

# Izvešće o aktivnostima Radne skupine za informacijsku i kibernetičku sigurnost (IKS) u 2024. godini

Hrvoje Belani<sup>1,2</sup>

<sup>1</sup>Ministarstvo zdravstva, Uprava za e-zdravstvo, Ksaver 200a, Zagreb

<sup>2</sup>Radna skupina IKS, Hrvatsko društvo za medicinsku informatiku, Zagreb, Hrvatska

E-pošta: [hrvoje.belani@miz.hr](mailto:hrvoje.belani@miz.hr); [orcid.org/0000-0003-1392-7502](https://orcid.org/0000-0003-1392-7502)

Radna skupina za informacijsku i kibernetičku sigurnost u zdravstvu (skraćeno: IKS) djeluje pri Hrvatskom društvu za medicinsku informatiku (HDMI) od 24. svibnja 2021. godine [1]. S obzirom na misiju i ciljeve, radna skupina djeluje kao platforma za promicanje i popularizaciju znanja te istraživačkih aktivnosti u područjima informacijske i kibernetičke sigurnosti u zdravstvu, a okuplja sljedeće članove, koji su ujedno i njeni inicijatori: Krunoslav Antoliš, Hrvoje Belani (voditelj), Kristina Fišter, Mira Hercigonja-Szekeres, Josipa Kern, Nikola Protrka i Krešimir Šolić.

S obzirom da to da je posljednje Izvešće o aktivnostima Radne skupine za informacijsku i kibernetičku sigurnost (IKS) [2] objavljeno u 2. broju 29. sveska Biltena HDMI-ja za 2023. godinu, njime nije obuhvaćen rad objavljen u istom broju Biltena HDMI-ja, kako slijedi:

„Visoko obrazovanje o informacijskoj i kibernetičkoj sigurnosti u Hrvatskoj s osvrtom na obrazovanje zdravstvenih djelatnika“ [3], uvodnik autora Hrvoja Belanija. Sažetak: „Kibernetičke ugroze i napadi sve su značajniji na zdravstvene sustave svijeta, s negativnim posljedicama na pružanje zdravstvene zaštite i medicinske skrbi, pa i pogubnim za zdravlje i život pacijenata. Nedostatak stručnjaka u području informacijske i kibernetičke sigurnosti, kao i digitalnih vještina zdravstvenih djelatnika vezanih uz to područje, sve su veći izazovi današnjice kako globalno, tako i u Hrvatskoj. Ovaj rad istražuje mogućnosti visokog obrazovanja o informacijskoj i kibernetičkoj sigurnosti na sveučilištima i veleučilištima u Hrvatskoj, s osvrtom na izbor kolegija, modula i nastavnih tema o informacijskoj i kibernetičkoj sigurnosti u sveučilišnim i veleučilišnim nastavnim planovima i programima za obrazovanje stručnjaka zdravstvenih i medicinskih struka. Rezultati daju pregled sveučilišnih i stručnih studija u području informacijske i kibernetičke sigurnosti te pregled studija zdravstvenih i medicinskih struka s popisom kolegija koji možebitno obrađuju područje informacijske i kibernetičke sigurnosti. U zaključku su dane preporuke i smjernice za prevladavanje ovih izazova.“

## Aktivnosti u 2024. godini

Radna skupina IKS održala je jedan sastanak u 2024. godini, i to 19. studenog 2024. virtualnim putem. Tijekom 2024. godine Radna skupina IKS je provela sljedeće aktivnosti:

- Sastavljen je prijedlog druge međunarodne znanstvene posebne sjednice „*The Second International Special Session on Cybersecurity in Healthcare and Medicine*“ (CyHeMe) i

kandidiran za održavanje u sklopu međunarodne znanstvene konferencije „*The 9th International Conference on Smart and Sustainable Technologies*“ (IEEE SpltTech 2024) [4], koja se održala od 4. do 7. rujna 2024. godine u Bolu na Braču. Prijedlog radionice je prihvaćen te se održala 4. rujna 2024. godine predstavivši šest znanstvenih radova nakon recenzijskog postupka na koji je bilo prijavljeno ukupno deset znanstvenih radova. Radovi su objavljeni u zborniku konferencije koji je dostupan putem platforme IEEE Xplore [15]. Među prihvaćenim radovima bio je i izvorni znanstveni rad člana Radne skupine IKS:

- „Zakonodavstvo Europske unije o kibernetičkoj sigurnosti za zdravstveni sektor: Izvješće o hrvatskom iskustvu“ autora Hrvoja Belanija, Tonija Perkovića i Petra Šolića. Sažetak: „Kibernetička sigurnost ima za cilj zaštititi digitalnu imovinu od ugrožavanja. Kibernetička sigurnost je zajednička odgovornost i trebala bi biti izgrađena unutar organizacijske kulture, postavljena kao prioritetna poslovna funkcija, kao i pravilno implementirana u postojeća tehnološka rješenja. Neki su sektori bitniji od drugih, poput zdravstvenog sektora, koji se bave osjetljivim korisničkim informacijama i podacima o zdravstvenom statusu, primijenjenim medicinskim postupcima, korištenim medicinskim proizvodima i medicinskim uređajima itd. Regulirani pristup kibernetičkoj sigurnosti nužno zahtijeva određenu razinu organizacijske centralizacija, kako na razini EU, tako i na razini država članica EU, gdje ne postoji jedinstveno rješenje. Razlika u pristupima uglavnom je rezultat različitog nacionalnog razvoja kibernetičkih resursa u prethodnim godinama. Kada je EU usvojila NIS Direktivu za jačanje kibernetičke sigurnosti na razini EU, transpozicija i provedba ovog pravnog akta predstavljala je izazov za države članice EU. Ovaj rad predstavlja izvješće o iskustvu Hrvatske u provedbi zakonodavstva EU-a za kibernetičku sigurnost u zdravstvenom sektoru. Prikazani su uspostavljeni procesi i smjernice te dani specifični izazovi unutar zdravstvenog sustava“ [5].
- o Članovi Radne skupine IKS objavili su sljedeće znanstvene radove u područjima informacijske i kibernetičke sigurnosti, odnosno sudjelovali na sljedećim pozivnim predavanjima na skupovima:
  - „Utjecaj starosne dobi i obrazovanja na kibernetičku sigurnost u digitalnom bankarstvu“ izvorni znanstveni rad autora M. Bukovec i Krunoslava Antoliša, pred objavljivanjem u znanstveno-stručnom časopisu za novinarstvo i medije „Medijska istraživanja“, ISSN 1330-6928 (tisak).
  - „Kibernetička sigurnost u poslovanju“ stručni rad autora Mihaela Budinskog, Nenada Sikirice i Mire Hercigonja-Szekeres na 6. stručnom skupu „Simpozij – Susreti 2024.“ u organizaciji Veleučilišta Hrvatsko zagorje Krapina. Sažetak: „Kibernetička sigurnost u poslovanju predstavlja skup praksi i tehnologija za zaštitu informacija, informacijskih sustava i mreže od kibernetičkih prijetnji. Središnji ciljevi u ovom području uključuju strategije za sprječavanje, otkrivanje i reagiranje na kibernetičke napade, kao i zaštitu osjetljivih podataka. Ključni aspekti kibernetičke sigurnosti uključuju primjenu jakih lozinki, upravljanje pristupom informacijama i redovito ažuriranje softvera. U današnjem digitalnom okruženju efikasna kibernetička sigurnost u poslovanju postaje sve važnija za održavanje povjerenja korisnika i zaštitu poslovnih operacija zbog

financijskih gubitaka i štete. U radu su opisani neki primjeri kibernetičke sigurnosti u Općoj bolnici Zabok“.

- Profesor Krunoslav Antoliš: pozivno predavanje na skupu „*Hybrid threats in the context of the regional crisis*“ održanom od 17. do 19. rujna 2024. godine u Chişinău, Moldavija, s dvije teme: „*Presentation of examples of effective approaches; debate and exchange of views on Cyber Security strategies in front of HTh*“ i „*Cyber threats to critical infrastructure; examples, Case studies*“, 17-19 Sept 2024, Chişinău, Moldova; pozivno predavanje „Razumijevanje informacijskog poremećaja i analiza primjera“ na skupu „Izazovi i prilike digitalnog okruženja u zdravstvu“, održanom od 4. do 5. listopada 2024. godine u organizaciji međunarodnog sveučilišta Libertas i Hrvatskog društva za poboljšanje kvalitete zdravstvene zaštite Hrvatskog liječničkog zbora, a sve u sklopu Akademije-kvaliteta zdravstvene zaštite i sigurnost pacijenta – cjeloživotno obrazovanje, Zagreb, Hrvatska; pozivno predavanje „Integracija umjetne inteligencije u kibernetičku sigurnost sustava socijalne skrbi: izazovi, prilike i budućni smjerovi“, održanom 21. i 22. listopada 2024. na Međunarodnoj znanstveno-stručnoj konferenciji „Koloriti zajedništva“, u organizaciji Centra za rehabilitaciju Zagreb; pozivno predavanje „*Cyber resilience act for healthcare system*“, održanom 24. listopada 2024. na znanstvenoj konferenciji „Bezbjednost zemalja regiona u svjetlu nove bezbjedonosne arhitekture“ u Banjoj Luci, Bosna i Hercegovina.

Srodne aktivnosti u kojima su članovi Radne skupine IKS sudjelovali ispred matičnih organizacija, a čiji rezultati su tematski povezani i korisni za daljnji rad Radne skupine IKS:

- o Profesor Krunoslav Antoliš sudjelovao je u radu na projektu ERASMUS+: KA220-HED – partnerska suradnja u visokom obrazovanju, u okviru čega je osobno vodio istraživački zadatak „Zloupotreba informacijsko-komunikacijskih tehnologija u kreiranju i širenju dezinformacija“, kojom prigodom je proveo istraživanje na Veleučilištu kriminalistike i javne sigurnosti te na Policijskoj školi „Josip Jović“, uz prethodno dobivene suglasnosti od Etičkog povjerenstva Veleučilišta kriminalistike i javne sigurnosti i od Ministarstva znanosti i obrazovanja, za provođenje istraživanja na Policijskoj školi „Josip Jović“; održao predavanja na teme „*Threats and modus operandi for affecting critical infrastructure and strategic objects of the state*“ i „*Supporting the resilience of the European Union and neighbours' critical infrastructure*“, u sklopu „*Session 3. Protection of critical infrastructure*“, u okviru *Micro-Credential Curriculum in Countering Hybrid Threats*, 9. rujna 2024.
- o „Umjetna inteligencija i zdravstvena skrb – izazovi i potencijali“ naziv je znanstvenog skupa održanog u petak, 29. studenoga 2024. na Hrvatskom katoličkom sveučilištu. Znanstvenim skupom obilježio se ujedno i završetak uspostavnog istraživačkog projekta Hrvatske zaklade za znanost „(Novi) etički i društveni izazovi digitalnih tehnologija u domeni zdravstvene skrbi – Digit-Heal“ pod vodstvom izv. prof. dr. sc. Ante Čartolovnog. Na znanstvenom skupu sudjelovali su istaknuti stručnjaci koji su pridonijeli raspravi iz liječničke, institucionalne, industrijske i pravne perspektive kroz izlaganja i panel raspravu. Hrvoje Belani iz Sektora za implementaciju i unaprjeđenje informacijskih sustava Uprave za e-zdravstvo Ministarstva zdravstva osvrnuo se na NIS2 direktivu [6] koja se fokusira na kibernetičku sigurnost u zdravstvenom sustavu te opisao na koji način

- će ista utjecati na hrvatski zdravstveni sustav te istaknuo koji su ključni aspekti kibernetičke sigurnosti.
- „*e-Health Cybersecurity and Asset Protection for Start-ups*“ naziv je dvosatne radionice koju je u sklopu ciklusa edukacija zimske škole AI4Health.Cro virtualnim putem u srijedu, 12. prosinca 2024. godine održao Hrvoje Belani. Riječ je o aktivnosti u sklopu istoimenog projekta kojim je uspostavljen Europski digitalni inovacijski hub za primjenu umjetne inteligencije [7], a polaznici su bili predstavnici startupova i zdravstvenih ustanova.
  - Profesor Krunoslav Antoliš imenovan je predsjednikom Strateškog vijeća XXIV Sigurnost i obrana, Agencija za znanost i visoko obrazovanje, od 11. prosinca 2024., na razdoblje od četiri godine.

## Zaključak

Za 2025. godinu u planu je Radne skupine IKS sastaviti projektni prijedlog za prijavu na poziv za prijedloge programa „*The NATO Science for Peace and Security (SPS) Programme*“, s rokom za dostavu prijedloga 5. siječnja 2025. godine [8]. Program nudi izvrsnu priliku za prijavu projekta vezanog za „Advanced Research Workshop“ (ARW) na temu kibernetičke sigurnosti u kontekstu obrambenih aktivnosti, posebno usmjerenog na zdravstvo i medicinu. Zdravstveni sustavi i IoMT (od engl. *Internet of Military Things*) predstavljaju specifičan segment ranjivosti, a napredna istraživanja u tom području mogu značajno doprinijeti sigurnosti vojnih i zdravstvenih operacija.

Također je u pripremi prijedlog treće međunarodne posebne sjednice „*The Third International Special Session on Cybersecurity in Healthcare and Medicine*“ (CyHeMe) za prijavu radi održavanja u sklopu međunarodne znanstvene konferencije „*The 10th International Conference on Smart and Sustainable Technologies*“ (SpliTech 2025) [9], koja će se održati u Splitu i Bolu na Braču od 16. do 20. lipnja 2025. godine. S obzirom na pozitivna iskustva s prethodnim izdanjima CyHeMe, i ovom se prilikom očekuje predstavljanje barem pet znanstvenih radova na temu informacijske i kibernetičke sigurnosti u zdravstvu i medicini.

## Literatura

1. Belani H. Radna skupina za informacijsku i kibernetičku sigurnost (IKS). Bilten Hrvatskog društva za medicinsku informatiku (Online) [internet]. 2021;27(2):38-41 [pristupljeno: 18.12.2024.]. Dostupno na: <https://hrcak.srce.hr/260279>
2. Belani H. Izvješće o aktivnostima Radne skupine za informacijsku i kibernetičku sigurnost (IKS). Bilten Hrvatskog društva za medicinsku informatiku (Online) [internet]. 2023;29(2):43-48 [pristupljeno: 18.12.2024.]. Dostupno na: <https://hrcak.srce.hr/310648>
3. Belani H. Visoko obrazovanje o informacijskoj i kibernetičkoj sigurnosti u Hrvatskoj s osvrtom na obrazovanje zdravstvenih djelatnika. Bilten Hrvatskog društva za medicinsku informatiku (Online) [internet]. 2023;29(2) [pristupljeno: 18.12.2024.]. Dostupno na: <https://hrcak.srce.hr/308293>
4. The 9th International Conference on Smart and Sustainable Technologies (SpliTech 2024) [internet]. Pristupljeno: 10.11.2024. Dostupno na: <https://2024.splitech.org/Home>.

5. H. Belani, T. Perković and P. Šolić, "The European Union Cybersecurity Legislation for the Health Sector: A Croatian Experience Report," 2024 9th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, 2024, pp. 1-6.

<https://doi.org/10.23919/SpliTech61897.2024.10612321>

6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Službeni list Europske unije, L 333/80, 27.12.2022. [pristupljeno: 10.11.2024.] Dostupno na:

<http://data.europa.eu/eli/dir/2022/2555/oj>.

7. Barešić A. U Hrvatskoj je pokrenut Europski digitalni inovacijski centar Umjetna inteligencija za pametno zdravstvo i medicinu (AI4Health.Cro). Bilten Hrvatskog društva za medicinsku informatiku (Online) [internet]. 2023;29(1):31-35 [pristupljeno 18.12.2024.]. Dostupno na: <https://hrcak.srce.hr/304691>

8. NATO Science for Peace and Security (SPS) Programme. Call for Proposals 2025. Pristupljeno: 10.11.2024. Dostupno na: <https://www.nato.int/cps/en/natohq/78209.htm>.

9. The 10th International Conference on Smart and Sustainable Technologies (SpliTech 2025). Pristupljeno: 10.11.2024. Dostupno na: <https://2025.splitech.org/Home>.