

1. пк др Радомир Продановић, дипл. инж., научни сарадник, председник комисије
2. пк доц др Бориша Јовановић, дипл. инж., научни сарадник члан
3. вс др Данијела Протић, дипл. инж., научни сарадник, члан

**Извештај комисије за избор
вс мр Дејан Бајић, дипл. инж. у звање
стручни сарадник.-**

Научном већу ТОЦ-а

На основу одлуке Научног већа Техничког опитног центра број 05-6200-11 од 21.10.2025. године, донете на 143. седници одржаној 17.10.2025. године, именовани смо за чланове Комисије за подношење извештаја за избор у стручно звање **стручни сарадник** вс мр Дејана Бајића, дипл. инж.

На основу увида у пристигли материјал који се односи на научноистраживачки рад пријављеног кандидата подносимо следећи

ИЗВЕШТАЈ КОМИСИЈЕ

БИОГРАФИЈА КАНДИДАТА

Војни службеник мр Дејан Бајић, дипл. инж, рођен је у Београду 1967. године. Основну и средњу школу завршио је у Бару. Дипломирао је 1993. године на Електротехничком факултету, Универзитета у Београду и стекао звање дипломираног инжењера електротехнике за аутоматiku и електронику. Магистрирао је 1999. године на Електротехничком факултету, Универзитета у Београду на катедри за Аутоматiku и Електронику област Управљање системима.

Од 1994. запослен је у ИПМЕ, и од тада ради као криптолог, а касније као виши криптолог на следећим радним местима:

- **1994-2000:** Криптолог у одељењу за криптозаштиту у телекомуникационим системима, ИПМЕ,
- **2000-2023:** Виши криптолог у одсеку за криптозаштиту у рачунарским мрежама одељења за развој и имплементацију криптоалгоритама, ЦПМЕ, УТИ (Ј-6) ГШ ВС
- **2023 и даље:** Виши криптолог у одсеку за криптозаштиту у рачунарским мрежама, одељењу за развој криптографских решења (ОдрКР), ЦПМЕ, УТИ (Ј-6) ГШ ВС

Аутор је једног стручног рада на домаћој стручној конференцији и једног стручног рада у часописима.

БИБЛИОГРАФИЈА КАНДИДАТА

Зборници научних скупова (M60)	
1.	Bajić, D. 2023. Using randomness tests for evaluation of datat security mechanisms in environnment with limited resources. <i>Proceedings of conference SYM-OP-IS</i> . Tara 18-21 September 2023. pp. 323-327 http://www.symopis2023.mod.gov.rs/download/SIM-OP-IS-2023-Zbornik.pdf (M63)

Радови у часописима (M50)	
1.	Jovanović, S., Protić, D., Antić, V., Grdović, M., Bajić, D. 2023. Security of wireless keyboards: Threats, vulnerabilities and countermeasures. <i>Vojnotehnički glasnik/Military technical Courier</i> 71(2), pp. 296-315. https://doi.org/10.5937/vojtehg71-43239 (M51)

АНАЛИЗА РАДОВА КОЈИ КАНДИДАТА КВАЛИФИКУЈУ У ПРЕДЛОЖЕНО ЗВАЊЕ

1. **Bajić, D.** 2023. Using randomness tests for evaluation of datat security mechanisms in environnment with limited resources. *Proceedings of conference SYM-OP-IS*. Tara 18-21 September 2023. pp. 323-327 <http://www.symopis2023.mod.gov.rs/download/SIM-OP-IS-2023-Zbornik.pdf>

У раду је описан метод тестирања јавног шифарског алгоритма *Ascon-128a* у *AEAD* (Authenticated encryption with associated data) моду рада са *NIST* пакетом статистичких тестова. Алгоритам припада класи “*Lightweight*” криптографије која се користи у заштити података у уређајима који имају ограничене хардверске ресурсе у погледу процесорске снаге рачунања, меморије, потрошње батерије итд. Главне области примене ове криптографије су *RFID* системи и тагови, уређаји у здравственој нези, медицински уређаји, мреже сензора, *ИоТ* “*Internet of Things*” итд.

Дефинисано је 8 сетова података који су генерисани са *Ascon-128a* алгоритмом у сврху тестирања са *NIST* пакетом тестова и дат кратак опис параметара алгоритма. Ови сетови података су изабрани јер се верује да су корисни у евалуацији квалитета блок шифарских алгоритама у *AEAD* моду рада. У *AEAD* моду алгоритма *Ascon-128a* се нису користили придружени подаци јер се они не штите. Такође укратко је описан *NIST* статистички пакет тестова за евалуацију квалитета генератора случајних бројева. У тесту криптографске заштите, *Ascon-128a* алгоритам је прошао свих 188 статистичких тестова за тест податке *Plaintext/Ciphertext Correlation*, *128-bit Key Avalanche*, *128-bit Nonce Avalanche*, *Low Density 128 bit Nonce*. Постоји потреба за додатним тестирањима са већим скуповима података јер не пролази све *NIST* тестове на неким скуповима података.

2. Jovanović, S., Protić, D., Antić, V., Grdović, M., **Bajić, D.** 2023. Security of wireless keyboards: Threats, vulnerabilities and countermeasures. *Vojnotehnički glasnik/Military technical Courier* 71(2), pp. 296-315. <https://doi.org/10.5937/vojtehg71-43239> (M51)

Овај рад приказује преглед истраживања рањивости рачунарских система изазваних компромитујућим електромагнетским зрачењем, код бежичних тастатура. Бежични уређаји користе комуникацију коју карактерише проблем очувања приватности информација због инхерентног, могућег отицања података изазваног емисијом радио таласа. Wireless повезивање је извор еманиције сигнала који мора бити заштићен у смислу безбедности података. Методе које су примењене у раду су разматрање рањивости бежичних тастатура и side-channel напада, с циљем истраживања отицања података због електромагнетске емисије. Добијени резултати указују на пропусте који су специфични за бежичне тастатуре. Резултати тестирања упада откривају рањивости таргетиране бежичне тастатуре који су посебно евидентни у случајевима застарелог софтвера, поузданости бежичног преноса и конекције. Доказано је да постоје безбедносни пропусти који ометају радио комуникацију, дајући малициозном кориснику могућност за потпуни приступ рачунару на који је бежична тастатура повезана.

ПРЕГЛЕД НАУЧНОГ И СТРУЧНОГ РАДА

Војни службеник мр Дејан Бајић, дипл. инж. бави се научноистраживачким радом у области криптозаштите у рачунарским мрежама и телекомуникацијама. Његова ужа специјалност је развој и имплементација криптографских решења примењивих у области заштите писаних и говорних информација.

У току каријере учествовао је у једном научно-истраживачком пројекату примењених истраживања израде генератора случајних импулса ГСИ који се у ЦПМЕ користи као основна сировина за израду криптографских кључева у разним шифарским системима и за израду СДКЗ са случајним низом за заштиту података у шифарском систему Ш-8.

ЗАКЉУЧАК СА ПРЕДЛОГОМ ЗА ОДЛУЧИВАЊЕ

Кандидат вс мр Дејан Бајић, дипл. инж. у свом досадашњем раду био је аутор два стручна рада.

Коефицијент научне компетентности мр Дејана Бајића, дипл. инж. у претходном трогодишњем периоду је:

$$M_{30} + M_{50} + M_{60} = 0 + 2 + 0.5 = 2.5$$

На основу критеријума за процену научне компетентности кандидата, кандидат је остварио следеће квантитативно изражене резултате:

Ознака групе резултата	Поени	Број радова	Укупно
M ₆₃	0.5	1	0.5
M ₅₁	2	1	2
Укупно			2.5

Комисија сматра да кандидат **вс мр Дејан Бајић**, дипл. инж., испуњава услове дефинисане Правилником о условима за стицање стручних звања у Техничком опитном центру и предлаже Научном већу ТОЦ-а да изабере кандидата у стручно звање **стручни сарадник**.

ЧЛАНОВИ КОМИСИЈЕ

пк др **Радомир Продановић**, дипл. инж., научни сарадник, председник

пк доц др **Бориша Јовановић**, дипл. инж., научни сарадник, члан

вс др **Данијела Протић**, дипл. инж., научни сарадник, члан

ТЕХНИЧКИ ОПИТНИ ЦЕНТАР

..... Бр. **05/4042-1**

18-11-2025 20..... год.

БЕОГРАД