УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Број: _____

Датум: _____
Београд, Господара Вучића бр. 50

НАСТАВНО-НАУЧНОМ ВЕЋУ
ФАКУЛТЕТА БЕЗБЕДНОСТИ УНИВЕРЗИТЕТА У БЕОГРАДУ

Одлуком донетој на 9. седници Наставно-научног већа Факултета безбедности Универзитета у Београду, одржаној дана 17.06.2020. године, одређена је Комисија за преглед и оцену докторске дисертације кандидата мр Перице Милетића под насловом: „Организационо и нормативно уређење заштите информација у функцији безбедности пословања банака и финансијских институција“ у саставу: др Бранкица Поповић, ванредни професор, Криминалистичко-полицијски универзитет, др Ненад Путник, ванредни професор Факултета безбедности Универзитета у Београду и др Меленко Ћелетовић, ванредни професор Факултета безбедности Универзитета у Београду.

Након што је прегледала и оценила рукопис докторске дисертације, Комисија подноси Наставно-научном већу Факултета безбедности следећи

РЕФЕРАТ О ЗАВРШЕНОЈ ДОКТОРСКОЈ ДИСЕРТАЦИЈИ

1. Основни подаци о кандидату

Кандидат мр Перица (Бранислав) Милетић, рођен је 30. марта 1964. године у Задру. Основно и средње образовање завршио је у Београду. Дипломирао је на Факултету Народне одбране 1991. године. Магистарски рад на тему "Образовање и иновација знања кадра безбедности и физичко-техничке заштите у предузећима и установама" одбранио је 2002. године.

Професионалну каријеру започео је на Факултету цивилне одбране (1994. до 1995. године), као млади истраживач, ангажован на прикупљању и обради података у оквиру пројекта „Заштита становништва од елементарних непогода и хемијских акцидената". Од 1995. до 2003. године проводи у ЈП ПТТ Саобраћаја „Србија", Сектору за безбедност, на стручним пословима планирања, организације и контроле физичко-техничке заштите. Од 2003. до 2005. године је ангажован у белгијско-српском предузећу за пружање безбедносних услуга, *Security consultancy and Partners International (SCPI)*, Београд, на позицији директора безбедносних услуга, одакле прелази у *Raiffesein* банку на позицију руководиоца Одељења безбедности и заменика руководиоца, где остаје до 2017. године, када прелази у шведско предузеће за пружање безбедносних услуга – *Securitas SE*, Београд, на позицију националног директора. Од 2017. године ангажован је као самостални консултант у области приватне бебедности.

Од 2002. до 2007. године учествовао је у планирању и организацији специјалистичких студија безбедносног менаџмента, Факултет безбедности, Универзитет у Београду, за област безбедносног менаџмента у банкама и финансијским институцијама. Од 2003. до 2013. године био је потпредседник Центра за превенцију криминалитета, Института за криминолошка и социолошка истраживања, где је учествовао у више пројеката едукације стручног кадра за приватну безбедност (Нафтна индустрија Србије, Агробанка, Београдска пекарска индустрија и друго). У периоду од 2007. до 2015. године, један је од оснивача и председавајући *American Society for Industrial Security (ASIS)*, Одељења у Србији, организације професионалаца у приватној безбедости која се претежно бави професионалном едукацијом стручних кадрова и одговарајућом цертификацијом. Такође, један је од оснивача и председник Групације менаџера безбедности у банкама, Одбора за банкарство и осигурање Привредне коморе Србије, у периоду од 2007. до 2017. године, првог удружења професиналаца у овој области код нас, које се бавило разменом искустава најбоље праксе и сарадњом са одговарајућим државним институцијама и међународним удружењима, по питањима која су од значаја за безбедност ових привредних субјеката.

Кандидат Милетић, учествовао је на различитим научним и стручним скуповима у земљи и иностранству. Објавио је више радова из области безбедности. Говори енглески језик.

Списак објављених радова кандидата:

- *Терор и тероризам*, зборник радова, Висока полицијска школа, Бања Лука, 2002. година;
- *Стање у области едукације кадра физичко-техничког обезбеђења – кадровска структура запослених у ЈП ПТТ Саобраћаја "Србија"*, зборник радова, Виша школа унутрашњих послова, Београд, 2003. година;
- *Значај развоја области "Private Security" и неки проблемски аспекти едукације професионалног кадра*, зборник радова, Институт за криминолошка и социолошка истраживања и Виша школа унутрашњих послова, Београд, 2003. година;
- *Едукација људских ресурса у области "Private Policing" – Република Србија*, зборник радова, Прва међународна конференција "Безбедност имовине и пословања - *Private Policing*", Факултет цивилне одбране и Центар за превенцију криминалитета, Београд, 2004. година;
- *Због чега ће међународна искуства у области едукације Security кадрова променити цивилни сектор безбедности у Србији*, XVI семинар права, "Тешки облици криминала", Будва, 2004. година;
- *Безбедносна провера запослених*, коаутор са Мандић, Г., The 7th scientific and professional conference – Management and safety, CONFERENCE THEME: Human resource management and safety, Чаковец, Хрватска, 2012. година.

2. Основни подаци о докторској дисертацији

Одлуком Универзитета у Београду 02-03 број: 61206-5884/-14 од 03.02.2015. године, кандидату мр Перици Милетићу одобрена је тема за израду докторске дисертације под насловом „Организационо и нормативно уређење заштите информација у функцији безбедности пословања банака и финансијских институција”, а за ментора је одређен проф. др Горан Мандић. На основу молбе кандидата бр. 700/5-13 од 29.11.2019. године, Факултет безбедности, Универзитет у Београду, одобрио је кандидату продужење рока за одбрану докторске дисертације одлуком бр. 778/7 од 25.12.2019. године – и то, до 30.09.2020. године. Кандидат је 12.05.2020. године предао текст дисертације обима 347 страна основног текста (А4 формат, ћирилични фонт 12, проред 1,0) који је усаглашен са стандардима Универзитета у Београду у погледу форме и садржаја докторске дисертације.

Структуру рада чине резиме на српском и енглеском језику, методолошки оквир истраживања, четири поглавља, закључак, списак коришћене литературе и прилози. Основна литература садржи 161 библиографску јединицу. Прилози садрже: биографију кандидата, изјаву о ауторству, изјаву о истоветности штампане и електронске верзије докторског рада и изјаву о коришћењу.

2.1. Предмет и циљ дисертације

Кандидат за предмет истраживања узима заштиту информација у банкама и финансијским институцијама, првенствено полазећи од организационог и нормативног аспекта уређења и обављања ових послова.

Два су основана разлога за овакав кандидатов одабир предмета исраживања: са једне стране он опажа значај нормативне уређености и организације, као претпоставке успешног функцинисања пословних функција, а посебно безбедносне пословне функције, док са друге стране уочава у пракси поистовећивање заштите информација (енгл: *Information Security - IS*) са информатичком заштитом (engl: *IT security*). Кандидат у овоме види опасност занемаривања других сегмената система безбедности за рачун, информационе безбедности – чиме се даље, како кандидат тврди, долази до конституисања некомплетног система безбедности, посебно у смислу његове неравномерне функционалне развијености и неефикасности у пракси.

Научни приступ у конципирању система безбедности подразумева разматрање свих извора угрожавања. У области заштите информација, то подразумева пре свега свест, а затим и прихватање специфичности које са собом носе технолошка знања и достигнућа у сфери информационих технологија, али и потреба да се овом проблему приступи систематично, одакле се информационе технологије могу посматрати као средство у постизању циљева система безбедности.

Заштита података у банкама и финансијским установама, са посебним освртом на организационо и нормативно уређење, није тако често спомињана тема у научним радовима у свету, док су у домаћој пракси ретки научни радови који се уопште баве информационом безбедношћу.

Кандидат је посматрао резултате истраживања у тринаест, по предмету свог истраживања, сродним научним радовима, па тако наводи да се на овај начин дошло до следећих закључака:

- савремена истраживања указују да се у безбедносним политикама заштите информација запоставља друштвени карактер ових феномена;
- приликом одређивања програмског садржаја у безбедносним обукама, првенствено у области развоја безбедносне свести (енгл: *Security Awareness*), примећује се да су безбедосне политике, обуке и сам кадар који обавља ове послове неоправдано често (само) техничке природе, те да је последица оваквог стања занемаривање других приступа (погледа), посебно погледа из угла друштвеног аспекта овог проблема;
- доказана је претпоставка да је у области заштите информација најцелисходније имати такав приступ који се базира на знањима и друштвених и техничких наука;
- запослени су највећа претња заштити информација, и у остваривању ове заштите најважнији је квалитет информација које запослени имају.

Кандидат примећује комплексност теоријског одређења кључних појмова и наводи да се она карактерише двема чињеницама: не постоји теоријска усаглашеност око самог појма безбедности, па тиме ни појмова који извиру из овог појмовног одређења и – област заштите информација, карактерише доминација информационе безбедности. Кандидат примећује и директну последицу овакве доминације, па тако примећује масовно преузимање неких појмова који су на глобалном нивоу опште прихваћени, са често основаним образложењем да су неки од појмова тешко преводиви (софтвер, хардвер, бекап, логовање, редундантност, интернет, ПИН код, пасворд, итд.) – али да је овакав тренд присутан чак и онда када за тим не постоји потреба.

Полазећи од предмета истраживања овог рада, кандидат је посебну пажњу посветио начину организовања заштите информација у банкама и сугерише да се у будућим истраживањима треба проучавати проблем са аспекта организационог понашања, полазећи од значаја који имају мотивација запослених, организационо учење, преговарање,

управљање конфликтима, организациона култура, а посебно свест коју запослени имају о потреби заштите информација.

Кандидат је операционо одређење предмета истраживања спровео кроз реализацију следећих истраживачких етапа и то:

Прва фаза односи се на теоријско одређење кључних појмова и њихову повезаност - узимајући у обзир начин на који је објашњена ова тематика у научној и стручној литератури.

Друга фаза односи се на анализу постојећег нормативног оквира који се бави питањем заштите информација (узимајући у обзир законе, стандарде, препоруке и друго), како на међународном, тако и на домаћем плану.

У *трећој фази* кандидат је сагледао савремене концепције заштите информација користећи допринос теорије и постојећи нормативни оквир, те је на тај начин анализом садржаја утврдио правце развоја система заштите информација у банкама и финансијским установама − у контексту боље фукционализације целокупног безбедносног система у овим субјектима.

Кључни појмови које кандидат наводи су: *Безбедност*, *Информација, Заштита информација*, *Нормативно уређење*, *Организацино уређење*, *Безбедносна свест запослених* (*енгл: Security Awareness*), *Банке и финансијске институције, и друго*.

Предмет истраживања овог рада је одређен већим бројем различитих теоријских дисциплина, међу којима су најзначајније оне из области наука безбедности и заштите као и њима сродних наука, као што су: менаџмент, криминологија, социологија, психологија, због чега ово истраживање има мултидисциплинарни карактер.

Временско одређење предмета истраживања обухвата период од почетка појаве заштите информација у банкама и финансијским институцијама, до данас. Овај период карактеришу динамичне промене у развоју информационих технологија, као и одговарајућих безбедносних ризика – услед чега је дошло и до промена у профилима безбедносних система и померања тежишта од опште ка информационој безбедности.

Кандидат истраживање, у ужем смислу, просторно ограничава на подручје Републике Србије – у делу истраживања нормативног уређења заштите информација, али и, полазећи од чињенице ширине сајбер простора, обухвата савремене трендове у области

система заштите информација у банкама и финансијским институцијама, посматрајући га на међународном нивоу.

Научни циљеви истраживања

Истраживањем је постигнута анализа проблема заштите информација у банкама и финансијским институцијама, са аспекта организационе и нормативне уређености, што посебно добија на значају дигитализацијом друштва, које поприма особине нове техничко технолошке револуције, са једне стране, и – са друге стране, направљен је допринос развоју домаће теоријске мисли на овом пољу, будући да су радови са предметном тематиком ретки и нису мултидисциплинарно опредељени, што налаже феноменологије заштите информација.

Значај истраживања испољава се у проналажењу научно верификованих теоријских и емпиријских сазнања о специфичностима система заштите информација у банкама и финансијским установама и предузимању потребних мера у циљу унапређења овог вида заштите.

Научни циљ истраживања је научна дескрипција и класификација при остваривању система заштите информација у банкама и финансијским институцијама, са аспекта организационе и нормативне уређености и давање научног објашњења о посматраним појавама. Добијена сазнања треба да омогуће унапређење система обезбеђења те функционализацију система безбедности.

Добијена сазнања могу се користити и у другим институцијама, као и државним органима и другим правним лицима. Напади не долазе само из сфере сајбер окружења, већ они стижу из многих других сфера, што опредељује мултидисциплинарност предмета истраживања.

Друштвени циљеви истраживања

Са друштвеног аспекта спроведено истраживање има значај за банке и финансијске институције у погледу организовања и нормативне уређености заштите информација,

чиме се доприноси већем нивоу безбедности како ових правних лица, тако и самих корисника услуга које чине и правна и физичка лица. Такође, резултати истраживања примењиви су и на друге индустрије и државне институције, будући да су истраживањем систематизовани организациони и нормативни принципи који су потребни као основа за развој заштите информација, као и да су у њему наведени главни елементи који су до сада били запостављени, а односе се на нетехнички аспект заштите информација и значај развоја свести људи у овој потреби.

2.2. Основне хипотезе од којих се полазило у истраживању

Кандидат мр Перица Милетић је у истраживању пошао од опште хипотезе да се *заштита информација у банкама и финансијским институцијама у пракси базира на информационој (IT) безбедности, чиме се имплицира развој других неопходних аспеката овог система заштите, а посебно у организационом и нормативном смислу*. Одговарајућим методолошким приступом, што је подразумевало анализу разуличитих извора података и различитих истраживачких метода, као што су: преглед научне и стручне литературе, анализа правних докумената, метод секундарне анализе, метод анализе садржаја, метод моделовања и компаративни метод, верификована је општа хипотеза, као и две посебне хипотезе.

Истраживањем је потрвђено да информациони систем обрађује информације на три нивоа: техничком (софтвер, хардвер, подаци и мрежне компоненте), формалном (документи, безбедносе стратегије, политике, упутства, смернице, стандарди и друго) и неформалном нивоу који се огледа у понашању људи (организациона култура, безбедносна култура, норме, веровања, ставови, неформална комуникација и друго). Кандидат је констатовао да се технички ниво у летаратури односи на информационе ресурсе, одакле се у пракси он често поистовећује са *IT* сегментом остваривања заштите информација (техничким аспектом), на рачун формалног и неформалног нивоа, који одговара организационом и нормативном уређењу заштите информација.

Коришћењем различитих метода и анализом извора података из више научних дисциплина полазна хипотеза је потврђена, будући да се истраживањем дошло до следећих закључака:

- заштита информација подразумева активности које се односе на људе, процесе и технологију;
- информациона безбедност се не може затварати у технички аспект и специфична *IT* знања, већ је потребно да она има активну сарадњу са другим пословним функцијама, а пре свега са другим сегментима система безбдности;
- безбедност информација је вишедимензионална дисциплина, а већина тих димензија је нетехничке природе;
- у структури информационих инцидената учешће запослених тих организација јавља се у значајној мери;
- људи су најслабија карика у ланцу остваривања заштите информација;
- едукација корисника за заштиту информација један је од кључних фактора у остваривању заштите информација и у том смислу обично се говори о развоју безбедносне свести (енгл: *security awareness*);
- тренинзи (обуке) информационе безбедности су углавном техничке природе, јер су безбедносне политике исте такве. Разлог за то је што се менаџери заштите информација претежно ослањају на јавно доступне смернице, политке и стандарде, које су такође техничке природе, па услед недостатка о општим знањима из безбедности писању докумената приступају рутински, користећи туђа решења и неразумевајући шири контекст безбедности;
- безбедност информација зависи од људи, а тренутни програми о развоју безбедносне свести не придају довољно пажње теоријама понашања;
- нормативни и организацнони аспекти у остваривању заштите информација се међусобно прожимају, јер се примена норми огледа у свести о безбедности, која је фундаментална за организацију и њену културу;
- нормативни оквир заштите информација утиче на свест о бебедности корисника (енгл: *security awareness*);
- организационе промене имају значајну улогу за остваривање заштите информација;
- безбедносна култура организације у значајној мери доприноси заштити информација;

- недостатак безбедносне културе је уочљив и на индивидуалном и на нивоу организације;
- у остваривању заштите информација важно је учешће више пословних функција организације, а не само безбедносна пословна функција – потребан је мултидисциплинарни приступ;
- подизање свести о информационој безбедности је могуће остварити преко организационе културе, као механизма контроле. Када у организацији постоји безбедносна култура, аспекти информационе безбедности се реализују као природан, рутински и свакодневни приступ од стране запослених;
- кључну улогу у култури информационе безбедности има пословодство организације, које заједно са запосленима утиче на вредности организације које су некада видљиве а некада не;
- неговање супкултуре безбедности информација не неопходно у организацији. У теорији је добро проучен проблем промене корпоративне културе, али је недовољно проучен процес промене супкултуре заштите информација;
- појавни облици и број напада на информационе системе је у порасту и тај тренд ће се наставити;

Полазна хипотеза је затим разрађена кроз посебне хипотезе.

Прва посебна хипотеза гласи: организациона структура и систематизација организације знатно утичу на профилисање система заштите и одређују његову ефикасност. Услови уске специјализације система заштите на нивоу техничких знања чине да се запостављају друге области које подразумевају ефикасан безбедносни систем, као што су питања физичке безбедности, питања свести запослених о безбедности, друга питања која се односе на безбедносну проблематику коју носе кадрови, проблеме интерних истрага, питања подршке руководећег менаџмента и друго.

На основу спроведеног истраживања прва посебна хипотеза је потврђена, којом приликом се у поступку верификације коришћена научна сазнања која одређују потребне функције за организовање програма заштите информација. Кандидат је констатовао да је данас теорија сагласна да се функције заштите информација и информационих

технологија требају раздвојити у организационом смислу, али и да према доступним информацијама та трансформација иде споро, будући да истраживања упућују на закључак да се заштита информација још увек третира као првенствено техничко питање, али да ће процес дигитализације убрзати тај процес. У многим случајевима, организационе део који је задужен за безбедност информација налази се у структури организације на таквом месту да показује њен маргинални статус. Организације трагају за таквим местом заштите информација у својој структури, које ће омогућити баланс између потреба информационе безбедности и могућности организације. Идеална је позиција која ће да омогући да информациона безбедност постане део организационе културе, са напоменом кандидата да само позиционирање у организационој структури није и гарант да ће послови заштите информација бити оптимално организовани. Избор одговарајућег модела организације послова заштите информација, закључује кандидат, зависи од више елемената, у које спадају: врста индустрије којој припада организација, национална култура (безбедносна култура), географски простор са својим економским особинама тржишта, нормативни оквир, величина организације, старост организације, степен криминалитета окружења, организациона култура, расположиви људски ресурси, пословни циљеви организације, величина буџета организације и друго.

Друга посебна хипотеза гласи: *нормативно организовање послова заштите информација у банкама и финансијским институцијама базира на стварању јединствених основа овакве заштите кроз стварање формалних докумената, који треба да представљају нормативне основе за остваривање ове врсте заштите, али који треба и да стандардизују поступке запослених, у смислу остваривања заштите информација, као и да омогуће њену контролну функцију.* Спроведено истраживање је потврдило и другу посебну хипотезу.

У поступку верификовања ове хипотезе анализирани су међународни и домаћи документи, који се односе на заштиту информација у банкама и финансијским институцијама, као и (интерна) норматива на нивоу самих организација. Анализирајући домаћи нормативни оквир кандидат је издвојио по својој важности Закон о банкама, који одређује обавезу банке да идентификује, мери, процењује и управља ризицима којима је банка изложена у свом пословању, а где се у групи оперативних ризика као ризик препознаје неодговарајуће управљање информационим технологијама. Такође, Одлука о

минималним стандардима управљања информационим системом финансијске институције и Одлука о управљању ризицима банке, кључне су за организовање послова заштите информација у банкама и финансијским институцијама, будући да својим одредбама у знатној мери експлицитно одређују обавезе ових субјеката у наведеном смислу, као што су: израда стратегије развоја информационог система, израда политика безбедности, израда Плана континуитета пословања (енгл: *Business Continuity Plan − BCP*), израда Плана опоравка активности у случају катастрофа (енгл: *Disaster Recovery Plan − DRP*), одређивање резервне локације за опоравак информационог система, стручно оспособљавање запослених за коришћење информационих система и друго. На међународном плану, кандидат поред стандарда серије ISO 27000 оправдано издваја споразум Базел II, будући да он третира оперативни ризик, који је кључан за област заштите информација у банкама и финансијским институцијама, и истиче значај подизања свести запослених и културу понашања у односу на изложеност оперативним ризицима. Посебан допринос кандидата теоријским основама будућих истраживања у области заштите информација у банкама и финансијским институцијама, као и допринос потврђивању хипотезе, дат је кроз анализу документа о сајбер резилијентности финансијске тржишне инфраструктуре, издате од стране Банке за међународна поравнања и Међународне комисије за хартије од вредности, који подразумева да сајбер резилијентност подразумева да: заштита мора да обухвата информатичке ресурсе, али и заштиту људи и процеса; да савремени концепт заштите обухвата и мере нетехничке природе, а посебно да у том смислу обухвата знања која долазе из менаџерских наука о управљању, планирању, организационој култури, едукацији запослених и слично – и, да савремени концепт заштите информација обухвата и неке традиционалне области безбедности, као што су физичко-техничка заштита, безбедносне провере, безбедносне истраге и друго.

2.3. Кратак опис садржаја дисертације

Дисертација се састоји од методолошког оквира истраживања, четири поглавља, закључка, пописа коришћене литературе и прилога. Поглавља су логички повезана и структурирана у већи број потпоглавља:

МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1. ПРИСТУП ПРОБЛЕМУ
2. ПРЕДМЕТ ИСТРАЖИВАЊА
3. ТЕОРИЈСКИ И КОНЦЕПТУАЛНИ ОКВИР ИСТРАЖИВАЊА
4. ОПЕРАЦИОНАЛНО ОДРЕЂЕЊЕ ПРЕДМЕТА ИСТРАЖИВАЊА
5. ВРЕМЕНСКО, ПРОСТОРНО И ДИСЦИПЛИНАРНО ОДРЕЂЕЊЕ

5.1. Временско одређење

5.2. Просторно одређење

5.3. Дисциплинарно одређење

6. ЦИЉ ИСТРАЖИВАЊА

6.1. Научни циљ истраживања

6.2. Практични циљеви истраживања

7. ХИПОТЕТИЧКИ ОКВИР
8. НАЧИН ИСТРАЖИВАЊА

I ПРЕГЛЕД РЕЛЕВАНТНИХ НАУЧНИХ РАДОВА

i. Разумевање и мерење културе информационе безбедности у земљама у развоју: случај Саудијске Арабије
ii. Управљање информационом безбедности: студија случаја културе информационе безбедности
iii. Друштвено-организациони приступ управљању безбедности информационих система у контексту интернет банкарства
iv. Безбедност електронског банкарства и организационе промене
v. Анализа упоређивања препорука најбоље праксе и законских услова приликом подизања свести кућних корисника онлајн банкарства
vi. Управљање пословима IT безбедности – упоредна студија у Пакистану и Краљевини Шведској
vii. Кибер ратовање – нови облик савремених друштвених конфликата
viii. Коцепт безбедносне културе и претпоставке његовог развоја
ix. Испитивање односа између организационих система и безбедоности информација
x. Како банке поступају у случају безбедносних инцидената на примеру оружаног разбојништва – питање кризног менаџмента
xi. Десет смртних грехова информационе безбедности
xii. Успостављање организационе културе информационе безбедности у организацијама: приступ на основу едукације

xiii. Обликовање перцепције менаџера кроз обуке о развоју безбедносне свести

xiv. Закључна разматрања поглавља

II ИНФОРМАЦИОНА БЕЗБЕДНОСТ

1. Значај заштите информација

1.1. Осврт на значење појмова информациона безбедност (енгл: Information Security − IS) и сајбер/ IT безбедност (енгл: Cyber/IT Security)

1.2. Информација и информатичко доба

1.3. Историјски развој информацине безбедности

1.4. Вредност информације

1.5. Информациона безбедност

1.6. Мере и стратегије заштите информационих система

2. Организационо уређење заштите информација

3. Место информационе безбедности у организацији

3.1. Информациона безбедност у оквиру IT послова

3.2. Информациона безбедност у оквиру безбедносне пословне фукције

3.3. Информациона безбедност у оквиру општих послова

3.4. Информациона безбедност у оквиру послова стратегије и развоја

3.5. Информациона безбедност у оквиру правних послова

3.6. Информациона безбедност у пословима осигурања и управљања ризиком

3.7. Организовање заштите информација у другим пословним функцијама

4. Нормативно уређење заштите информација

5. Нормативно уређење заштите информација у организацијама

6. Закључна разматрања поглавља

III НОРМАТИВНО УРЕЂЕЊЕ ЗАШТИТЕ ИНФОРМАЦИЈА У БАНКАМА И ФИНАНСИЈСКИМ ИНСТИТУЦИЈАМА

1. Уставни и законски оквир заштите података

1.1. Законска регулатива прикупљања, обраде и заштите података

1.2. Тајност података

1.3. Заштита пословне тајне

1.4. Заштита података о личности и слободан приступ информацијама од јавног значаја

1.5. Нормативни оквир информационе безбедности

2. Интерни акти правног лица и процена ризика у заштити података

2.1. Правилник о пословној тајни

2.2. Правилник о приватности

2.3. Безбедносна правила и процедуре

2.4. Свест о безбедности и потреби примена нормативних мера за заштиту информација

3. Нормативни оквир заштите информација у банкама и финансијским институцијама

3.1. Појам и дефиниција банке

3.2. Класификација банака

3.3. Народна банка Србије (НБС)

3.4. Управљачка структура банке

3.5. Организациона јединица за контролу усклађености банке

(енгл: Compliance Unit)

3.6. Организациона јединица унутрашње ревизије (енгл: Internal Audit)

3.7. Организација банке по пословима

3.8. Територијална организованост банака

3.9. Банкарски ризици

3.10. Банкарски ризици у светлу кризе изазване вирусом COVID −19

4. Домаћи нормативни оквир у остваривању заштите информација у банкама и финансијским институцијама

4.1. Закон о банкама

4.2. Одлука о минималним стандардима управљања информационим системом финансијске институције

4.2.1. Основни појмови

4.2.2. Оквир за пурављање информациним системом

4.2.3. Управљање ризиком информационог система и унутрашња ревизија

4.2.4. Безбедност информационог система

4.2.5. Управљање континуитетом пословања и опоравак активности у случају катастрофа

4.2.6. Развој и одржавање информационог система

4.2.7. Поверавање активности у вези са информационим системом трећим лицима

4.2.8. Електронске услуге

4.3. Одлука о управљању ризима банке

4.3.1. Стратегија, политике и процедуре

4.3.2. Унутрашња организација (организациона структура)

4.3.3. Процес управљања ризицима

4.3.4. Систем унутрашњих контрола

4.3.5. Информациони систем

4.3.6. Систем извештавања о ризицима

4.3.7. Стрес тестирање

4.3.8. Управљање оперативним ризицима банке

4.3.9. Ризици који настају по основу активности које је банка поверила трећим лицима

4.3.10. Ризик од прања ноца и финансирања тероризма

5. Међународни нормативни оквир заштите информација у банкама и финансијским институцијама

5.1. Базелски споразуми

5.2. Резилијентност информационих система у банкама и финансијским институцијама

5.3. Међународне институције од значаја за развој резилијентности банака и финансијских институција

5.4. Водич за сајбер резилијентност финансијске тржишне инфраструктуре

5.5. Документ Европске централне банке о надгледању сајбер резилијентности инфраструктуре финансијског тржишта

5.6. Упутство за опис послова вишег извршног директора задуженог за сајбер резилијентност

6. Преглед додатне међународне нормативе која се односи на сајбер безбедност финансијских институција

7. Међународни стандарди у остваривању заштите информација

8. Закључна раматрања поглавља

IV МОГУЋНОСТИ УНАПРЕЂЕЊА ОРГАНИЗАЦИОНОГ УРЕЂЕЊА ЗАШТИТЕ ИНФОРМАЦИЈА У ФУНКЦИЈИ БЕЗБЕДНОСТИ БАНАКА И ФИНАНСИЈСКИХ ИНСТИТУЦИЈА

1. Појам информационе безбедносне културе

2. Новија одређења информационе безбедносне културе и организационе културе – претпоставке унапређења заштите информација у банкама и финансијским институцијама

3. Организација као научна област и њен допринос унапређењу заштите информација у банкама и финансијским институцијама

3.1. Области истраживања организације као научне области

3.2. Организационо понашање у контексту могућности унапређења понашања запослених према заштити информација

3.3 Модел организационог понашања у контексту могућности унапређења понашања запослених према заштити информација

4. Појам и значај организационе културе као претпоставке развоја културе заштите информација

4.1. Садржај организационе културе у контексту унапређења заштите информација

4.2. Класификација организационих култура и механизми унапређења заштите информација

4.3. Безбедносна култура као супкултура организације

4.4. Могућности унапређења културе заштите информација кроз спровођење стратегије промене организационе културе

5. Унапређење културе заштите информација кроз организационо учење

5.1. Процес организационог учења и неке рефлексије на заштиту информација

6. Унапређење културе заштите информација кроз спровођење организационих промена

6.1. Развој свести о безбедности у светлу узрока организационих промена

6.2. Садржај унапређења културе заштите информација у контексту организационих промена

6.3. Организационо унапређење заштите информација кроз разумевање процеса организационих промена и отпори промена у организацији

7. Закључна разматрања поглавља

V ЗАКЉУЧНА РАЗМАТРАЊА

VI ЛИТЕРАТУРА

VII ПРИЛОЗИ

Сажетак рада по поглављима:

У првом поглављу дисертације дефинисан је методолошки оквир истраживања кроз приказ приступа проблему, одређењу предмета истраживања, објашњењу теоријског и концептуалног оквира истраживања, операционалном одређењу предмета истраживања, временском, просторном и дисциплинарном одређењу, као и кроз одређење циља истраживања, хипотетичког оквира и начина истраживања. У истраживању се пошло од научне поставке да се приликом конципирања система безбедности полази од свих извора угрожавања, а не само од појединих облика угрожавања, одакле се последично јављају облици супротстављања у које спадају и организационе и нормативне мере у остваривању заштите информација у банкама и финансијским институцијама. У том смислу информационе технологије, поред свог неупитног значаја које имају за обављање пословних процеса, карактерише да их треба посматрати као средство у постизању заштите информација, а не као извориште и циљ заштите, од којег не видимо друге аспекте безбедносног организовања у остваривању заштите информација.

У другом поглављу дисертације кандидат је приступио анализи објављених научних радова чији је предмет истрживања заштита информација у банкама и финансијским институцијама, првенствено полазећи од организационог и нормативног аспекта уређења и обављања ових послова. Кандидат је за ове потребе користио алате као што су претраживачи КоБСОН и *Sciencedirect*, односно други слободни интернет претраживачи, што је наведено у одговарајућим напоменама. На основу научне анализе изведен је закључак да се информациона безбедност не може посматрати искључиво са техничког аспекта, већ да се том приликом морају уважити и други, нетехнички аспекти, који обухватају и организационо и нормативно уређење заштите информација.

У трећем поглављу дисертације кандидат је разматрао значај заштите информација за пословање банака и финансијских институција, којом приликом је дато објашњење основних појмова који се односе на заштиту информација. Такође, приказане су основне фукције које треба да испуњава систем заштите информација, које не морају да се нужно налазе у пословној функцији безбедности, што је даље кандидату послужило за анализу неколико карактеристичних модела организовања послова заштите информација који се данас могу најчешће пронаћи у практичном остваривању ових послова. Истичући особине појединих решења, кандидат је закључио да безбедносну пословну фукцију, посебно када су у питању банке и финансијске институције, треба организовати на такав начин да она обухвата целу организациону структуру и да њене базичне безбедносне функције не треба да буду распршене по различитим пословним функцијама, а посебно да се управљање заштитом информација не треба организовати у оним пословним функцијама где је могућ сукоб интереса, као што је пословна фунција IT-а.

У четвртом поглављу под називом „Нормативно уређење заштите информација у банкама и финансијским институцијама" кандидат анализира нормативни оквир који се састоји од релевантних прописа државних органа, специфичних закона и подзаконских аката које доноси надлежни регулатор, Народна банка Србије, међународних стандарда, смерница, упутстава и препорука најбоље праксе из области заштите информација који се односе на пословање банака и финансијских институција. Домаће законодавство кандидат анлизира посматрајући акта које се директно односе на обавезе банака и финансијских истиуција према заштити информација, којом приликом се по свом значају истичу Закон о банкама, Одлука о минималним стандардима управљања информационим системом

финансијске институције и Одлука о управљању ризицима банке, као и друге релевантне прописе. Међународни нормативни оквир кандидат анализира кроз приказ базелских споразума, где посебну пажњу посвећује анализи споразума Базел II, будући да он третира оперативни ризик као формализовану групу ризика која се односи на област заштите информација у банкама и финансијским институцијама и истиче значај подизања свести запослених о заштити информација и културу њиховог понашања у односу на изложеност оперативним ризицима. Кандидат посебан допринос изучавању заштите информација у банкама и финансијским институцијама даје кроз анализу савременог концепта који се испољава кроз резилијентност информационих система у банкама и финансијским институцијама, будући да он подразумева предвиђање и прилагођавање променама у окружењу, задржавање и брзи опоравак од сајбер инцидената. Такође, сајбер резилијентност у банкама и финансијским институцијама обухвата заштиту људи и процеса, као и мере нетехничке природе које су засноване на знањима менаџерских наука о управљању, планирању, организационој култури и едукацији запослених. Саставни део сајбер резилијентности су традиционалне области безбедности, као што су физичко-техничка заштита, безбедносне истраге и друго. Кандидат је у оквиру обог поглавља приказао и међународне стандарде који се односе на заштиту информација, а посебно је анализирао стандард ISO/IEC 27002.

Пето поглавље дисертације, под називом „Могућности унапређења организационог уређења заштите информација у функцији безбедности банака и финансијских институција" заснива се на претходно утврђеним научним чињеницама да је информациона безбедносна култура неодвојиви садржај заштите информација у банкама и финансијским институцијама, као и да се подизање свести о заштити информација може остварити преко промена у сфери организационе кулуре. С тим у вези, кандидат је приказао модел из којег следи да култура заштите информација зависи од бројних фактора, као што су национална култура, организациона култура, прихватање промена у оргазацији, развијеност културе ризика у организацији, понашање запослених, њихова едукација и личне вредности које укључују и знања о заштити информација. У оквиру овог поглавља, кандидат је приредио осврт на основне теоријске поставке организације као научне области, којом приликом је овај садржај приказао у контексту њеног доприноса заштити информација.

Закључна разматрања докторске дисертације представљају сажетак добијених резултата истраживања. Кандидат Милетић је констатује да је научна теорија утврдила да се у приступу и остваривању заштите информација недовољно посматрају нетехнички аспекти, који могу бити кључни за успешно остваривање овог концепта, будући да заштита информација у банкама и финансијским институцијама зависи у великој мери од организационог и нормативног уређења ове области. Постојећом међународном и домаћом правном регулативном стварају се јединствене основе за стандардизовање поступака у области заштите информација у банкама и финансијским институцијама, као и одговарајући правни механизми издати од стране регулатора, а банке и финансијске институције својим интерним актима конкретизују прописана начела и прилагађавају их конкретним условима, укључујући при томе мере техничке и нетехничке природе, које обухватају информатичке ресурсе, људе и процесе. Организациона култура је од суштинског значаја за подизање свести запослених о значају заштите информација и преко ње се може утицати на културу информационе безбедности.

Кандидат Милетић на основу спроведеног истраживања и обављене научне анализе проучаваног проблема и предмета дисертације, закључује да су потврђене општа и посебне хипотезе од којих је пошао у истраживању. Он предвиђа раст безбедносних ризика у области информационе безбедности у банкама и финансијским институцијама, што ће довести до уже специјализације људских ресурса који се ангажују на пословима заштите информација у оквиру безбедносне пословне функције, као и до потребе мултидисциплинарног приступа у производњи потребних образовних профила за ове потребе. С тим у вези, кандидат сугерише да Факултет безбедности, Универзитет у Београду, полазећи од тренутних образовних програма и расположивих кадровских потенцијала, може да на основу утврђених потреба за образовањем стручних кадрова у области заштите информација креира одговарајући образовни садржај и да на тај начин допринесе усклађивању потреба за развојем стручњака безбедности са потребама које намеће савремено пословно окружење.

3. Остварени резултати и научни допринос дисертације

Докторска дисертација кандидата мр Перице Милетића под називом „Организационо и нормативно уређење заштите информација у функцији безбедности пословања банака и финансијских институција“ је за свој основни циљ имала да истражи и анализира феномен заштите информација у банкама и финансијским институцијама, са организационог и нормативног аспекта. Сходно дефинисаном предмету и циљевима истраживања, научно-теоријски допринос дисертације огледа се у следећем:

1. Спроведено истраживање употпуњује теоријска знања о методологији истраживања заштите информација у банкама и финансијским институцијама
2. Спроведено истраживање потенцира потребу превазилажења приступа у којем се заштита информација посматра као техничко питање и скреће пажњу на важност прихватања других, нетехничких аспеката, као што су организационо и нормативно уређење области заштите информација.
3. У функцији потпуног научног објашњења истраживане појаве у делу нормативне уређености заштите информација, извршена је анализа постојећег нормативног оквира заштите информација у банкама и финансијским институцијама, на националном и међународном плану, што представља значајан допринос проширењу и синтетизовању укупног научног фонда у овој области.
4. Спроведено истраживање употпуњује теоријска знања о модалитетима и специфичностима организовања послова заштите информација у банкама и финансијским институцијама, којом приликом се ставља акценат на услове пословног амбијента и потреба конкретне оргаизације.
5. Спроведеним истраживањем потенцирају су предности савременог приступа у остваривању заштите информација у банкама и другим финансијским институцијама, кроз примену концепта сајбер резилијентности, који подразумева равноправну заштиту информатичких ресурса, људи и процеса и примену знања из техничких и нетехничких научних области.

6. Спроведено истражовање пружа допринос појмовном одређењу заштите информација у банкама и финансијским институцијама, што доприноси разјашњењу терминолошких и семантичких недоумица у овој области.
7. Спроведено истраживање је верификовало постављене хипотезе о организационом и нормативном уређењу заштите информација у банкама и финансијским институцијама.
8. Спроведено истраживање има и практичан значај за безбедност банака и других финансијских институција у области заштите информација јер пружа конкретне смернице и препоруке за организовање заштите информација у банкама и финансијским институцијама.
9. У докторској дисертацији дата је сугестија о потреби профилисања новог образовног програма који би производио стручњаке за заштиту информација, којом приликом би се применио мултидисциплинарни приступ.
10. Спроведено истраживање пружа сазнања на нивоу научне дескрипције, класификације и објашњења, услед чега представља основу за даља истраживања ове области код нас – посебно узимајући у обзир недостатак домаћих научних радова из области заштите информација у банкама и финансијским институцијама, и готово потпуног недостатка истраживања нетехничких аспеката остваривања заштите информација.

На основу изнетих констатација, Комисија констатује да докторска дисертација кандидата мр Перице Милетића представља значајан допринос научном сазнању у области наука безбедности.

4. Закључак и предлог Комисије

Комисија је мишљења да је докторска дисертација кандидата мр Перице Милетића, под насловом „Организационо и нормативно уређење заштите информација у функцији безбедности пословања банака и финансијских институција“, израђена у складу са одобреном структуром на коју је сагласност дало Наставно-научно веће Факултета безбедности Универзитета у Београду и Стручно веће Универзитета у Београду.

Комисија констатује да је кандидат успешно обрадио постављену тему. Предмет и циљеви истраживања су адекватно постављени, а теоријски и методолошки оквир рада су кохерентни и утемељени на релевантним научним достигнућима и савременој емпиријској пракси. Дисертација је резултат самосталног теоријског рада и спроведеног истраживања кандидата, а рад је написан стручним језиком и адекватним стилом, разумљивим за читаоце.

На основу изложеног, имајући у виду резултате спроведеног истраживања, као и његов научни и друштвени допринос, чланови Комисије једногласно позитивно оцењују текст дисертације и са задовољством предлажу Наставно-научном већу Факултета безбедности Универзитета у Београду да поступи у складу са утврђеном процедуром и одобри јавну одбрану дисертације мр Перице Милетића под насловом „Организационо и нормативно уређење заштите информација у функцији безбедности пословања банака и финансијских институција“.

У Београду, 23. јула 2020. године

КОМИСИЈА:

Др Бранкица Поповић, ванредни професор,
Криминалистичко-полицијски универзитет

Др Ненад Путник, ванредни професор Факултета
безбедности Универзитета у Београду

Др Миленко Целетовић, ванредни професор Факултета
безбедности Универзитета у Београду