https://doi.org/10.17559/JF-2026010000021

Zaprimljen: 21.10.2025.
Odobren za objavu: 27.1.2026.
Pregledni rad

SIGURNOSNI ASPEKTI UPRAVLJANJA ZNANJEM

Jerko Glavaš
Ekonomski fakultet Sveučilišta Josipa Jurja Strossmayera u Osijeku, Trg Ljudevita Gaja 7, 31000 Osijek, Hrvatska,
ePošta: jerko.glavas@efos.hr

Sažetak: Upravljanje znanjem postaje ključni čimbenik uspjeha suvremenih organizacija koje se suočavaju s brzim tehnološkim promjenama i rastućom količinom podataka. Međutim, dok učinkovito upravljanje znanjem može povećati inovativnost i konkurentnost, istovremeno otvara niz sigurnosnih izazova.

Ovaj rad istražuje sigurnosne aspekte upravljanja znanjem, s posebnim naglaskom na zaštitu povjerljivih informacija, intelektualnog vlasništva te sigurnost digitalnih sustava za pohranu i dijeljenje znanja. Analiziraju se prijetnje poput neovlaštenog pristupa, curenja podataka te rizika povezanih s ljudskim faktorom. Kroz pregled literature i primjere iz prakse, rad ističe važnost integracije sigurnosnih mjera u sve faze ciklusa upravljanja znanjem – od prikupljanja i pohrane do distribucije i primjene.

Zaključno, sigurnost upravljanja znanjem ne smije se promatrati kao tehničko pitanje već kao sastavni dio organizacijske strategije koja osigurava dugoročnu održivost i zaštitu konkurentskih prednosti.

Ključne riječi: Upravljanje, znanje, upravljanje znanjem, sigurnost

1. Uvod

Razumijevanje upravljanja znanjem započinje razlikovanjem između podataka, informacija i znanja. Iako znanje nije isto što i podatak ili informacija, ono ne može postojati bez njih (Saaristo, 2012).

Novo znanje nastaje kada se postojeća uvjerenja pojedinca povežu s novim podatcima koji proizlaze iz dostupnih informacija. Koskinen i Pihlanto opisuju podatke kao sirove činjenice — poput brojeva i slova — koje dobivaju značenje tek kada se smjeste u odgovarajući kontekst, čime nastaju informacije. Kada se te informacije spoje s prethodnim iskustvima, percepcijom i vještinama pojedinca, rezultat je stvaranje znanja. Stoga se podatci, informacije i znanje promatraju kao odvojeni, ali međusobno povezani koncepti (Miloloža et.al, 2021).

Pojam upravljanja znanjem ima brojne definicije. Seiner (2001) ga opisuje kao „koncept prema kojem organizacija prikuplja, organizira, dijeli i analizira znanje pojedinaca i timova u cijelom sustavu na načine koji izravno utječu na njezine performanse". Levinson (2007) smatra da je upravljanje znanjem „proces kojim organizacije stvaraju vrijednost koristeći svoja intelektualna i znanjem temeljena sredstva".

Prema Sveibyju (1996), upravljanje znanjem uključuje „identifikaciju i analizu postojećih i potrebnih znanja i procesa kako bi se ostvarili ciljevi organizacije". Villegas (2000) ga jednostavno definira kao „prijenos znanja između pojedinaca,

pri čemu primatelj stječe korist od iskustva i mudrosti iskusnijih članova organizacije". Estacio (2006) dodaje da je upravljanje znanjem „ciklički sustav koji omogućuje organizaciji učinkovitije postizanje ciljeva kroz pretvaranje implicitnog i eksplicitnog učenja u navike, bolje planiranje i provedbu" (Milološa et.al, 2021).

2. Metodologija

U radu su korištene deskriptivna metoda, kvantitativna metoda, induktivna metoda, metoda analiza i sinteze.

Napravljena je obrada i analiza sekundarnih podataka koji se koriste kao primarni podatci za dokazivanje postavljene hipoteze u radu:

H1: Korištenje digitalnih alata za pohranu i dijeljenje znanja povećava produktivnost, ali i izloženost sigurnosnim prijetnjama ako nisu primijenjene adekvatne zaštitne mjere.

Za empirijsku analizu korišten je EBRD Knowledge Economy Index, koji mjeri stupanj razvoja gospodarstva znanja u 46 zemalja. Indeks se sastoji od četiri stupa: (1) institucije za inovacije, (2) vještine za inovacije, (3) inovacijski sustav i (4) ICT infrastruktura. Svaki stup ocjenjuje se na ljestvici od 1 do 10. Analiza uključuje usporedbu EBRD i OECD zemalja te promjene u razdoblju 2011.–2018.

3. Sigurnost informacija u kontekstu upravljanja znanjem

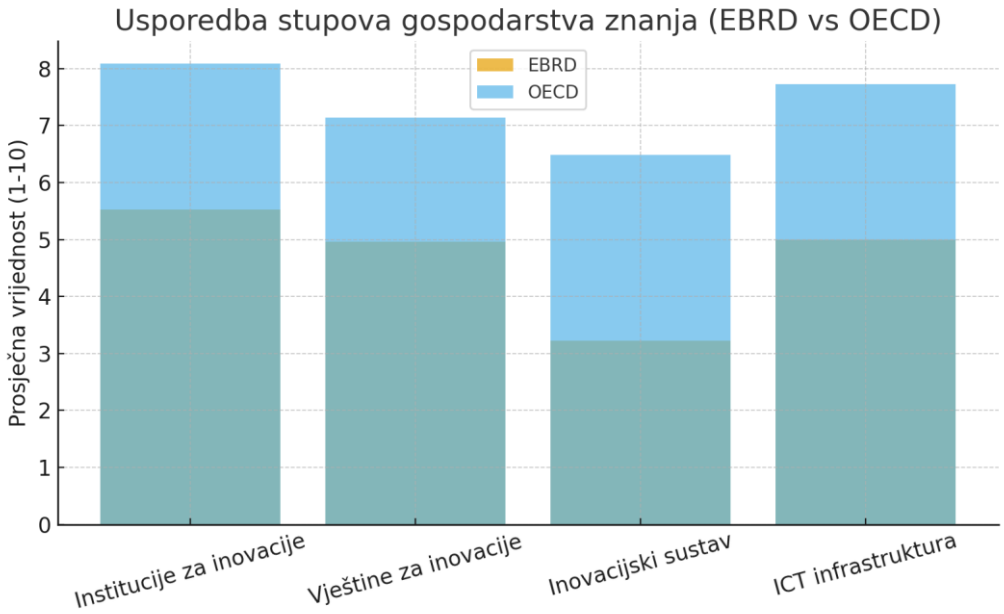
Sigurnost i upravljanje znanjem isprepleteni su jer je znanje vrijedna organizacijska imovina koju treba zaštititi. Učinkoviti sustavi upravljanja znanjem (KM) zahtijevaju snažne sigurnosne mjere za zaštitu intelektualnog vlasništva, dok se upravljanje sigurnošću oslanja na znanje i obuku svojih korisnika kako bi bilo uspješno. Ključne komponente uključuju implementaciju kontrola pristupa, osiguranje digitalne pohrane, sigurno odlaganje zastarjelih informacija i obuku zaposlenika o praksama KM-a i sigurnosnoj svijesti.(Viibe, 2022.)

Upravljanje znanjem postalo je temeljni element suvremenih organizacija i nacionalnih gospodarstava. U društvu znanja, informacije i njihova zaštita predstavljaju ključni resurs. Sigurnosni aspekti upravljanja znanjem obuhvaćaju institucionalne mehanizme, zaštitu informacija, digitalnu sigurnost i etičke dimenzije. Cilj ovog rada je analizirati kako se sigurnosni aspekti odražavaju kroz pokazatelje gospodarstva znanja prema EBRD indeksu.

5. Rezultati empirijskog istraživanja

Za empirijsku analizu korišten je EBRD Knowledge Economy Index, koji mjeri stupanj razvoja gospodarstva znanja u 46 zemalja. Indeks se sastoji od četiri stupa: (1) institucije za inovacije, (2) vještine za inovacije, (3) inovacijski sustav i (4) ICT infrastruktura. Svaki stup ocjenjuje se na ljestvici od 1 do 10. Analiza uključuje usporedbu EBRD i OECD zemalja te promjene u razdoblju 2011.–2018.

Analiza pokazuje znatne razlike između EBRD i OECD zemalja. Najveći jaz uočava se u inovacijskom sustavu, dok je najmanji u vještinama za inovacije. ICT infrastruktura pokazuje najveći napredak između 2011. i 2018. godine. Najveći doprinos prijelazu iz rane u srednju fazu razvoja gospodarstva znanja ima ICT infrastruktura (37%). Dostupni su i djelomični noviji podatci ali nisu kompletirani te nije moguće napraviti detaljniju analizu što je jedno od ograničenja istraživanja.



Slika 1. Usporedba EBRD i OECD zemalja po stupovima gospodarstva znanja.

Analiza potvrđuje da razvoj društva znanja zahtijeva uravnotežen razvoj svih aspekata upravljanja znanjem. ICT infrastruktura i institucionalni okvir ključni su za rane faze, dok inovacijski sustav i specijalizirane vještine postaju presudni u naprednim fazama. Postoji visoka korelacija između indeksa znanja i BDP-a ($r \approx 0,85$).

4. Zaključak

Sigurnosni aspekti upravljanja znanjem povezani su s institucionalnim kapacitetima i digitalnom infrastrukturom. Zemlje koje imaju stabilne institucije i razvijenu ICT infrastrukturu lakše uspostavljaju sustave zaštite informacija i inovacijskih resursa. Usporedba pokazuje da EBRD regije, iako napreduju u digitalizaciji, i dalje zaostaju u institucionalnoj sigurnosti. Slabosti u zakonodavnom okviru i provedbi politike zaštite podataka predstavljaju glavni rizik za održivost gospodarstva znanja.

Rezultati istraživanja potvrđuju da su sigurnosni aspekti sastavni dio učinkovitog upravljanja znanjem. ICT infrastruktura i institucije predstavljaju ključne čimbenike sigurnosti, dok inovacijski sustav zahtijeva dodatna ulaganja u istraživanje, razvoj i zaštitu intelektualnog vlasništva. Razvijanje sigurnosne kulture unutar organizacija i na nacionalnoj razini presudno je za održivost društva znanja.

5. Literatura

Viibe, 2022., https://viibe.co/knowledge-management/security-in-knowledge-management/

Miloloža, I., Glavaš, J., Ravlić, S. (2021) Upravljanje znanjem i karijerom, Fakultet z dentalnu medicinu i zdravstvo, Sveučilište Josipa Jurjs Strossmayera u Osijeku, Osijek

European Bank for Reconstruction and Development (2019). Introducing the EBRD Knowledge Economy Index.

World Bank (2020). The Knowledge Economy Framework.

OECD (2021). Innovation and Knowledge Management in the Digital Era.

Nonaka, I. & Takeuchi, H. (1995). The Knowledge-Creating Company. Oxford University Press.

SECURITY ASPECTS OF KNOWLEDGE MANAGEMENT

Abstract: Knowledge management is becoming a key success factor for modern organizations facing rapid technological change and growing amounts of data. However, while effective knowledge management can increase innovation and competitiveness, it also opens up a number of security challenges.

This paper explores the security aspects of knowledge management, with a particular focus on the protection of confidential information, intellectual property, and the security of digital systems for storing and sharing knowledge. Threats such as unauthorized access, data leakage, and risks related to the human factor are analyzed. Through a literature review and practical examples, the paper emphasizes the importance of integrating security measures into all phases of the knowledge management cycle – from collection and storage to distribution and application.

In conclusion, knowledge management security should not be viewed as a technical issue but as an integral part of an organizational strategy that ensures long-term sustainability and protection of competitive advantages.

Keywords: Management, knowledge, knowledge management, security