УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ – 6**
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ИЗВЕШТАЈ О ОЦЕНИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

I ПОДАЦИ О КОМИСИЈИ

1. Датум и орган који је именовао комисију:

Решење Декана Факултета техничких наука у Новом Саду на основу одлуке Наставно научног већа Факултета, бр. 012-199/52-2021 од 26.05.2022. године.

2. Састав комисије у складу са *Правилима докторских студија Универзитета у Новом Саду*:

1.	Зарић Мирослав	Ванредни професор	Примењене рачунарске науке и информатика, 20.06.2018.
	презиме и име	звање	ужа научна област и датум избора
	Факултет техничких наука Нови Сад		Председник комисије
	установа у којој је запослен-а		функција у комисији
2.	Ердељан Александар	Редовни професор	Аутоматика и управљање системима, 14.07.2016.
	презиме и име	звање	ужа научна област и датум избора
	Факултет техничких наука Нови Сад		Члан
	установа у којој је запослен-а		функција у комисији
3.	Вујовић Владимир	Ванредни професор	Рачунарске науке, 02.08.2021.
	презиме и име	звање	ужа научна област и датум избора
	Електротехнички факултет, Универзитет у Источном Сарајеву		Члан
	установа у којој је запослен-а		функција у комисији
4.	Вуковић Жељко	Доцент	Примењене рачунарске науке и информатика, 01.07.2020.
	презиме и име	звање	ужа научна област и датум избора
	Факултет техничких наука Нови Сад		Члан
	установа у којој је запослен-а		функција у комисији
5.	Сладић Горан	Редовни професор	Примењене рачунарске науке и информатика, 13.09.2021.
	презиме и име	звање	ужа научна област и датум избора
	Факултет техничких наука Нови Сад		Ментор
	установа у којој је запослен-а		функција у комисији

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: **Милан, Јован, Стојков**

2. Датум рођења, општина, држава: **07.08.1991, Зрењанин, Република Србија**

3. Назив факултета, назив претходно завршеног нивоа студија и стечени стручни/академски назив: **Факултет техничких наука Универзитета у Новом Саду, Рачунарство и аутоматика, Дипломирани инжењер електротехнике и рачунарства - мастер.**

4. Година уписа на докторске студије и назив студијског програма докторских студија: **2015, Рачунарство и аутоматика**

III НАСЛОВ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure

Српски: Модел за праћење усклађености између безбедносних стандарда и приоритизацију захтева у критичним инфраструктурама

IV ПРЕГЛЕД ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Навести кратак садржај са назнаком броја страница, поглавља, слика, схема, графикона и сл.

Докторска дисертација написана је на 222 стране Б5 формата на енглеском језику. Главни део дисертације садржи 5 поглавља уз додатне сегменте за апстракт, резиме рада написан на српском језику, библиографију, биографију и план третмана података. Дисертација садржи 12 слика, 18 табела и 212 навода литературе. Кључна документацијска информација написана је на српском и енглеском језику.

Докторска дисертација се састоји од следећих поглавља:

1. Увод
2. Преглед тренутног стања у области
3. Модел за репрезентацију захтева
4. Валидација модела
5. Закључак

V ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Докторска дисертација је организована у пет поглавља.

У првом поглављу дат је опис мотивације истраживања са јасно дефинисаним истраживачким питањима и хипотезама. Описан је појам критичних инфраструктура и представљене су методе за њихову заштиту.

Друго поглавље садржи преглед релевантне литературе из области дисертације. Представљени су најзначајнији модели за презентацију безбедносних захтева. Описана је анализа софтверских алата који за циљ имају процене отпорности система на нападе и усклађености са стандардима. У наставку поглавља су представљени најзначајнији модели којима се може на квалитативни начин описати зрелост организација и система са аспекта безбедности. У поглављу су презентовани и често коришћени начини за анализу ризика као једне од главних активности које треба спроводити у циљу побољшања безбедности. Представљени су кораци два стандардизована приступа за спровођење анализе ризика: NIST SP 800-30 и ISO/IEC 27005:2011. На крају поглавља описане су постојеће методе за доношење одлука на основу скупа критеријума и њихова примена при одабиру безбедносних захтева.

У трећем поглављу дат је опис методологије за креирање модела и компоненти за његово проширење. Методологија за креирање и валидацију модела састоји се из три корака. У склопу првог корака, представљени су резултати и ограничења анализе доступне литературе која ставља акценат на безбедносне стандарде, стручне смернице и регулативе који су примењиви на критичне инфраструктуре. Анализа је спроведена у циљу избора адекватних публикација чија структура ће се даље анализирати. Финални скуп публикација које су коришћене за даљу анализу чине: IEC 62443-3-3:2013, ISO/IEC 27001/27002, NIST SP 800-53 и NERC CIP. У склопу другог корака дефинисана су четири критеријума за приоритизацију одабира захтева за имплементацију:

резултат анализе ризика, зависности између учесника задужених за имплементацију захтева, ниво важности захтева за усклађеност и припадност захтева одговарајућем домену. Анализиране су изабране публикације и њихови захтеви и дефинисан је скуп од 24 домена у који се могу сврстати захтеви, а који прави прецизнију класификацију захтева у односу на постојећа решења. Припадност захтева једном од 24 домена уједно представља један од критеријума за приоритизацију. У наставку поглавља дефинисани су нивои важности за усклађеност са стандардима. Понуђени модел за нивое важности је дводимензионалан. Прва димензија тиче се важности захтева за постизање одређеног нивоа безбедности, док се друга бави зрелошћу саме имплементације. Трећи критеријум приоритизације представљају информације које уносе зависности између различитих улога учесника из организационе структуре задужених за имплементацију захтева. Зависности које они могу да направе међусобно могу бити прилично комплексне. Концепти дефинисани у i* (иЗвезда) радном оквиру прилагођени су потребама ове дисертације тако да се дефинише граф зависности учесника. На овај начин прате се све зависности између учесника у процесу имплементације захтева и детектују комплексни графови који могу утицати на подизање приоритета имплементације. Као последњи критеријум представљен је резултат анализе ризика. Анализа ризика издвојена је као најважнија активност за одређивање приоритета имплементације захтева. Такође је описан критеријум за избор методе за рачунање приоритета захтева и демонстриран је поступак одређивања редоследа имплементације. На крају поглавља је представљен модел са свим релевантним елементима и њиховим зависностима.

У склопу последњег корака, у четвртом поглављу представљен је радни оквир као механизам за потврду употребљивости предложеног модела. Детаљно су описане његове активности и безбедносни концепти на којима почива. Радни оквир служи као смерница за процену нивоа безбедности организације или система који се посматра, као и анализу, приоритизацију и имплементацију безбедносних захтева. Представља систематски приступ за повезивање релевантних елемената дефинисаног модела: имовине, безбедносних циљева, кључних критеријума учинка, претњи, рањивости, учесника у процесу имплементације захтева и анализе ризика. Радни оквир се састоји из низа активности које су груписане у три фазе: фаза скупљања података, фаза вршења процене усклађености и фаза праћења имплементације захтева за које је утврђена неусклађеност. Прва фаза прописује унос у базу знања информација од значаја које укључују попис ресурса, могућих претњи, рањивости и безбедносних захтева са којима се остварује усклађеност. Друга фаза прописује вршење иницијалне процене усклађености са одабраним захтевима у циљу одређивања нивоа зрелости безбедности и препознавања скупа захтева које треба додатно обрадити. У последњој фази дефинишу се циљеви које треба задовољити, а који могу бити условљени циљевима пословања, потребама и очекивањима корисника. Прописује се дефинисање скупа захтева које треба имплементирати, те се за њих додатно дефинишу начини за праћење имплементације, листе учесника и спровођење анализе ризика. У истом поглављу приказана је употребљивост предложеног радног оквира на примеру произвођача индустријског контролног система за паметне мреже. Анализиран је стандард који није био део иницијалне анализе при дефинисању модела, а са чијим захтевима се тестира усклађеност. Добијени резултати показали су да се елементи захтева могу мапирати на елементе дефинисаног модела. Такође, демонстрирано је одређивање приоритета имплементације захтева са којима не постоји адекватна усклађеност у складу са методама и критеријумима представљеним кроз треће поглавље. У последњој секцији наведене су предности и недостаци модела и радног оквира који га користи.

Пето поглавље представља последње поглавље дисертације. У овом поглављу сумирани су доприноси ове дисертације и дато је образложење потврђености полазних хипотеза. На самом крају поглавља дат је преглед даљих праваца истраживања.

VI СПИСАК НАУЧНИХ И СТРУЧНИХ РАДОВА КОЈИ СУ ОБЈАВЉЕНИ ИЛИ ПРИХВАЋЕНИ ЗА ОБЈАВЉИВАЊЕ НА ОСНОВУ РЕЗУЛТАТА ИСТРАЖИВАЊА У ОКВИРУ РАДА НА ДОКТОРСКОЈ ДИСЕРТАЦИЈИ:

Таксативно навести називе радова, где и када су објављени. Прво навести најмање један рад објављен или прихваћен за објављивање у складу са *Правилима докторских студија Универзитета у Новом Саду* који је повезан са садржајем докторске дисертације. У случају радова прихваћених за објављивање, таксативно навести називе радова, где и када ће бити објављени и приложити потврду уредника часописа о томе.

Рад у истакнутом међународном часопису (М22)

Stojkov M, Dalčeković N, Markoski B, Milosavljević B, Sladić G. Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid. Energies. 2021; 14(21) 6862. ISSN: 1996-1073 DOI: https://doi.org/10.3390/en14216862

Саопштење са међународног скупа штампано у целини (М33)

Stojkov M., Simić M., Sladić G., Milosavljević B.: Traditional and Blockchain-based access control models in IoT: A review, 10. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for Information Systems and Computer Networks, 8-11 March, 2020, pp. 51-55, ISBN 978-86-85525-24-7

Stojkov M., Sladić G., Milosavljević B., Zarić M., Simić M.: Privacy concerns in IoT smart healthcare system, 9. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for information systems and computer networks, 10-13 March, 2019, pp. 62-65, ISBN 978-86-85525-24-7

Stojkov M., Simić M., Sladić G., Milosavljević B.: Two-step process for secure registration of nodes in IoT systems, 8. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for information systems and computer networks, 11-14 March, 2018, pp. 28-31, ISBN 978-86-85525-22-3

Stojkov M., Milosavljević B., Sladić G.: On the Usability of Access Control Models in IoT , 8. PSU-UNS International Conference on Engineering and Technology - ICET, Novi Sad: University of Novi Sad, Faculty of Technical Sciences, 8-10 June, 2017, pp. 1-4, ISBN 978-86-7892-934-2

Luburić N., **Stojkov M.**, Savić G., Sladić G., Milosavljević B.: Crypto-tutor: An educational tool for learning modern cryptography, 14. IEEE International Symposium on Intelligent Systems and Informatics (SISY), Subotica, 29-31 August, 2016, pp. 205-210, ISSN 1949-0488, DOI: 10.1109/SISY.2016.7601498

VII ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА:

Овим истраживањем представља се једно могуће решење за дефинисање модела који има релевантне елементе за адекватно представљање безбедносних захтева из различитих типова публикација, као и њихово међусобно поређење у циљу планирања и праћења имплементације. Дефинисани су критеријуми за приоритизацију одабира захтева за имплементацију који директно зависе од четири фактора: резултата анализе ризика, зависности између учесника задужених за имплементацију захтева, нивоа важности захтева за усклађеност и припадности захтева одговарајућем домену. Применом оваквог модела могуће је довести информације из различитих публикација у стандардизовани облик који ће даље олакшати рад и софтверску аутоматизацију. Радни оквир базиран је на претходном моделу и садржи низ корака који воде кориснике кроз процес анализе, планирања и праћења задовољења безбедносних захтева. Такође, може послужити као основа за алат који би аутоматизовао активности које се односе на попуњавање базе новим захтевима, класификацију захтева у одговарајуће домене, анализу захтева и квантификацију резултата спроведених ревизија.

Модел и радни оквир могу користити организације на чији су софтвер или услуге примењиви различити безбедносни стандарди, услед коришћења од стране различитих клијената, у различитим доменима или у различитим географским регионима. На овај начин, организације могу демонстрирати своју усклађеност са више безбедносних стандарда, стручних смерница или регулатива чији су захтеви дефинисани на различитим нивоима детаља. Модел и радни оквир могу користити и сви остали који желе да разумеју шта су и како изгледају стандардизовани безбедносни захтеви. Такође, пружена је могућност планирања приоритизације имплементације безбедносних захтева одабраних стандарда која укључује и спровођење анализе ризика, те предложено решење могу користити и сви остали пружаоци услуга који желе да повећају зрелост безбедности своје организације или система. Део модела за опис безбедносних захтева може бити уобличен и коришћен као формат за размену безбедносних захтева између апликација којима је примарна намена рад са безбедносним захтевима у циљу креирања безбедносних планова за организације или системе.

VIII ОЦЕНА НАЧИНА ПРИКАЗА И ТУМАЧЕЊА РЕЗУЛТАТА ИСТРАЖИВАЊА:

Експлицитно навести позитивну или негативну оцену начина приказа и тумачења резултата истраживања.

Тумачење добијених резултата је јасно и прегледно. Формирани закључци у раду су поткрепљени одговарајућим теоријским анализама и резултатима истраживања. Резултати су приказани исцрпно и прегледно уз навођење претходних истраживачких резултата у овој области. Дисертација је

проверена у софтверу за детекцију плагијаризма iThenticate.
Оцена начина приказа и тумачења резултата истраживања је позитивна.

IX КОНАЧНА ОЦЕНА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Експлицитно навести да ли дисертација јесте или није написана у складу са наведеним образложењем, као и да ли она садржи или не садржи све битне елементе. Дати јасне, прецизне и концизне одговоре на 3. и 4. питање:

1. Да ли је дисертација написана у складу са образложењем наведеним у пријави теме?
Докторска дисертација је написана у складу са образложењем наведеним у пријави теме.

2. Да ли дисертација садржи све битне елементе?
Дисертација садржи све битне елементе.

3. По чему је дисертација оригиналан допринос науци?
Оригинални доприноси дисертације могу се разложити у три сегмента. Први сегмент представља дефинисање модела за репрезентацију безбедносних захтева који се може користити за праћење имплементације и процене усклађености са више стандарда, стручних смерница и регулатива у исто време на униформан начин. Други сегмент представља дефинисање критеријума приоритизације за потребе имплементације безбедносних захтева са којима организација или систем нису усаглашени. Критеријум приоритизације је базиран на четири фактора: резултатима анализе ризика, зависностима између учесника задужених за имплементацију захтева, нивоима важности захтева за усклађеност и припадности захтева одговарајућем домену. Последњи сегмент представља дефинисање радног оквира и смерница за његово коришћење за потребе демонстрације примене модела.

4. Који су недостаци дисертације и какав је њихов утицај на резултат истраживања?
Дисертација нема недостатке који утичу на резултате истраживања.

X ПРЕДЛОГ:

На основу наведеног, комисија предлаже:

Да се докторска дисертација Милана Стојкова, под називом „Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure“ (срп. „Модел за праћење усклађености између безбедносних стандарда и приоритизацију захтева у критичним инфраструктурама“) прихвати, а кандидату одобри одбрана.

Место и датум: Нови Сад, 01.06.2022:

1. др Мирослав Зарић, ванредни професор
_____, председник

2. др Александар Ердељан, редовни професор
_____ члан

3. др Владимир Вујовић, ванредни професор
_____, члан

4. др Жељко Вуковић, доцент
_____, члан

5. др Горан Сладић, редовни професор
_____, ментор

НАПОМЕНА: Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај и да исти потпише.