SYM-OP-IS 2025
52. Simpozijum o operacionim istraživanjima
Palić, 7 - 10.9.2025.

UNIVERZITET U BEOGRADU
FAKULTET ORGANIZACIONIH NAUKA

Originalni članak **https://doi.org/10.5281/zenodo.17534411**

ANALIZA SAJBER RIZIKA PORTALA EUPRAVA KORIŠĆENJEM OCTAVE ALLEGRO PRISTUPA

ANALYZING CYBERSECURITY RISKS OF THE SERBIAN EGOVERNMENT PORTAL THROUGH OCTAVE ALLEGRO

ANDRIJANA DŽAMIĆ[1], ISIDORA GAĆEŠA[2], DRAGANA MAKAJIĆ-NIKOLIĆ[3]

[1] Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, andrijana.dzamic@fon.bg.ac.rs, 0000-0002-6398-4495
[2] Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, isidora.gacesa@fon.bg.ac.rs, 0009-0002-0907-7170
[3] Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, dragana.makajic-nikolic@fon.bg.ac.rs, 0000-0002-0790-6791

Rezime: *U radu je sprovedena analiza sajber rizika portala eUprava Republike Srbije korišćenjem metodologije OCTAVE Allegro. Kroz četiri faze ove metodologije identifikovani su ključni elementi informacione imovine, pretnje i ranjivosti, kao i njihova verovatnoća i posledice. Poseban akcenat stavljen je na tehničke mere zaštite i njihov uticaj na funkcionisanje kritične infrastrukture i poverenje građana. Analizom je izdvojeno više scenarija rizika, pri čemu su kao najkritičniji identifikovani DoS napadi i prenos podataka bez enkripcije. Na osnovu procene, predložene su konkretne mere smanjenja rizika. Rad ukazuje na potencijal OCTAVE Allegro pristupa kao korisnog alata u unapređenju sajber bezbednosti javnih digitalnih servisa.*

Ključne reči: *Sajber bezbednost, eUprava, Analiza rizika, OCTAVE Allegro.*

Abstract: *This paper presents a cybersecurity risk analysis of the Serbian eGovernment portal using the OCTAVE Allegro methodology. Through four phases, key elements of information assets, threats, and vulnerabilities were identified, along with their likelihood and potential impact. The analysis focused on technical security measures and their influence on the functioning of critical infrastructure and public trust. It also identified several critical risk scenarios, including DoS attacks and unencrypted data transmission. Based on the assessment, specific risk mitigation measures were proposed. The study highlights the potential of the OCTAVE Allegro approach as a valuable tool for improving cybersecurity in public digital services.*

Keywords: *Cybersecurity, eGovernment, Risk Analysis, OCTAVE Allegro.*

1. UVOD

Razvoj informacionih tehnologija i digitalizacija društva doneli su značajne koristi, ali i nove rizike, naročito u domenu sajber bezbednosti. Zavisnost institucija od digitalnih sistema izlaže ih stalnim pretnjama koje mogu ugroziti kritičnu infrastrukturu i zaštitu podataka (ENISA Threat Landscape, 2023). U tom kontekstu, posebno je važno razmatrati rizike najveće digitalne platforme javne uprave Republike Srbije, portala eUprava.

Jedan od ključnih izazova jeste održavanje balansa između dostupnosti usluga i bezbednosti. Efikasna e-usluga zahteva brz odziv i poverenje građana, ali i doslednu primenu mehanizama zaštite (Bada, Sasse & Nurse, 2020). Privatni sektor u tom pogledu brže uvodi savremene digitalne prakse, dok javni sektor često kasni zbog regulatornih procedura, nedostatka stručnjaka i ograničenih resursa, što ga čini posebno ranjivim na napade motivisane političkim ili strateškim ciljevima (Mushi, 2023). Prema *CyberPeace* institutu (2023), broj napada na državne servise u Evropi porastao je za 30% u odnosu na 2022, a najčešće mete su portali koji obrađuju lične podatke građana.

OECD (2021) i Paigude (2024) ukazuju da javni sektor često nema jasne strategije i protokole zaštite, dok problemi poput zastarele infrastrukture i niske svesti zaposlenih dodatno otežavaju reakciju na incidente. Istovremeno, digitalna transformacija i sve šira primena veštačke inteligencije uvode nove rizike, uključujući manipulaciju algoritmima i automatizaciju sajber napada (United Nations E-Government Survey, 2024).

U literaturi se ističu preporuke za unapređenje bezbednosti javne uprave kroz nacionalne okvire, centralizovanu koordinaciju, timove za brzo reagovanje i modernizaciju tehničkih mera poput enkripcije i višefaktorske autentifikacije (Mushtaq & Shah, 2024; Schneider, 2025). OECD (2021) naglašava da sajber bezbednost mora biti stub, a ne dodatna komponenta digitalne transformacije.

Prema ITU izveštaju (2024), Srbija je ocenjena kao uzorna zemlja sa indeksom sajber bezbednosti od 96,82, naročito u oblasti pravnih normi i međunarodne saradnje. Ipak, oblast tehničkih mera ostaje najniže ocenjena i predstavlja prostor za dalja unapređenja. U tom smislu, cilj rada je da primenom OCTAVE Allegro metodologije predloži pristup za procenu sajber rizika portala eUprava i ponudi konkretne tehničke i organizacione preporuke u svrhu smanjenja pretnji.

2. TEHNIČKE MERE U DOMENU PREVENCIJE SAJBER PRETNJI

Tehničke mere u sajber bezbednosti obuhvataju tehnologije, procedure i metode kojima se štite informacioni sistemi od različitih pretnji. Njihova svrha je očuvanje osnovnih principa poverljivosti, integriteta i dostupnosti (CIA trijada), kao i zaštita privatnosti korisnika i njegovih podataka (Shostack, 2020; ENISA Threat Landscape, 2023). Efikasnost mera zavisi od njihove dosledne primene tokom celog životnog ciklusa informacionog sistema, od dizajna, implementacije i održavanja, do evaluacije i prenosa stečenih iskustava u nove prakse.

Spektar mera je širok i uključuje kontrolu pristupa, identifikaciju i autentifikaciju, enkripciju, detekciju zlonamernog softvera, kao i bezbednosno logovanje i reviziju. Kontrola pristupa obezbeđuje da samo ovlašćeni korisnici imaju pristup resursima, koristeći mehanizme poput RBAC-a, VPN-a i IP filtera. Identifikacija i autentifikacija podrazumevaju lozinke, biometriju i višefaktorsku autentifikaciju (MFA), dok enkripcija štiti podatke u prenosu i mirovanju primenom TLS/SSL protokola, kriptografskih ključeva i digitalnih potpisa. Detekcija zlonamernog softvera sprovodi se kroz antivirusne alate, kontinuirano skeniranje i integraciju sa SIEM sistemima, dok logovanje i revizija omogućavaju praćenje aktivnosti, forenzičku analizu i brzu reakciju na incidente.

U skladu sa preporukama NIST-a (2023) i ENISA-e (2023), ove mere čine osnovu za sistemsku zaštitu informacionih resursa, a njihova primena treba da bude integrisana u sve faze rada javnih digitalnih servisa. Time se obezbeđuje otpornost sistema i minimiziraju posledice eventualnih incidenata.

3. PROCES UPRAVLJANJA RIZIKOM

Prema ISO 31000 standardu, upravljanje rizikom obuhvata tri koraka: (1) ***uspostavljanje konteksta***, gde se analiziraju strateški i organizacioni faktori, (2) ***procenu rizika***, kojom se identifikuju i analiziraju rizični događaji i definišu prioriteti i (3) ***tretman rizika***, koji obuhvata mere smanjenja, prenosa, tolerisanja ili uklanjanja rizika (ISO, 2018; Makajić-Nikolić, 2022). Proces je kontinuiran i integrisan u poslovanje, dok se faza procene rizika ponavlja nakon svake značajne promene ili implementacije mera (Björnsdóttir et al., 2022).

Procena rizika ima ključnu ulogu jer omogućava prepoznavanje potencijalnih događaja, procenu verovatnoće i posledica, te određivanje prioriteta delovanja. Realizuje se kroz tri faze: identifikaciju, analizu i evaluaciju rizika (Makajić-Nikolić, 2022). U praksi se koriste različite kvalitativne, kvantitativne i kombinovane metode, a u ovom radu akcenat je na OCTAVE Allegro metodologiji.

3.1. OCTAVE Allegro metodologija

OCTAVE Allegro (*Operationally Critical Threat*, *Asset* and *Vulnerability Evaluation*) predstavlja fleksibilan i jasno strukturiran okvir namenjen kvalitativnoj i kvantitativnoj analizi rizika u sajber bezbednosti. Za razliku od ranijih verzija, OCTAVE i OCTAVE-S, koje su prvenstveno bile namenjene velikim organizacijama sa složenom infrastrukturom i razvijenim sistemima odgovornosti, OCTAVE Allegro je oblikovan tako da bude primenljiv u organizacijama svih veličina, uključujući i one manje koje nemaju napredne bezbednosne strukture.

Metodologija se zasniva na osam koraka grupisanih u četiri faze: (1) definisanje kriterijuma uticaja, (2) profilisanje imovine, (3) identifikacija pretnji kroz realistične scenarije i (4) analiza i izbor mera na osnovu procene verovatnoće i posledica (Caralli et al., 2007; Aryanti et al., 2023). Na taj način kvalitativne procene dobijaju kvantitativni okvir, što omogućava jasniju sliku o pretnjama i prioritetima delovanja.

Prednost OCTAVE Allegro pristupa je i radionički karakter njegove primene. Implementaciju dodatno olakšava postojanje predefinisanih radnih listova i obrazaca, dostupnih već gotovo dve decenije, što ubrzava sprovođenje metodologije čak i u institucijama bez specijalizovanih timova za informacionu bezbednost (Caralli et al., 2007; Zafar et al., 2022).

4. SAJBER BEZBEDNOST EUPRAVE: OCTAVE ALLEGRO ANALIZA

4.1. Faza 1: Utvrđivanje kriterijuma za merenje rizika

Prva faza primene OCTAVE Allegro metodologije podrazumeva identifikovanje i rangiranje kritičnih područja uticaja (Tabela 2) sajber rizika na nacionalnom nivou Republike Srbije, sa fokusom na tehničke mere i uticaj na vitalne funkcije države, institucija i činilaca javnog poverenja.

Tabela 1: Kritična područja uticaja (utvrđeno prema (ITU,2024))

Prioritet	***Područje uticaja***
1	Funkcionisanje kritične infrastrukture
2	Reputacije države i poverenje javnosti
3	Međunarodna usklađenost i uključenost
4	Finansijski aspekt
5	Održivost i kapacitet odgovora institucija

Najviši prioritet u procesu identifikacije kritičnih područja uticaja dodeljen je funkcionisanju kritične infrastrukture, jer kompromitovanje digitalnih javnih servisa može ugroziti osnovna prava građana i kontinuitet rada institucija. Drugi rang zauzimaju reputacija države i poverenje javnosti, budući da svaki incident, poput curenja podataka ili prekida usluga, direktno narušava kredibilitet javne uprave i međunarodni imidž. Treći prioritet odnosi se na međunarodnu usklađenost i uključenost, jer neusklađenost sa bezbednosnim i tehničkim standardima može ograničiti saradnju i ugroziti digitalni suverenitet. Niže rangirani, ali i dalje značajni faktori su finansijski aspekt i institucionalna održivost, koji se posmatraju kao sekundarni u odnosu na direktne rizike po dostupnost, integritet i poverenje. U svrhu kvalitativne procene kreirana je tabela za svako od područja uticaja, pri čemu Tabela 2 ilustruje jedno od kritičnih područja kao primer daljeg sistematskog razmatranja.

Tabela 2: Funkcionisanje kritične infrastrukture

KRITERIJUM ZA MERENJE RIZIKA - Funkcionisanje kritične infrastrukture			
Područje uticaja	*Nisko*	*Srednje*	*Visoko*
Pristup javnim e-uslugama	Dolazi do kraćih prekida pristupa pojedinim e-servisima, ali građani mogu izvršiti ključne obaveze alternativnim putem.	Višednevni prekidi pristupa eUpravi utiču na registracije, uverenja, poreske obaveze, te tako nastaje institucionalna zagušenost.	Potpuni prekid funkcionisanja sistema eUprave paralizuje administrativni aparat i onemogućava ostvarivanje osnovnih prava građana.
Pravna sigurnost i evidencija	Pojedini podaci su privremeno nedostupni, ali su bezbedno očuvani i lako se obnavljaju.	Dolazi do delimičnog gubitka pristupa bazama ili ažuriranjima, što izaziva greške i kašnjenja u odlučivanju.	Gubitak ili kompromitovanje ključnih elektronskih zapisa narušava pravnu sigurnost i pokreće niz pravnih postupaka.
Institucionalna efikasnost	Smanjena efikasnost u pojedinim službama, ali se osnovne funkcije i dalje obavljaju.	Vidljiv pad u obradi zahteva i upravljanju dokumentima, uz rast frustracije korisnika.	Sistem administracije postaje nefunkcionalan; hitne intervencije se ne mogu sprovesti na vreme.
Upravljanje digitalnim procesima	Manje tehničke smetnje usporavaju obradu zahteva, ali se ne narušava kontinuitet rada.	Poremećaj u integraciji sektorskih sistema dovodi do neusklađenosti u radu i pogrešnih administrativnih radnji.	Potpuni kolaps digitalnog lanca uprave izaziva pravni, logistički i organizacioni haos na nacionalnom nivou.

4.2. Faza 2: Profilisanje imovine

Druga faza primene OCTAVE Allegro metodologije podrazumeva profilisanje imovine kroz tri podfaze:

a) Profilisanje informacione imovine. Identifikuju se i klasifikuju podaci i resursi od ključne vrednosti za eUpravu. Kritičnu imovinu čine: lični podaci građana, prebivalište i biračko pravo, poreski i finansijski podaci, imovinski podaci, podaci o obrazovanju i zaposlenju, lični i porodični status, pristupni podaci i autentifikacija, logovi i istorija aktivnosti, kao i metapodaci i tehnički zapisi. Svi oni zahtevaju visok stepen zaštite od neovlašćenog pristupa i zloupotrebe.

b) Identifikacija internih nosilaca. Uključuje entitete unutar sistema eUprave koji upravljaju i održavaju podatke. To su pre svega serveri baza podataka, aplikacioni serveri i sistem autentifikacije, unutrašnja mrežna infrastruktura (VPN, LAN), sistemi za logovanje i reviziju, rezervni medijumi (*backup*), kao i serveri za integraciju sa drugim institucijama (npr. RGZ, NBS).

c) Identifikacija eksternih nosilaca. Odnosi se na subjekte van eUprave koji imaju pristup kritičnoj imovini. Tu spadaju eksterni serverski sistemi i baze podataka, internet konekcija i DNS provajderi, eksterni web servisi, kao i sertifikacioni autoriteti koji izdaju digitalne sertifikate i omogućavaju elektronsko potpisivanje (KITEU, n.d.; ZZPL, 2018; Vlada RS, 2023).

4.3. Faza 3: Identifikacija pretnji

Treća faza OCTAVE Allegro metodologije podrazumeva prepoznavanje događaja i okolnosti koje mogu ugroziti informacioni sistem. Analiza je sprovedena kroz dve podfaze: (1) identifikaciju oblasti interesovanja i (2) definisanje scenarija pretnji.

Uzimajući u obzir složenost analiziranog sistema i veliki broj inicijalno identifikovanih oblasti, radi bolje preglednosti i efikasnijeg sprovođenja analize, one su klasifikovane u pet ključnih kategorija (prema ENISA, 2023):

- Pristup i kontrola pristupa - neadekvatna kontrola privilegija, zloupotreba administratorskih naloga, neovlašćen eksterni pristup.
- Autentifikacija i kredencijali - slabe lozinke, nedostatak MFA, krađa eID podataka, loše upravljanje sesijama.
- Zaštita podataka i privatnost - prenos podataka bez enkripcije, kompromitovanje logova, loše čuvanje rezervnih kopija.
- Eksterni napadi i mrežna bezbednost - DoS/DDoS, malver, ranjivi API-ji, presretanje komunikacije, phishing.
- Operativne i ljudske greške - greške zaposlenih, neusaglašene procedure, loše konfiguracije sistema.

Za svaku oblast definišu se scenariji sa potencijalnim posledicama: od modifikacije ili gubitka podataka, preko obelodanjivanja osetljivih informacija, do potpunog prekida rada sistema. U Tabeli 3 prikazan je primer po jedne oblasti interesovanja iz svake kategorije, zajedno sa odgovarajućim scenarijem i uticajem, što omogućava ilustraciju načina na koji se pretnje razrađuju u okviru OCTAVE Allegro metodologije.

Tabela 3: Primer oblasti interesovanja, scenarija i uticaja

Kategorija	***Oblast interesovanja (primer)***	***Scenario***	***Područje uticaja***
Pristup i kontrola pristupa	Neautorizovani pristup podacima	Zaposleni iz jedne institucije pristupa podacima druge putem eUprave bez ograničenja.	Obelodanjivanje podataka
Autentifikacija i kredencijali	Nedostatak MFA	Neovlašćeni akter koristi ukradene kredencijale i pristupa sistemu bez dodatne verifikacije.	Neautentifikovani pristup
Zaštita podataka i privatnost	Prenos podataka bez enkripcije	Podaci se razmenjuju u otvorenom tekstu, što omogućava napadaču da dođe u posed ličnih informacija.	Curenje podataka
Eksterni napadi i mrežna bezbednost	DoS napad	Server je preplavljen zahtevima i portal eUprava postaje nedostupan korisnicima.	Prekid rada
Operativne i ljudske greške	Greška pri unosu podataka	Ovlašćeno lice greškom unosi netačne podatke u sistem, što dovodi do pogrešnih poreskih obaveza.	Modifikacija podataka

4.4. Faza 4: Analiza i utvrđivanje mera

U završnoj fazi OCTAVE Allegro metodologije vrši se kvantitativna procena rizika kroz kombinovanje posledica i verovatnoće nastanka pojedinačnih pretnji. Za svaku pretnju najpre se određuje kumulativna ocena posledica u odnosu na prethodno definisana područja uticaja i njihove prioritete. Time se omogućava jasnija interpretacija ukupnog rizika i preciznije izdvajanje kritičnih oblasti za delovanje (Caralli et al., 2007; Kuzminykh et al., 2021; Zafar, 2022).

Tabela 4: Matrica vrednosti uticaja

Područje uticaja	***Prioritet***	***Nisko (1)***	***Srednje (2)***	***Visoko (3)***
Funkcionisanje kritične infrastrukture	1	1	2	3
Reputacije države i poverenje javnosti	2	2	4	6
Međunarodna usklađenost i uključenost	3	3	6	9
Finansijski aspekt	4	4	8	12
Održivost i kapacitet odgovora institucija	5	5	10	15

Pored matrice posledica, koristi se i skala verovatnoće (niska - 1, srednja - 2, visoka - 3), koja omogućava pojednostavljenu, ali efektivnu procenu rizika. Iako se u izvornim definicijama OCTAVE Allegro

metodologije verovatnoća procenjuje kvalitativno (Caralli et al., 2007), novija literatura predlaže dodeljivanje numeričkih vrednosti, čime se omogućava preciznije poređenje rizika i njihovo rangiranje.

Na osnovu ukupne ocene posledica i verovatnoće, kreirana je matrica relativne procene rizika koja grupiše rizike u tri kategorije: prihvatljive, one koji zahtevaju nadzor i one koji traže hitnu reakciju.

Tabela 5: Matrica relativne procene rizika

MATRICA RELATIVNE PROCENE RIZIKA		
Ukupan rizik	**Kategorija**	**Tip mere (Pristup)**
90 - 135	Visok rizik	Prioritetni rizici za sanaciju - scenariji koji zahtevaju hitnu reakciju.
45 - 89	Srednji rizik	Rizici za nadzor, mogu se odložiti ili tretirati delimično.
0 - 44	Nizak rizik	Rizici koji su prihvatljivi i najčešće se samo nadgledaju.

Na osnovu ove klasifikacije izdvojena su dva najrizičnija scenarija: (1) Prenos podataka između sistema bez prethodne enkripcije i (2) Uskraćivanje usluge pristupa eUprava portalu putem DoS napada. Njihova detaljna procena prikazana je u Tabeli 5.

Tabela 6: Detaljan proces ocenjivanja rizika za dva najrizičnija scenarija

Rizik	***Funkcionisanje kritične infrastrukture***	***Reputacija države i poverenje javnosti***	***Međunarodna usklađenost i uključenost***	***Finansijski aspekt***	***Održivost i kapacitet odgovora institucija***	***Ukupna ocena posledica (Σ)***	***Verovatnoća***	***Ocena rizika (Σ × ver.)***
Prenos podataka između sistema bez prethodne enkripcije	Srednje (2)	Visoko (6)	Srednje (6)	Srednje (8)	Srednje (10)	32	Visoka (3)	**96**
Uskraćivanje usluge pristupa eUprava portalu putem DoS napada	Visoko (3)	Srednje (4)	Nisko (3)	Srednje (8)	Visoko (15)	33	Visoka (3)	**99**

U završnom koraku OCTAVE Allegro metodologije biće dat predlog konkretnih mera sanacije (Tabela 7), u cilju smanjenja verovatnoće njihovog nastanka i uticaja posledice.

Tabela 7: Mere za smanjenje rizika

Rizik	***Tip mere***	***Nosilac***	***Mera***
Prenos podataka između sistema bez prethodne enkripcije.	Otklanjanje (prioritetna sanacija) (potencijalno otklanjanje)	Unutrašnja mrežna infrastruktura (VPN, LAN)	Sva komunikacija između sistema umreženih institucija mora biti šifrovana korišćenjem protokola koji sprečavaju presretanje i manipulaciju podacima.
		Internet konekcija i eksterni DNS serveri	Upotreba posebnih bezbednosnih protokola (npr. DoH) za prevođenje internet adresa (izvršavanje DNS upita).
Uskraćivanje usluge pristupa eUprava portalu putem DoS napada.	Otklanjanje (prioritetna sanacija)	Serveri baza podataka	Ograničeni broj upita i keširanje podataka koji su često predmet istih.
		Internet konekcija i eksterni DNS serveri	Uvođenje CDN zaštite praćeno ograničavanje broja zahteva koje jedan korisnik može da uputi sistemu u određenom vremenskom periodu (rate-limiting).

5. ZAKLJUČAK

U radu je primenjena OCTAVE Allegro metodologija kao okvir za sistematsku identifikaciju, analizu i procenu sajber rizika portala eUprava. Najkritičniji identifikovani događaj bio je DoS napad, što je poslužilo kao osnova za definisanje odgovarajućih tehničkih mera zaštite. Analiza je pokazala da OCTAVE Allegro pruža jasnu osnovu za rangiranje pretnji i donošenje odluka radi očuvanja funkcionalnosti i poverenja u digitalne servise javne uprave. Budući pravci istraživanja obuhvataju proširenje primene metodologije na druge servise javne infrastrukture, uključivanje većeg broja eksperata za reprezentativniju procenu rizika, kao i dugoročno praćenje efekata mera radi evaluacije njihove efikasnosti i pravovremenog prilagođavanja strategija zaštite.

LITERATURA

Aryanti, U., Anwar, M. T., & Rahmawati, T. (2023). Information security risk management using OCTAVE Allegro method at university. International Journal of Ethno-Sciences and Education Research, 3(4), 137–145. http://dx.doi.org/10.46336/ijeer.v3i4.506

Awad, A. I., Shokry, M., Khalaf, A. A. M., & Abd-Ellah, M. K. (2023). Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach. Computers and Electrical Engineering, 108, 108667.

Bada, M., Sasse, A. M., & Nurse, J. R. (2020). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process. Hanscom AFB, MA. https://doi.org/10.1184/R1/6574790.v1

CyberPeace Institute. (2023). Annual report on targeted cyber attacks against European public digital services.

European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape 2023. https://doi.org/10.1016/j.compeleceng.2023.108667

International Organization for Standardization. (2018). *ISO 31000:2018—Risk management—Guidelines*. ISO. https://www.iso.org/standard/65694.html

International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024 (5th ed.).

Kancelarija za informacione tehnologije i elektronsku upravu (KITEU). (n.d.). Portal eUprava Republike Srbije. https://euprava.gov.rs

Keating, C. G. (2024). Validating the OCTAVE Allegro information systems risk assessment methodology: A case study (Master's thesis). Nova Southeastern University.

Kuzminykh, I., Ghita, B. V., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. Encyclopedia, 1(3), 602–617. https://doi.org/10.3390/encyclopedia1030050

Makajić-Nikolić, D. D. (2022). Metode i tehnike za procenu rizika. Fakultet organizacionih nauka.

Mushi, J. (2023). Examining the factors obstructing cyber security readiness in public sector (Doctoral dissertation, IAA).

Mushtaq, S., & Shah, M. (2024). Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. Information, 15, 619. https://doi.org/10.3390/info15100619

National Institute of Standards and Technology (NIST). (2023, November 7). Supplemental material: Changes in SP 800-53 Release 5.1.1. In Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

OECD. (2021). The E-Leaders handbook on the governance of digital government. OECD Digital Government Studies. OECD Publishing. https://doi.org/10.1787/ac7f2531-en

Paigude, S. D. (2024). A review of cybersecurity policies in the public sector: Challenges and solutions. Computer Fraud & Security (November), Article 28. https://doi.org/10.52710/cfs.28

Schneider, G. B. C. (2025). The importance of cybersecurity in digital government implementations. COGNITIONIS, 5(1), Article 585. https://doi.org/10.38087/2595.8801.585

Shostack, A. (2020). Threat modeling: Designing for security (2nd ed.). Wiley.

United Nations, Department of Economic and Social Affairs. (2024). United Nations e-government survey 2024: Accelerating digital transformation for sustainable development, with the addendum on artificial intelligence. United Nations.

Vlada Republike Srbije. (2023). Program razvoja elektronske uprave u Republici Srbiji za period od 2023. do 2025. godine sa akcionim planom za njegovo sprovođenje („Službeni glasnik RS", br. 33/2023-127).

Zafar, S. (2022). Vulnerability assessment of IoT-based smart lighting systems (Master's thesis, University of Skövde).

Zakon o zaštiti podataka o ličnosti (ZZPL). („Službeni glasnik RS", br. 87/2018). (2018). Pristupljeno 15. juna 2025. sa https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html