



Institut za ekonomsku diplomatiju vas poziva na praktičnu radionicu

Obavezna obuka zaposlenih prema Zakonu o informacionoj bezbednosti

OBAVEZNA EDUKACIJA ZAPOSLENIH UZ PROVERU STEČENOG ZNANJA - OBUČITE KORISNIKE I OSPOSOBITE INTERNE PREDAVAČE

Arhiv Jugoslavije, 20. oktobar 2026. godine od 10h

Novi Zakon o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025) donosi značajne promene u oblasti zaštite IKT sistema i jasno postavlja informacionu bezbednost kao odgovornost koja se ne završava u IT sektoru. Iz tog razloga, uvodi se obavezna obuka zaposlenih za pouzdano i bezbedno korišćenje informacionih sistema.

Član 10. tačka 4. Zakona propisuje **OBAVEZU OPERATORA IKT SISTEMA DA OBEZBEDI DA LICA KOJA KORISTE ILI UPRAVLJAJU IKT SISTEMOM BUDU OSPOSOLJENA** za poslove koje obavljaju i razumeju svoju odgovornost. Obavezna obuka zaposlenih je **jedna od zakonom propisanih mera zaštite IKT sistema**.

A KO SU ZAPRAVO “LICA KOJA KORISTE ILI UPRAVLJAJU IKT SISTEMOM”?

IKT sistem nije samo server, programiranje, kod, IT infrastruktura ili posao sistem-administratora. **Korisnici IKT sistema nisu samo zaposleni u IT sektoru**. Ukoliko u obavljanju svog posla imaju pristup IKT sistemima organizacije, obavezom edukacije mogu biti obuhvaćeni zaposleni u:

administraciji • računovodstvu • finansijama • ljudskim resursima • sekretarijatu • pravnoj službi • komercijali • prodaji • nabavci • marketingu • korisničkoj podršci • logistici • menadžmentu, kao i druga zaposlena i angažovana lica.

A pristup IKT sistemu može podrazumevati korišćenje:

službenog računara ili laptopa • poslovnog e-maila • Microsoft 365 ili Google Workspace okruženja • ERP ili CRM sistema • SEF-a • ePoreza • eUprave • elektronskog bankarstva • elektronske pisarnice • DMS-a • cloud servisa • poslovnih baza podataka • mrežnih resursa • internih poslovnih aplikacija i drugih digitalnih resursa organizacije.

Dakle, obaveza edukacije nije ograničena na zaposlene koji „rade u IT-u“. U savremenom poslovnom okruženju pristup nekom obliku IKT sistema ima veliki deo, a u mnogim organizacijama gotovo svi zaposleni.

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs



Kao korisnici IKT sistema, polaznici će biti osposobljeni da:

- razumeju svoje obaveze i odgovornosti u bezbednom korišćenju IKT sistema;
- **primenjuju osnovna pravila informacione i sajber bezbednosti** u svakodnevnom radu;
- prepoznaju phishing, vishing, ransomware, socijalni inženjering i druge najčešće sajber pretnje;
- pravilno koriste lozinke, poslovni e-mail i druge IKT resurse;
- prepoznaju sumnjive događaje i potencijalne bezbednosne incidente;
- **znaju šta treba odmah da urade, kome da prijave incident i šta ne smeju da rade samoinicijativno;**
- **provere stečeno znanje kroz završno testiranje.**

Istovremeno, polaznici koji su u svojim organizacijama zaduženi za informacionu bezbednost, usklađenost ili edukaciju zaposlenih biće osposobljeni da:

- obavezna obuka zaposlenih bude interno sprovedena;
- prenesu zaposlenima praktična pravila bezbednog korišćenja IKT resursa;
- upoznaju ih sa njihovim obavezama i odgovornostima;
- pripreme ih za pravilno postupanje u slučaju incidenta;
- organizuju proveru usvojenog znanja;
- dokumentuju sprovedenu edukaciju.

Obuka je, dakle, namenjena kako zaposlenima koji treba da steknu znanja neophodna za bezbedno korišćenje IKT sistema, tako i licima koja će stečena znanja dalje prenositi i organizovati edukaciju u svojim organizacijama. ZADRŽAVANJEM ZNANJA I EKSPERTIZE UNUTAR ORGANIZACIJE smanjuje se potreba za angažovanjem eksternih saradnika za svaku narednu internu edukaciju zaposlenih.

PROGRAM OBUKE

1) NOVI ZAKON O INFORMACIONOJ BEZBEDNOSTI – ŠTA SE MENJA?

- ključne izmene Zakona o informacionoj bezbednosti za 2025/2026. godinu;
- ko su obveznici novog Zakona – prioritetni i važni subjekti;
- mere zaštite IKT sistema;
- obavezna edukacija zaposlenih koji imaju pristup IKT sistemima;
- odgovornost menadžmenta;
- uloga lica odgovornih za informacionu bezbednost;
- **matrica odgovornosti: direktor – CISO – IT menadžer – administrator – zaposleni;**
- odgovornost i kazne za rukovodioce;
- informaciona bezbednost kao odgovornost cele organizacije, a ne samo IT sektora.



2) SAVREMENE SAJBER PRETNJE – KAKO DANAS IZGLEDA NAPAD?

- **Ransomware i Ransomware-as-a-Service;**
- **Phishing;**
- **Vishing;**
- **Whaling** – napadi usmereni na rukovodioce;
- socijalni inženjering;
- AI botovi i njihova zloupotreba;
- **deepfake napadi;**
- DDoS napadi;
- napadi na veb-aplikacije;
- indikatori kompromitacije sistema;
- aktuelni trendovi i statistika incidenata u Srbiji.

3) KAKO SE BRANIMO?

- **MFA – multifaktorska autentifikacija;**
- bezbedno kreiranje i korišćenje kompleksnih lozinki;
- backup;
- **Zero Trust model;**
- svakodnevna bezbednosna higijena zaposlenih.

4) „PRVIH 10 MINUTA“ – ŠTA ZAPOSLENI MORA DA URADI KADA SE DOGODI INCIDENT?

Šta se događa kada zaposleni klikne na sumnjiv link, otvori zaraženi prilog, primeti anomaliju u sistemu ili posumnja da je njegov nalog kompromitovan?

- prepoznavanje incidenta;
- prvi koraci zaposlenog;
- šta zaposleni treba odmah da uradi;
- šta **ne sme da radi samoinicijativno;**
- kome prijavljuje sumnjivi događaj;
- interna eskalacija;
- lanac obaveštavanja;
- odgovornost zaposlenog;
- uloga CISO-a, IT menadžera, administratora i rukovodstva;
- pravila ponašanja tokom trajanja incidenta ili veće krize.

5) KOME, KADA I KAKO SE PRIJAVLJUJE INCIDENT?

- obaveštavanje eksternih institucija;
- Nacionalni CERT;
- rokovi za prijavljivanje;
- Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti;
- Narodna banka Srbije;
- postupanje kada incident uključuje podatke o ličnosti;
- procedura obaveštavanja građana u slučaju curenja podataka.

6) BEZBEDNOSNA KULTURA – PRAVILA KOJA ZAPOSLENI MORA DA ZNA

- pravila za kreiranje i korišćenje lozinki;
- bezbedno korišćenje poslovnog e-maila;

Informacije: 011/3077612, 3077613, 063/509972;

prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;

www.economicdiplomacy.co.rs



- prepoznavanje sumnjivih poruka i zahteva;
- pravila korišćenja IKT resursa;
- bezbednost opreme koja ostaje bez nadzora;
- pravilo „čistog stola“;
- zaštita poslovnih i poverljivih podataka;
- odgovornost zaposlenih za zloupotrebu IKT resursa;
- „Lista dužnosti korisnika IKT resursa“;
- obaveze iz Ugovora o neotkrivanju podataka trećim licima (NDA);
- pravila i odgovornosti u vezi sa zaštitom podataka o ličnosti.

7) KAKO ORGANIZOVATI OBUKU ZAPOSLENIH U SOPSTVENOJ ORGANIZACIJI?

Poseban fokus biće na tome kako stečeno znanje preneti zaposlenima i primeniti ga u sopstvenoj organizaciji. Polaznici će biti pripremljeni da zaposlene upoznaju sa:

- osnovnim sajber rizicima;
- pravilima bezbednog korišćenja IKT sistema;
- odgovornošću svakog korisnika;
- prepoznavanjem phishing, vishing i drugih oblika socijalnog inženjeringa;
- pravilnim postupanjem u slučaju incidenta;
- internim lancem obaveštavanja;
- pravilima korišćenja poslovnih IKT resursa;
- obavezom zaštite poverljivih podataka.

8) DOKUMENTOVANJE SPROVEDENE EDUKACIJE

Sprovođenje edukacije treba da bude praćeno odgovarajućom dokumentacijom kojom organizacija može da evidentira i potvrdi preduzete aktivnosti.

- evidencije sprovedenih obuka;
- evidencije prisustva zaposlenih;
- programa i materijala korišćenih tokom edukacije;
- dokumentovanja sprovedene provere znanja;
- rezultata testiranja;
- dokumentacije kojom se potvrđuju aktivnosti na kontinuiranoj edukaciji zaposlenih.

PRAKTIČNI DEO – PROVERA ZNANJA

Obavezna obuka zaposlenih se završava **proverom usvojenog znanja**.

Test obuhvata ključne oblasti obrađene tokom obuke:

- odgovornost menadžmenta i zaposlenih;
- prepoznavanje phishing i drugih sajber pretnji;
- ransomware;
- bezbedno korišćenje IKT resursa;
- postupanje u slučaju incidenta;
- interni protokol i lanac obaveštavanja.

Testiranje omogućava učesnicima da provere koliko su osposobljeni da prepoznaju rizik i pravilno reaguju u konkretnoj situaciji.

Informacije: 011/3077612, 3077613, 063/509972;

prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;

www.economicdiplomacy.co.rs



Učesnicima koji uspešno završe obuku i proveru znanja izdaje se **sertifikat o uspešno završenoj obuci iz oblasti informacione bezbednosti**.

KOME JE OBUKA NAMENJENA?

Obavezna obuka zaposlenih je namenjena svima koji imaju pristup IKT sistemima, a posebno zaposlenima u:

administraciji • računovodstvu • finansijama • ljudskim resursima • sekretarijatu • pravnoj službi • komercijali • prodaji • nabavci • marketingu • korisničkoj podršci • logistici • menadžmentu, kao i drugim zaposlenima koji u svakodnevnom radu koriste IKT resurse organizacije.

Obuka je istovremeno posebno značajna za lica koja su odgovorna za organizovanje, sprovođenje i kontrolu informacione bezbednosti i edukaciju drugih zaposlenih:

direktore i rukovodioce • CISO i druga lica odgovorna za informacionu bezbednost • IT menadžere i administratore • pravne i compliance službe • lica za zaštitu podataka o ličnosti (DPO) • interne revizore informacione bezbednosti, kao i druga lica zadužena za sprovođenje internih obuka.

Predavačica:

Dragana Jakovljević, ekspertkinja za informacionu bezbednost i upravljanje rizicima

Specijalista je za transformaciju kompleksnih teorijskih i regulatornih zahteva u praktične operativne procedure, sa dugogodišnjim iskustvom u oblasti informacione bezbednosti i upravljanja rizicima.

Poseban fokus njenog rada je na primeni mera koje doprinose kontinuitetu poslovanja, razvoju bezbednosne kulture i dokumentacionoj spremnosti organizacije za proveru usklađenosti i inspeksijski nadzor.

NAPOMENA: Polaznicima će biti obezbeđene prezentacije i materijali u elektronskom obliku.

Način realizacije, kotizacija i popusti

Obuka se realizuje isključivo u nastavnoj sali, zbog izrazite interaktivnosti predavanja, u jednom od **najlepših i najreprezentativnijih zdanja starog Beograda – Arhivu Jugoslavije**. Smeštena u monumentalnoj zadužbini kralja Aleksandra I Karađorđevića iz 1933. godine, zgrada je proglašena spomenikom kulture i predstavlja jedno od najznačajnijih ostvarenja beogradske međuratne arhitekture.

Posebnu atmosferu daje i prostrani park koji okružuje kompleks, pa će učesnici tokom pauze imati priliku da uživaju u jednom od najlepših zelenih ambijenata ovog dela grada, a po želji i da obiđu aktuelnu izložbu Arhiva Jugoslavije i deo bogatog kulturno-istorijskog nasleđa koje ova ustanova čuva.

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs



Kotizacija iznosi 25.800,00 (+PDV) i obuhvata nastavu, nastavni materijal, odgovore na pitanja, proveru usvojenog znanja, sertifikat o odslušanoj obuci, kao i posluženje u pauzama

Popusti:

- **Za sve prijave** odobravamo popust od 5%
- **Za dva i više učesnika** iz iste organizacije, odobravamo dodatnih 10% popusta.
- **Za učesnike naših prethodnih obuka iz oblasti IKT bezbednosti**, odobravamo dodatnih 5% popusta.

Informacije i prijavljivanje:

Prijavu možete izvršiti klikom na dugme "Prijavite se" gde možete popuniti elektronsku prijavu ili preuzeti obrazac u .doc formatu i poslati ga na bilo koju od naših e-mail adresa

Za dodatne informacije kontaktirajte nas na:

011/3077612, 3077613, 063/509972

prijava@economicdiplomacy.co.rs

ied.bg@mts.rs

Informacije: 011/3077612, 3077613, 063/509972;
prijava@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs