ВЕЋУ ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ ФАКУЛТЕТА ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА АЛФА БК УНИВЕРЗИТЕТА

На основу одлуке бр. 846 Већа за последипломске студије Алфа БК Универзитета, са седиштем у Београду, на седници која је одржана 25.05.2025. године, именовани смо за чланове Комисије за оцену и јавну одбрану докторске дисертације кандидата Ален Камиша под називом „ Defense in Depth стратегија информационе сигурности за предузећа мале и средње величине у БиХ".

Комисија у саставу:

1) Проф. др Милан Глигоријевић, Алфа БК Универзитет, Београд, председник;
2) Доц. др Александар Закић, Алфа БК Универзитет, Београд, ментор;
3) Проф. др Славиша Трајковић, Економски факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици, члан;
4) Доц. др Јелена Стојановић, Алфа БК Универзитет, Београд;
5) Проф. др Лидија Беко, Рударско-геолошки факултет Универзитета у Београду, члан;

У складу са Правилником о докторским академским студијама Алфа БК Универзитета, на основу детаљног прегледа достављене докторске дисертације, подноси следећи:

ИЗВЕШТАЈ О ОЦЕНИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

1.ОСНОВНИ ПОДАЦИ О КАНДИДАТУ

1.1. Биографија кандидата

Ален Камиш рођен је 8. априла 1978. године у Сарајеву, где је завршио основно и средње образовање. Своје високо образовање започео је на Високој школи за услужни бизнис у Источном Сарајеву – Соколац, где је стекао звање дипломирани менаџер пословне информатике с просјечном оцјеном 8,60. Даље академско усавршавање наставио је на Универзитету за пословни инжењеринг и менаџмент ПИМ, на Факултету информационих технологија, где је стекао звање дипломирани инжењер рачунарства и информатике с просјечном оцјеном 8,82, а потом завршио и мастер студиј с просјечном оцјеном 9,50, чиме је стекао звање мастер рачунарства и информатике. С циљем даљег научно-истраживачког и стручног развоја, 2021. године уписује докторске студије на Алфа БК Универзитету у Београду, на студијском програму Информационо-комуникационе технологије.

Током своје професионалне каријере, која траје дуже од двије деценије, стекао је богато искуство у области информационих технологија, са посебним фокусом на сајбер сигурност, системску интеграцију, виртуализацију, мрежне технологије и управљање сложеним ИТ инфраструктурама. Учествовао је у пројектовању, имплементацији и одржавању напредних информационих система у сложеним продукционим окружењима, примјењујући савремене стандарде, најбоље праксе и међународне сигурносне оквире. Његов стручни профил карактерише континуирано професионално усавршавање и активно праћење савремених технолошких трендова.

Аутор је и коаутор 16 научних радова публикованих у међународним и домаћим часописима и научним скуповима, од којих је 3 објављен или прихваћен за објављивање у часописима са СЦИ листе.

1.2. Списак објављених и прихваћених радова за објављивање кандидата

Библиографија кандидата обухвата следеће радове:

Рад у истакнутом међународном часопису (М22):

Камиш, А. , Закиц, А., Поповиц, Г. , Богавац, М., Милиц Д., Игњатовиц Б., Лакхми Ц. Ј. (2026)." *Development of a cloud-based WebRTC VoIP application using the Docker platform for an educational environment,* International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 2334-8496

Рад у међународном часопису (М23):

Камиш, А., Закиц, А., & Кукољ, С. (2023).*Elimination of interference with wireless mesh networks through binary symmetrical channels*. STED Journal - Journal of Social and Technological Development, 2637–2614. https://doi.org/10.7251/STED2302074K

Кукољ, С., Деретиц, Н., & **Камиш, А**.(2023).*Research on the quality of work life and employee motivation in IT company*. SCIENCE International Journal, Skopje, North Macedonia, 2(3). https://doi.org/10.35120/sciencej0203157k

Саопштења са међународног скупа штампана у целини (М33):

Поповиц Г., **Камиш А.**, Закиц А., Игњатовић Б., Милиц Д., Сарцевиц Дј. (2026), *Процјена сајбер ризика вођена вјештачком интелигенцијом у савременим пословним информационим системима*. 25th International Symposium INFOTEH-JAHORINA

Дениц, Н., Милосевиц, М., **КамишА**., Михајловиц, С., Милиц, С. (2025).*New possibilities and paradigms of applying artificial intelligence in electronic business*. 7th International conference on applied engineering and natural sciences icaens 2025, Turkey

Камиш, А., Закиц, А., Закиц, М. , Деретиц, Н., (2025).*"Eyes wide open" – one of the fundamentals of information security,* XIV International Conference on Social and Technological Development Trebinje BIH, 2303-498X.

Закиц, А., Закиц М., Трајковиц, С., **Камиш, А**. *Github copilot: budućnost veb razvoja,* IV Scientific Meeting "Balkan on Jahorina 2025" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667.

Камиш, А., Закиц, А., Кукољ, С., Деретиц, Н., (2024).,W*avelet transformation with examples,* XIII International Conference on Social and Technological Development Trebinje BIH, 2303-498X.

Камиш, А., & М Стаменковић, Н.(2023). *Defense in Depth of modern radio systems.* XII International Conference on Social and Technological Development Trebinje BIH, 2303-498X.

Камиш, А., Кукољ, С., Пењисевиц, А., & Санцанин, Б. (2023). *Defense in Depth protection strategy against social engineering and phishing attacks*. II Scientific Meeting "Balkan on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667.

Камиш, А. (2022). *Establishing secure communication using SSL VPN*. XI International Conference on Social and Technological Development Trebinje BIH, 2303-498X.

Камиш, А. (2022*). Creating cloud based WEBRTC voice over IP applications for wired and wireless users*. XI International Conference on Social and Technological Development Trebinje BIH, 2303-498X.

Закиц, М., **Камиш, А.**, & Закиц А.(2022). *Status and perspectives of the development of electronic government in the countries of the Western Balkans*. I Scientific Meeting "Balkan on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667.

Трајковиц, С., Јаксиц, К., **Камиш, А.**, & Закиц, М. (2022).*Integration of electronic services during the Covid 19 pandemic*. I Scientific Meeting "Balkan on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667. -

Камиш, А. (2020). *Methodological basis of designing, implementation and administration IoT.* IX International Conference on Social and Technological Development Trebinje BIH, 2303-498X. https://doi.org/10.7251/ZRPIM2001359K

Камиш, А. (2020). Cyber attack and threat protection. IX International Conference on Social and Technological Development Trebinje BIH, 2303-498X. https://doi.org/10.7251/ZRPIM2001365K

Научна компетентност кандидата из области докторске дисертације:

Категорија	M22	M23	M33	**Укупан индекс**
Број радова	1	1	10	
Бодови	5	3	1	
Укупно	5	3	10	18

Укупна научна компетентност кандидата:

Категорија	M22	M23	M33	**Укупан индекс**
Број радова	1	2	13	
Бодови	5	3	1	
Укупно	5	6	13	24

1.3 Назив рада и име часописа у коме је кандидат као први аутор објавио рад у складу са стандардима

Кандидат је испунио услов који је предвиђен чланом 30. Правилника, којим треба да има као први аутор најмање један рад објављен или прихваћен за објављивање у часопису са СЦИ листе, који је садржајем повезан са докторском дисертацијом. Кандидат има један објављен научни рад и један научни рад прихваћен за објављивање као први аутор у часописима са СЦИ листе, који су садржајем повезани са докторском дисертацијом:

Рад у истакнутом међународном часопису (M22):

Камиш, А. , Закиц, А., Поповиц, Г. , Богавац, М., Милиц Д., Игњатовиц Б., Лакхми Ц. Ј. (2026)." *Development of a cloud-based WebRTC VoIP application using the Docker platform for an educational environment,* International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 2334-8496

Рад у међународном часопису (M23):

Камиш, А., Закиц, А., & Кукољ, С. (2023).*Elimination of interference with wireless mesh networks through binary symmetrical channels*. STED Journal - Journal of Social and Technological Development, 2637–2614. https://doi.org/10.7251/STED2302074K

2. ОСНОВНИ ПОДАЦИ О ДОКТОРСКОЈ ДИСЕРТАЦИЈИ

2.1 Наслов докторске дисертације

Наслов докторске дисертације на српском језику: Defense in depth стратегија информационе сигурности за предузећа мале и средње величине у БиХ.

Наслов докторске дисертације на енглеском језику: Defense in Depth Strategy for Information Security in Small and Medium-Sized Enterprises in Bosnia and Herzegovina.

2.2 Научна област докторске дисертације

Истраживања спроведена у оквиру докторске дисертације „Defense in Depth стратегија информационе сигурности за мала и средња предузећима у Босни и

Херцеговини“ припадају основном научно-образовном пољу техничко-технолошких наука, у оквиру опште научне области информационо-комуникационих технологија, са посебним фокусом на ужу научну област информационе сигурности.

Дисертација се такође сврстава у научну област електротехнике и рачунарског инжењерства, односно ужу научну област рачунарских наука.

У складу са тематиком истраживања, посебан акценат је стављен на примену савремених приступа заштити информационих система, укључујући концепт „Defense in Depth “ за информациону сигурност у малим и средњим предузећима у Босни и Херцеговини.

2.3 Садржај докторске дисертације

Докторска дисертација кандидата Ален Камиша написана је на 156 страна (не укључујући биографију и изјаве), укључује 1 график, 6 табелљ, као и 356 литературна навода. Докторска дисертација садржи шест поглавља (не укључујући Прилоге и Биографију): Увод, Теоријско разматрање о информационој сигурности, Defense in Depth стратегија информационе сигурности, Рроцјена свијести о сајбер сигурности, Побољшање информационе безбједности примјеном Defense in Depth за МСП у БИХ, Закључак, Литература.

2.4 Кратак опис појединачних поглавља докторске дисертације

Докторска дисертација је организована у следеће логички повезане целине:

Прво поглавље рада представља увод у истраживану проблематику информационе сигурности у малим и средњим предузећима у Босни и Херцеговини. Дефинисан је предмет истраживања кроз анализу изазова савремених сајбер пријетњи, са посебним освртом на техничке и организационе аспекте заштите информационих система . Истакнут је значај интегрисаног приступа управљању безбједносним ризицима, укључујући улогу људског фактора и савремених метода заштите. У оквиру поглавља дефинисан је циљ истраживања, који се односи на развој и примјену Defense in Depth приступа у унапређењу информационе сигурности. Такође су постављене истраживачке хипотезе које се односе на ефикасност предложеног модела у смањењу ризика и повећању

Друго поглавље поставља теоријске основе истраживања и пружа систематичан преглед релевантне научне и стручне литературе из области информационе сигурности. У оквиру поглавља разматрају се основни појмови и значај информационе сигурности, укључујући њену улогу у савременом пословању, као и јасно разграничење између информационе и сајбер сигурности. Посебна пажња посвећена је анализи глобалних оквира и стандарда, као што су ISO 27001 и NIST, уз осврт на међународне стандарде, регулаторне захтеве и утицај глобализације и дигитализације на безбједносне изазове. Поглавље такође обухвата улогу националних институција у систему сајбер заштите, са акцентом на функцију и значај CERT тимова, као и препоруке за њихов даљи развој. У завршном дијелу

анализирају се савремене информационе пријетње, укључујући активности сајбер криминалаца, еволуцију малвера и актуелне типове напада. Оваква свеобухватна анализа представља основу за разумевање комплексности безбједносног окружења и поставља темељ за развој ефикасних модела заштите у наставку дисертације.

Треће поглавље доноси детаљан приказ концепта Defense in Depth стратегије информационе сигурности, са циљем да се постави теоријски оквир за њену примену у савременим информационим системима. У оквиру поглавља дефинисан је појам и значај ове стратегије, приказан њен историјски развој, као и разлике у односу на друге приступе заштити. Посебна пажња посвећена је анализи предности и ограничења слојевитог приступа безбједности. Поглавље обухвата детаљну разраду кључних слојева Defense in Depth стратегије, укључујући периметарску и унутрашњу заштиту, механизме аутентификације и ауторизације, као и улогу корисничке едукације и подизања свијести о сајбер безбједности. Такође се разматрају аспекти редундантности и опоравка од катастрофе, кроз анализу backup стратегија и планова континуитета пословања. У наставку су представљени механизми надзора и мониторинга, укључујући примену SIEM система, реално-временског праћења и аналитике безбједносних догађаја. Поглавље такође обухвата безбједност апликација кроз принципе сигурног кодирања и тестирања рањивости, као и управљање идентитетима кроз IAM системе и управљање животним циклусом корисничких налога. Овако постављен теоријски оквир представља основу за даљу примену и евалуацију Defense in Depth стратегије у контексту истраживања.

Четврто поглавље приказује процену свијести о сајбер сигурности у оквиру истраживања, са циљем да се утврди ниво знања, перцепције ризика и понашања запослених у контексту информационе безбједности. У оквиру поглавља представљена је методологија истраживања, укључујући приступ прикупљању података и избор релевантних метода анализе. Посебна пажња посвећена је креирању и примени упитника намењеног особљу компанија, који је коришћен за прикупљање података о свијести и праксама у области сајбер сигурности. У циљу статистичке обраде података примењен је χ^2 (hi-kvadrat) тест, који омогућава анализу зависности између посматраних варијабли у контексту информационе безбједности. У завршном дијелу поглавља представљени су резултати истраживања и спроведених интервјуа, уз интерпретацију добијених података и идентификацију кључних слабости и потенцијала за унапређење свијести о сајбер сигурности у организацијама. Ови резултати представљају основу за даље дефинисање мера и модела за побољшање безбједносне праксе.

Пето поглавље се бави унапређењем информационе безбједности применом Defense in Depth стратегије у малим и средњим предузећима у Босни и Херцеговини. У оквиру поглавља анализирају се кључни изазови са којима се МСП суочавају, са посебним освртом на ограничене ресурсе и потребу за оптималним одређивањем приоритета улагања у безбједност. Посебна пажња посвећена је анализи ризика прије и након имплементације Defense in Depth стратегије, кроз више сценарија који укључују различите нивое заштите – од основних контрола као што су firewall и вишефакторска аутентификација, до напреднијих

мера као што су сегментација мреже, едукација корисника, мониторинг и SIEM системи, као и усклађеност са ISO 27001 стандардом. Оваквим приступом омогућена је свеобухватна процена унапређења информационе безбједности у зависности од нивоа имплементираних контрола.

У оквиру подpoglavља које се односи на разматрање и анализу резултата примене Defense in Depth стратегије, извршена је интерпретација добијених резултата, при чему је потврђено да предложени модел у потпуности верификује постављене истраживачке хипотезе.

У завршном дијелу поглавља дат је осврт на будући развој Defense in Depth стратегије, са посебним акцентом на примену машинског учења и вештачке интелигенције у области информационе безбједности, укључујући детекцију аномалија, предиктивну анализу пријетњи и аутоматизоване одговоре на безбједносне инциденте. Ови правци развоја указују на потенцијал даљег унапређења система заштите у динамичном сајбер окружењу.

Шесто поглавље закључује рад осврtом на спроведено истраживање, при чему се издвајају најзначајнији резултати који су произашли из анализе информационе безбедности и примене Defense in Depth стратегије. Посебно је истакнут значај добијених резултата у контексту унапређења заштите информационих система у малим и средњим предузећима, као и њихов допринос разумевању управљања сајбер ризицима.

Поглавље указује на практичну применљивост предложеног модела, посебно у условима ограничених ресурса, и наглашава значај систематског и слојевитог приступа информационој безбједности. Такође, отвара се простор за будућа истраживања, са посебним освртом на примену напредних технологија као што су машинско учење и вештачка интелигенција у циљу даљег унапређења сајбер сигурности.

У литератури поглављу излистани су литературни наводи који су коришћени у овој докторској дисертацији.

3. ОЦЕНА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

3.1 Предмет докторске дисертације

Предмет истраживања докторске дисертације обухвата проучавање информационе безбедности у малим и средњим предузећима у Босни и Херцеговини, са посебним освртом на примену Defense in Depth стратегије у циљу унапређења заштите информационих система. Истраживање је развијено у оквиру области информационих технологија и рачунарских наука, при чему интегрише техничке, организационе и људске аспекте сајбер безбедности, са циљем превазилажења постојећих ограничења у приступу заштити података и система.

Дисертација полази од чињенице да савремена мала и средња предузећа, упркос све већој зависности од дигиталних технологија, често немају адекватно развијене безбедносне механизме, што их чини посебно рањивим на различите облике сајбер претњи. Традиционални приступи заштити често су фрагментисани и не пружају довољан ниво

отпорности, док ограничени ресурси додатно усложњавају имплементацију свеобухватних безбедносних решења. У том контексту, Defense in Depth стратегија се издваја као систематичан и слојевит приступ који омогућава интеграцију различитих безбедносних контрола у циљу смањења ризика.

Досадашња истраживања указују на недостатак јединственог и практично применљивог модела који је прилагођен специфичностима МСП, посебно у условима ограничених финансијских и људских ресурса. Такође, недовољна свест запослених о значају сајбер безбедности и недовољна интеграција организационих и техничких мера представљају додатне изазове у успостављању ефикасног система заштите. У том смислу, дисертација се бави релевантним научним проблемом који се односи на анализу, процену и унапређење информационе безбедности кроз примену слојевитог приступа заштити, уз укључивање више нивоа безбедносних механизама и пракси.

Предмет ове дисертације је значајан и актуелан, јер се бави комплексним изазовима заштите информација у савременом дигиталном окружењу, са јасним потенцијалом да допринесе унапређењу постојећих теоријских знања и понуди применљив модел за побољшање безбедносне праксе у малим и средњим предузећима.

3.2 Циљ докторске дисертације

У оквиру рада, кандидат се усмерава на реализацију општег циља докторске дисертације – истраживање унапређења информационе безбедности у малим и средњим предузећима у Босни и Херцеговини кроз примену Defense in Depth стратегије. Посебан акценат стављен је на анализу постојећих безбедносних изазова, процену нивоа сајбер свести запослених, као и на дефинисање и евалуацију слојевитог модела заштите у условима ограничених ресурса. Реализација општег циља остварена је кроз три фазе:

1) Аналитичку фазу, у којој је извршена анализа стања информационе безбедности у МСП, идентификација кључних ризика, претњи и рањивости, као и процена нивоа свести запослених путем упитника и интервјуа.
2) Фазу моделовања, у којој је развијен модел Defense in Depth стратегије прилагођен МСП, кроз дефинисање више нивоа безбедносних контрола (firewall, MFA, сегментација мреже, едукација корисника, мониторинг и SIEM), уз анализу њиховог утицаја на смањење ризика.
3) Фазу примене, која је обухватила евалуацију предложеног модела кроз поређење стања безбедности пре и након имплементације различитих нивоа заштите, као и формулисање препорука за практичну примену у МСП.

Општи циљ је разложен на подциљеве – дефинисане конкретне кораке истраживања, који укључују:

- анализу стања информационе безбедности у МСП,
- процену нивоа сајбер свести запослених,

- идентификацију кључних безбедносних ризика и рањивости,
- развој слојевитог модела заштите заснованог на Defense in Depth приступу,
- евалуацију ефеката примене различитих безбедносних контрола,
- и формулисање препорука за унапређење информационе безбедности у МСП.

Циљ докторске дисертације је јасно формулисан, систематично операционализован кроз међусобно повезане фазе истраживања и у потпуности реализован кроз анализу, моделовање и примену предложеног приступа.

3.3 Хипотезе од којих се полазило у истраживању

На основу јасно дефинисаног предмета и циља истраживања, као и формулисаних истраживачких корака и полазних претпоставки, у оквиру докторске дисертације доказана су сбе истраживачке хипотезе (општа и помоћне), које гласе:

H0: Могуће је имплементирати Defense in Depth стратегију информационе безбедности и у зависности од величине компаније изабрати потребни хардвер и софтвер који ће унапредити и заштитити информациони систем. Имплементацијом стратегије смањује се ризик информационе безбедности. Стратегија је и додатна полазна тачка за увођење додатних квалитета компанији кроз сертификацију за ISO стандарде (нпр. ISO 9000, 9001, 22301 и 27001).

H2: Стратегија Defense in Depth повећава сигурност информационог система, а самим тим и целокупне компаније.

H3: Кроз имплементацију нових платформи уводи се склад и хармонизација процеса компаније која на крају доводи до задовољавања светских стандарда.

H4: Имплементација Defense in Depth стратегије смањује ризик од злоупотребе података.

H5: Defense in Depth стратегија помаже у смањењу финансијских губитака услед безбедносних инцидената.

H6: Defense in Depth стратегија побољшава перцепцију и поверење клијената и партнера у компанију.

H7: Имплементација Defense in Depth стратегије захтева већи број техничких ресурса (заснованих на новој AI, ML и Docker инфраструктури) у већим компанијама.

На основу спроведене анализе и добијених резултата, може се закључити да су све појединачне хипотезе потврђене у складу са очекивањима, што пружа снажну емпиријску

подршку генералној истраживачкој хипотези и потврђује њену научну оправданост у контексту дефинисаних циљева дисертације.

3.4 Остварени резултати и научни допринос докторске дисертације

Докторска дисертација припада области информационе безбедности и рачунарских наука, са посебним фокусом на анализу, унапређење и примену Defense in Depth стратегије у малим и средњим предузећима у Босни и Херцеговини. У раду је успешно адресиран низ истраживачких празнина, од којих је посебно значајна недовољна заступљеност систематичних и практично применљивих модела информационе безбедности прилагођених специфичностима МСП.

Остварен је допринос у теоријском разумевању информационе безбедности кроз анализу савремених сајбер претњи, рањивости система и улоге људског фактора у заштити информација. Развијен је модел заснован на Defense in Depth приступу, који омогућава структурисану имплементацију више нивоа безбедносних контрола, чиме се постиже већи степен отпорности информационих система. Предложени модел показује значајно унапређење у смањењу ризика, што потврђује његову практичну применљивост.

Поред тога, рад је донео оригиналан допринос кроз формулисање практично применљивих смерница за унапређење информационе безбедности у МСП. Ове смернице су резултат анализе односа између техничких, организационих и људских фактора, и имају значајан потенцијал за примену у реалним пословним окружењима. Оне могу послужити као основ за доношење одлука у области безбедности, као и за планирање инвестиција у безбедносну инфраструктуру.

Такође, предложен је модел имплементације који обухвата више нивоа заштите, укључујући firewall системе, вишефакторску аутентификацију, сегментацију мреже, едукацију корисника, мониторинг и примену SIEM решења. Овај приступ представља технолошки и методолошки искорак ка успостављању интегрисаног система заштите који је прилагођен ограниченим ресурсима МСП. Резултати истраживања могу се применити у постојећим информационим системима, као и користити као основ за даљи развој безбедносних стратегија.

Један од значајних аспеката дисертације јесте примена добијених резултата, који имају вредност како у научном, тако и у практичном смислу. Предложени модел и смернице омогућавају унапређење безбедносне праксе, смањење ризика и повећање поверења корисника и партнера. У светлу све већих сајбер претњи, овај рад пружа основу за даља истраживања и развој напредних решења у области информационе безбедности.

Верификација резултата истраживања потврђена је кроз објављивање више научних радова у релевантним међународним часописима, чиме је дат значајан научни допринос у области којом се дисертација бави.

4. ЗАКЉУЧАК И ПРЕДЛОГ

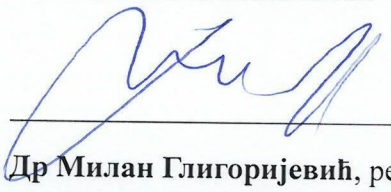
Током писања овог извештаја Комисија је узела у обзир све релевантне чињенице које формирају коначну слику о докторској дисертацији. Докторска дисертација кандидата Алена Камиша под називом „Defense in depth стратегија информационе сигурности за предузећа мале и средње величине у БиХ“ у целини је написана у складу са образложењем које је наведено у пријави теме и испуњава све законске, формалне и суштинске услове и критеријуме који се примењују приликом вредновања докторске дисертације.

Током израде докторске дисертације, кандидат је спровео детаљан преглед научне и стручне литературе из релевантних научних области повезаних са проблематиком информационе безбедности. Већина анализираних радова потиче из врхунских међународних часописа и објављена је од стране истакнутих стручњака у области која је предмет истраживања. Овим прегледом кандидат је стекао свеобухватан увид у досадашње резултате истраживања који се тичу обрађиване проблематике.

Научни доприноси, иновативан приступ примени Defense in Depth стратегије, као и анализа и евалуација предложеног модела у реалном окружењу показују зрелост кандидата и способност за самосталан научно-истраживачки рад. Комисија је мишљења да докторска дисертација садржи оригиналне научне доприносе са доказаном практичном применом у области информационе безбедности, укључујући унапређење заштите информационих система, смањење ризика од сајбер претњи, као и формулисање смерница за имплементацију безбедносних стратегија у малим и средњим предузећима.

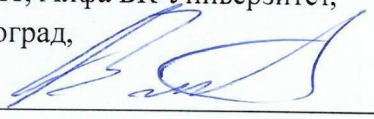
На основу претходно изнетих чињеница, као и на основу детаљне оцене дисертације, Комисија са задовољством предлаже Већу за последипломске студије Алфа БК Универзитета да се докторска дисертација под наведеним насловом прихвати, изложи на увид јавности и упути на коначно усвајање Сенату Алфа БК Универзитета, а кандидату одобри јавна одбрана докторске дисертације.

ЧЛАНОВИ КОМИСИЈЕ



Др Милан Глигоријевић, редовни професор, председник

ФИТ, Алфа БК Универзитет, Београд,



Др Александар Закић, доцент, ментор

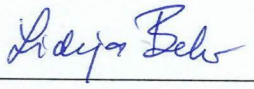
ФИТ, Алфа БК Универзитет, Београд,

Др Славиша Трајковић, редовни професор, члан

Економски факултет, Универзитет у Приштини, Косовска Митровица

Др Јелена Стојановић, доцент, члан

ФМРН, Алфа БК Универзитет, Београд,



Др Лидија Беко, редовни професор, члан

Рударско-геолошки факултет,

Универзитет у Београду, Београд