 62443-4-1:2019** - Bezbjednost sistema za industrijsku automatizaciju i kontrolu – Dio 4-1: Zahtjevi za bezbjedan razvoj životnog vijeka proizvoda

- **MEST EN IEC 62443-3-3:2020** - Industrijske komunikacione mreže – Bezbjednost mreže i sistema – Dio 3-3: Zahtjevi za bezbjednost sistema i nivoi bezbjednosti
- **MEST EN IEC 62443-4-2:2021** - Bezbjednost za industrijsku automatizaciju i kontrolne sisteme – Dio 4-2: Tehnički bezbjednosni zahtjevi za IACS komponente
- **MEST EN IEC 62443-3-2:2021** - Bezbjednost sistema za industrijsku automatizaciju i upravljanje – Dio 3-2: Ocjenjivanje bezbjednosnih rizika i projektovanje sistema
- **MEST ETSI EN 319 401 V3.1.1:2026** - Elektronski potpisi i infrastrukture (ESI); Opšti zahtjevi koje moraju da ispune pružaoci usluga od povjerenja
- **MEST EN 303 645 V3.1.3:2026** - Sajber-prostor - Sajber-sigurnost za internet stvari koji je namijenjen potrošačima - Osnovni zahtjevi

Najčešće zahtijevani ICT standardi bi bili:

- **MEST EN ISO/IEC 27001:2024** - Bezbjednost informacija, sajber bezbjednost i zaštita privatnosti – Sistemi menadžmenta bezbjednošću informacija – Zahtjevi
- **MEST ISO/IEC 20000-1:2019** - Informacione tehnologije - Upravljanje uslugama - Dio 1: Zahtjevi sistema upravljanja uslugama
- **MEST ISO/IEC 20000-2:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 2: Uputstvo za primjenu sistema upravljanja uslugama
- **MEST ISO/IEC 20000-3:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 3: Uputstvo za definiciju područja i primjene i primjenjivosti standarda ISO/IEC 20000-1
- **MEST ISO/IEC TR 20000-7:2020** - Informacione tehnologije - Upravljanje uslugama - Dio 7: Smjernice za integraciju i korelaciju ISO/IEC 20000-1: 2018 sa ISO 9001: 2015 i ISO/IEC 27001: 2013
- **MEST EN ISO 9001:2016** - Sistemi menadžmenta kvalitetom – Zahtjevi
- **MEST EN ISO 22301:2020** - Bezbjednost i otpornost - Sistemi menadžmenta kontinuitetom poslovanja – Zahtjevi
- **MEST EN ISO/IEC 27701:2026** - Bezbjednost informacija, sajber-bezbjednost i zaštita privatnosti – Sistemi menadžmenta informacijama o privatnosti – Zahtjevi i smjernice (ISO/IEC 27701:2025)

- **MEST ETSI EN 319 401 V3.1.1:2026** - Elektronski potpisi i infrastrukture (ESI); Opšti zahtjevi koje moraju da ispune pružaoci usluga od povjerenja
- **MEST EN 303 645 V3.1.3:2026** - Sajber-prostor - Sajber-sigurnost za internet stvari koji je namijenjen potrošačima - Osnovni zahtjevi

Specijalizovani ICT standardi su:

- **MEST EN ISO/IEC 27017:2023** - Informacione tehnologije – Tehnike bezbjednosti – Pravilo dobre prakse za kontrole bezbjednosti informacija zasnovane na ISO/IEC 27002 za usluge u kladu
- **MEST EN ISO/IEC 27018:2022**– Informacione tehnologije – Tehnike bezbjednosti – Pravilo dobre prakse za zaštitu ličnih identifikacionih informacija (PII) u javnom kladu u kojem se vrši obrada ličnih identifikacionih informacija (PII)
- **MEST EN 300 328 V2.2.2:2023** – Širokopojasni prenosni sistemi; Uređaji za prenos podataka koji rade u ISM pojasu na 2,4 GHz; Harmonizovani standard za pristup radio spektru
- **MEST EN 301 489-20 v2.2.1:2025** - Standard elektromagnetne kompatibilnosti (EMC) za radio opremu i usluge; Dio 20: Specifični uslovi za mobilne zemaljske stanice (MES) koje se koriste u mobilnim satelitskim uslugama (MSS); Harmonizovani standard za elektromagnetnu kompatibilnost
- **MEST EN 303 645 V3.1.3:2026** - Sajber-prostor - Sajber-sigurnost za internet stvari koji je namijenjen potrošačima - Osnovni zahtjevi

Zaključak

ICT standardi predstavljaju temelj savremenih informaciono-komunikacionih tehnologija. Njihova primjena omogućava da računarski sistemi, mreže i softverske aplikacije različitih proizvođača rade zajedno na siguran, pouzdan i efikasan način. Danas se koriste u gotovo svim oblastima – od obrazovanja, zdravstva i industrije, preko telekomunikacija i bankarstva, do državne uprave i svakodnevne upotrebe interneta. Zbog toga su ICT standardi ključni za razvoj digitalnog društva, unapređenje poslovanja i sigurnu razmjenu informacija na globalnom nivou.

ICT standardi su nevidljivi stubovi na kojima počiva naša digitalna budućnost. Oni pretvaraju izolovanu tehnologiju u globalno povezan sistem, garantujući da svaka razmjena podataka bude bezbjedna, a svaki uređaj interoperabilan. U svijetu koji se neprestano mijenja, ovi standardi nijesu samo tehnička pravila, već ključ za izgradnju povjerenja, inovacija i održivog digitalnog društva.



THE CONSORTIUM

