UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj 4 – 241/2019 od 20.12.2019. godine i broj 4-64/2020. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Dragana Savića, mastera, pod nazivom „Kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja“, o čemu podnosimo sledeći

I Z V E Š T A J

1. Osnovni podaci o kandidatu i doktorskoj disertaciji

Kandidat Dragan Savić rođen je 22.09.1974. godine u Petrovcu na Mlavi, Republika Srbija. U Petrovcu na Mlavi završio je osnovnu školu, a potom i Gimnaziju „Mladost“. Visoko obrazovanje stekao je na Vojnoj akademiji, odsek Ratna Mornarica u Beogradu 1997. godine i stekao zvanje oficir pomorstva. Specijalističke akademske studije 2. stepena završio je na Kriminalističko-policijskoj akademiji u Beogradu 2010. godine i stekao zvanje diplomirani kriminalista-specijalista. Master studijski program „Savremene informacione tehnologije“ završio je na Univerzitetu „Singidunum“ 2014. godine i stekao zvanje master – informatičar. Doktorske akademske studije na studijskom programu „Napredni sistemi zaštite“, Univerziteta „Singidunum“, upisao je školske 2014/2015. godine. Sve ispite predviđene planom i programom doktorskih studija je položio s prosečnom ocenom 10 (deset) do 29.09.2016. godine. Zahtev za odobravanje teme za izradu doktorske disertacije podneo je 17.02.2017. godine.

Svoju profesionalnu karijeru započeo je u septembru 1997. godine u sastavima Vojske Srbije i Ministarstva odbrane Republike Srbije. Od 2006. godine predavač na raznim stepenima usavršavanja u sistemu obrazovanja u Vojsci Srbije, i povremeni predavač na Vojnoj akademiji Univerziteta Odbrane u Beogradu na predmetu Strategija – obaveštajne i bezbednosne službe i obaveštajno obezbedjenje.

Njegova trenutna istraživačka interesovanja orijentisana su na bezbednost podataka, informacione i komunikacione tehnologije, računarske mreže i kriptografiju.

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4 – 241/2019 od 20.12.2019. godine, nakon izmene drugog člana, formirana je Komisija u sastavu:

1. Prof. dr Mladen Veinović, redovni profesor Univerziteta Singidunum, mentor,
2. Prof. dr Milan Milosavljević, redovni profesor Univerziteta Singidunum,
3. Prof. dr Goran Šimić, vanredni profesor Vojne akademije u Beogradu.

za ocenu doktorske disertacije pod nazivom: „Kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja“. Za člana komisije imenovan je redovni prof. Univerziteta Singidunum dr Milan Milosavljević, umesto prof. dr Jelene Đorđević-Boljanović. Za mentora je imenovan redovni prof. redovni profesor Univerziteta Singidunum dr Mladen Veinović.

Odlukom Veća Departmana za poslediplomske studije i međunarodnu saradnju Univerziteta Singidunum, broj: 4 – 64/2020 od 22.05.2020. godine, nakon izmene trećeg člana, formirana je Komisija u sastavu:

1. Prof. dr Mladen Veinović, redovni profesor Univerziteta Singidunum, mentor,
2. Prof. dr Milan Milosavljević, redovni profesor Univerziteta Singidunum,
3. Prof. dr Petar Spalević, redovni profesor FTN-a Univerziteta u Prištini sa privremenim sedištem u Kosovskoj Mitrovici.

za ocenu doktorske disertacije pod nazivom: „Kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja". Za člana komisije imenovan je prof. dr Petar Spalević, umesto prof. dr Gorana Šimića. Završnu verzija doktorske disertacije u elektronskom i štampanom obliku Dragan Savić predao Univerzitetu 20.02.2020. godine.

Kandidat je koautor na jednom radu iz **kategorije M22** koji je prihvaćen za objavljivanje. Potvrda urednika časopisa je u prilogu ovog Izveštaja:

1. Maksimovic Vladimir, Petrovic Mile, Savic Dragan, Jaksic Branimir, Spalevic Petar (2020), New Approach for Estimating Edge Detection Threshold and Application of Adaptive Detector Depending on Image Complexity, Ref. No.: IJLEO-D-21-00088, Optik, Elsevir (https://www.journals.elsevier.com/optik).

čime je ispunjen preduslov za odbranu doktorske disertacije.

Spisak rezultata M33

1. Savić Dragan, Damjanović Slobodan; The Attacks on the RSA Algorithm; Sinteza 2016, DOI: https://doi.org/10.15308/Sinteza-2016, pp. 131-136, 2016.
2. Savić Dragan, Mladen Veinović; Challenges of General Data Protection Regulation (GDPR); DOI: https://doi.org/10.15308/Sinteza-2018, pp. 23 – 30; 2018.

Spisak rezultata M14

1. Mijalković Saša, Savić Dragan: „New Border Security Concept of the Republic of Serbia – Meeting European Standards of National and International Security", Serbian Law in Transition – Changes and Challenges, Institute for Comparative Law, Belgrade, 2009, pp. 295–314, ISBN 978-86-80059-66-2; (ed. Monika Milošević),

Objavljene knjige:

1. Savić Dragan., Vladisavljević Dragan., Životić Aleksandar., Božić Nikola., Stanković Predrag., Novaković Slobodan., Đokić S., Vukadinović-Šundrić Snežana., :"Vojnoobaveštajna služba u Srbiji" , Medija centar "Odbrana", Beograd, 2012 (ISBN 978-86-335-0367-9) – monografija od nacionalnog značaja.
2. Savić D, "Obaveštajne službe, terorizam i borba protiv terorizma" , Borotehna, Beograd, 2015 (COBISS.SR-ID 213136140) - monografija

Radovi poslati na recenziju:

1. Savic D., Veinovic M., A survey of cryptanalytic attacks on RSA algorithm and its variants, Romanian Journal of Information Science and Technology – rad je u toku procesa recenzije.
2. Djordjevic B., Timcenko Valentina, Sarac M., Adamovic S., Gnjatovic M., Savic D., Macek N., Comprehensive survey of cancelable biometrics and biometric cryptosystems, Acta Polytechnica Hungarica – rad je u toku procesa recenzije.
3. Savic D., Veinovic M., Milosavljevic M., Can computers learn cryptanalysis, International Journal of Computer Systems Science and Engineering - rad ima jednu recenziju i čeka na drugu.
4. Savić D., Damjanović S., Veinović M., "Napadi na RSA Algoritam", Vojnotehnički glasnik.

Doktorska disertacija kandidata Dragana Savića je urađena na ukupno 230 strana, od čega 38 strana čine prilozi i spisak literature. Spisak literature obuhvata 654 referenci koje čine naučni radovi, knjige, zbornici radova, zakonski propisi, kao i elektronski izvori. Uz osnovni tekst disertacija sadrži i 69 slika i 29 tabela.

Doktorska disertacija kandidata Dragana Savića bila je podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). Ukupan procentualni iznos zapaženih preklapanja iznosi 12% disertacije. Uvidom u izveštaj Komisija konstatuje da su svi detektovani izvori sa poklapanjem ispod 1%, da se odnose na veliki broj citirane literature, kao i na standardne termine i definicije koji se koriste u oblasti iz koje je i sama disertacija.

2. Predmet i cilj istraživanja

Predmet istraživanja ove doktorske disertacije su kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja. Ovakav integrisani automatizovani proces posebno je koristan u objašnjavanju složenih poslovnih situacija koje se mogu javiti u praksi svake moderne kompanije. On omogućava efikasno upravljanje razmenom informacija između korisnika sistema, poštujući definisane radne procedure, odnosno definisane tokove informacija u poslovnom sistemu, što donosi i omogućava efikasno praćenje događaja u sistemu. Zaštita i bezbednost memorije organizacije kroz kriptografska rešenja trebaju da zadovolje balans između zahteva korisnika, projektovanja memorije organizacije, potrebe zaštite osetljivih podataka i njihov integritet. Funkcije koje bi trebalo da omogući obuhvataju: rukovanje fizičkim skladištenjem dokumenata; organizaciju dokumenata u logičke strukture; rukovanje životnim ciklusom dokumenata; akcije za rad sa dokumentima; digitalizaciju papirne dokumentacije; pretraživanje dokumenata; digitalno potpisivanje dokumenata; kontrolu pristupa dokumentima; arhiviranje dokumenata; podršku za kolaboraciju više učesnika; podršku za definisanje poslovnih procesa (*workflow*); automatske procedure za vođenje poslovnih procesa; beleženje svih događaja u radu sa dokumentima; notifikaciju o događajima u sistemu. Jedan od predloženog načina zaštite integrisanog sistema za proces upravljanja memorijom organizacije biće mogućnost njihovog snimanja u šifrovanom obliku, čime će podaci postati dostupni isključivo kroz sam sistem. Pristup dokumentu bi imali samo korisnici sistema koji su za to eksplicitno ovlašćeni kroz sistem za upravljanje dozvolama pristupa. Neporecivost dokumenata i njihova nepromenljivost će se obezbediti digitalnim potpisivanjem,

što ova platforma obezbeđuje u skladu sa aktuelnim zakonskim propisima za elektronski dokument. Ovakav predlog kriptografske zaštite integrisanog automatizovanog procesa upravljanja memorijom organizacije predstavlja rešenje koje bi svoju upotrebu moglo da nađe kako u oblasti učenja inteligentnih sistema, tako i u postojećim sistemima savremenog poslovnog odlučivanja.

Osnovni cilj istraživanja koji je realizovan u doktorskoj disertaciji je da se na osnovu šire literature sagleda problem rešenja kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja, kao i da se istraži mogućnost formalizacije i integrisane automatizacije memorije organizacije sa stanovišta menadžmenta znanja.

Posebni ciljevi ovog istraživanja ogledaju se u ispitivanju mogućnosti formalizacije i integrisane automatizacije eksplicitnog i implicitnog znanja jedne organizacije – kompanije u delu prikupljanja podataka, obrade podataka iz operativne baze memorije organizacije (skladišta podataka) i kriptografske zaštite. Isto tako ispitivanje mogućnost uticaja formalizacije i digitalizacije memorije organizacije na brzinu i kvalitet dizajna i dobijanja informacija o poslovnim procesima i potrebama korisnika za informacijama. Pored toga, u ovoj doktorskoj disertaciji prikazane su upotrebne vrednosti automatizacije memorije organizacije, kroz obezbeđivanje njene zaštite i olakšavanja pristupa, deljenja podataka i informacija i njeno ponovno korišćenje kroz integrisani automatizovani proces upravljanja znanjem. Samim time, istražena je mogućnost primene kriptografske zaštite integrisanog automatizovanog procesa za upravljanje memorije organizacije u oblasti poslovnog odlučivanja, kroz elektronsko upravljanje podacima prilagođeno korisničkom nivou, ali u isto vreme istražene su i mogućnosti kriptografskih rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja, sa težištem na očuvanje poverljivosti, integriteta i dostupnosti resursa memorije organizacije u procesu poslovnog odlučivanja u modernim kompanijama. Na kraju disertacije dat je predlog kriptografskog rešenja u zaštiti integrisanog automatizovanog procesa upravljanja memorijom organizacije, koji bi nadomestio nedostatke prikazanih rešenja i uveo određene nove koncepte i smernice za dalji rad.

Razvoj predloženog modela kriptografskih rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja može doprineti većoj društvenoj prihvatljivosti i podstaći kompanije i korisnike da koriste sredstva i mogućnosti za zaštitu svojih podataka i informacija kako bi bili istovremeno zaštićeni i poslovno efikasni. Sa podizanjem opšte svesti o jednostavnosti upotrebe predloženog modela i ukazivanjem na širok spektar mogućnosti koji se nude krajnjim korisnicima – kompanijama i njihovim zaposlenima društveni cilj ovog istraživanja bi bio u potpunosti zadovoljen.

3. Hipotetički okvir istraživanja

Na osnovu ciljeva rada proizilazi sledeći hipotetički okvir koji se sastoji od generalne hipoteze i posebnih hipoteza.

U radu se postavlja sledeća generalna hipoteza koja obuhvata preliminarno i teoretsko određenje predmeta istraživanja.

- Kriptografska zaštita integrisanog automatizovanog procesa upravljanja memorijom organizacije osnovni je preduslov za efikasno učenje, ali i brže i sadržajnije poslovno odlučivanje kompanije koja ga koristi.

Iz generalne hipoteze izvode se sledeće posebne hipoteze koje obrađuju delove predmeta istraživanja:

- Uspešnost kompanije i njenih poslovnih rezultata direktno zavisi od efikasnosti zaposlenih, međusobnim deljenjem znanja.
- Memorija organizacije je jedna od najvažnijih organizacijskih elemenata koju kompanija ima, tako da je potrebno projektovati načine da sadržaji memorije budu dostupni svima u kompaniji (prema nivoima odlučivanja) i da se ista adekvatno i efikasno zaštiti.
- Integrisano automatizovani proces upravljanja memorijom organizacije omogućava evidenciju podataka o dokumentima, elektronsko upravljanje dokumentacijom iz poslovnog sistema, upravljanje definisanim procedurama za rad sa poslovnim dokumentima ili predmetima (skupovima dokumenata).
- Korišćenjem integrisanog automatizovanog procesa upravljanja memorijom organizacije realizuje se politika sigurnosti, sistem upravljanja kvalitetom, sigurnost zaposlenih, i upravljanje kontinuitetom poslovanja čime se doprinosi povećanju kvaliteta i efikasnosti poslovnog odlučivanja.
- Zaštitom integrisanog automatizovanog procesa upravljanja memorijom organizacije mora se obezbediti visok nivo sigurnosti i zaštite svih dokumenta putem definisanja pristupa na nivou pojedinačnih pristupa korisnika paralelno sa upravljanjem dokumentima u memoriji.

4. Metodologija istraživanja

Metodologija istraživanja u okviru ove doktorske disertacije sadrži složen pristup koji se sastoji od logičkih načela i principa po definisanim fazama. Polazna metoda bila je prikupljanje i izučavanje dostupnih izvora literature, njihova analiza i sistematizacija, u cilju ukazivanja na opravdanost i korisnost razvoja kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja.

Za izradu doktorske disertacije osim opštih naučnih metoda, korišćene su i metode modelovanja i analitičko-deduktivna tehnika. Metoda modelovanja je upotrebljena prilikom definisanja modela memorije organizacije, implementacije kriptografskih rešenja i praktične provere rezultata istraživanja. Analizom postojećih rešenja menadžmenta znanja, kriptografske zaštite i skladištenja podataka korišćena je analitičko-deduktivna tehnika, odnosno metoda. Osim navedenih metoda, prilikom definisanja modela memorije organizacije, korišćeni su i posebni metodološki postupci kao što su generalizacija (definicija generičkog tipa) i specijalizacija kao inverzni postupak (definisanje specifičnih osobina nekih objekata).

Istraživanje je sprovedeno kroz nekoliko faza. U okviru prve faze je prikupljena i proučena dostupna literaturra u oblasti projektovanja memorije organizacije, menadžmenta znanja i kriptografskih rešenja, njena analiza i sistematizacija, sa akcentom na automatizaciji projektovanja memorije organizacije sa stanovišta menadžmenta znanja i implementaciji kriptografske zaštite. Identifikovani su i kategorizovani postojeći pristupi. Naredna faza istraživanja bila je proučavanje memorije organizacije (na principu Data Warehouse), analiza njenih prednosti i nedostataka. Glavni deo istraživanja odnosio se na formalizaciju upravljanja memorijom organizacije u svrhu principijelnog upravljanja fizičkim skladištenjem

dokumenata; njihovom organizacijom u logičke strukture; upravljanju životnim ciklusom; akcijama za rad sa dokumentima; digitalizacijom; pretraživanjem; digitalnom potpisivanju dokumenata; kontroli pristupa; arhiviranju dokumenata; podršci za kolaboraciju više učesnika; podršci za definisanje poslovnih procesa *(workflow)*; automatskim procedurama za vođenje poslovnih procesa; beleženju svih događaja u radu sa dokumentima, kao i notifikaciji o događajima u sistemu. Poseban akcenat dat je i na zaštiti integrisanog sistema za upravljanje memorijom organizacije kroz ispitivanje mogućnosti snimanja dokumenata u šifrovanom obliku, čime su podaci postali dostupni isključivo kroz sistem, dok je pristup dokumentima garantovan samo korisnicima sistema koji su za to eksplicitno ovlašćeni preko definisanih dozvola pristupa.

U poslednjoj fazi istraživanja implementirana je kriptografska zaštita u memoriji organizacije zasnovane na menadžmentu znanja i demonstrirana je upotrebna vrednost rezultata istraživanja na praktičnom primeru modela jedne organizacije.

Ovakav izbor metoda istraživanja je korišćen u svrhu korektnog izvođenja istraživanja i toka istraživačkog procesa u svim fazama, odnosno identifikaciji i formulaciji problema, planiranju dizajna istraživanja, prikupljanju, obradi i analizi podataka, kao i definisanju zaključaka u skladu sa osnovnim načelima naučnoistraživačkog rada. Svi metodološki postupci su podjednako zastupljeni, čime se ostvaruje integrativan i sintetički pristup istraživanju.

5. Kratak prikaz sadržaja doktorske disertacije

Doktorska disertacija se sastoji iz 10 (deset) poglavlja: Uvod, Metodološke osnove istraživanja, Teorija znanja, Menadžment znanja, Konceptualna tehnološka infrastruktura, Rudarenje podataka/Data Mining, Memorija organizacije, Optimizacija zaštite memorije organizacije, Kriptografija, Studija slučaja: Kriptografska rešenja zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije, Zaključak, Literatura.

U prvom poglavlju, daje se kratak prikaz sveobuhvatnog poduhvata i svih izazova istraživanja, kroz uvod u područje i probelem koji se istražuje. Definiše se predmet i cilj istraživanja, daje se pregled dosadašnjih rezultata u oblasti istraživanja, zatim polazne hipoteze, osvrt na metode istraživanja kao, i očekivani naučni i stručni doprinos rezultata istraživanja

Drugo poglavlje posvećeno je teoriji znanja i razmatrano je opšte stanje u oblasti istraživanja. Opisane se razlike značenja podatka, informacije i znanja kao i kategorizacija znanja uz konsultovanje različitih izvora i teorija. U nastavku poglavlja opisane su strategije upravljanja zanjem kroz opis generičke i opšte strategije uz objašnjenje elementa strategije upravljanja znanjem i savete kako i na koji način izgraditi strategiju menadžmenta znanja. Poglavlje se završava elaboriranjem ekonomije znanja kroz prednosti primene i pepreke i poteškoća u menadžmentu znanja.

U trećem poglavlju opisane su teorijske osnove istraživanja menadžmenta znanja kao jedne od tri celine istraživanja u ovoj doktorskoj tezi. Analizirane su definicije menadžmenta znanja i objašnjena suština samog koncepta menadžmenta znanja. Poseban osvrt u ovom delu disertacije posvećen je intelektualnom kapitalu, menadžmentu znanja i znanju kao nevidljivoj imovini svake kompanije. Uvidom u veći broj naučnih radova koji obrađuje ovu problematiku, analizirani su elementi i modeli menadžmenta znanja kao i implementacija menadžmenta znanja u praksi. U završnom delu ovog poglavlja objašnjene su tehnologije i alati menadžmenta znanja i predstavljene perspektive primene koncepta menadžmenta znanja u praksi u budućnosti.

U četvrtom poglavlju akcenat je dat na konceptualnu tehnološku infrastrukturu kompanije kao celinu koja je preduslov za razvijanje informacionih sistema i kreiranje znanja u kompanijama. Dat je kritički osvrt na proces reinženjeringa u kompanijama kroz analizu uvođenja savremenih organizacionih struktura, procesnog pristupa i razvoj informacionih sistema u kompanijama koji pre svega treba da služi automatizaciji i integraciji proizvodnih i poslovnih procesa sa jedne strane, kao i da predstavlja glavnu komunikacionu osnovu između pojedinih organizacionih celina u kompanijama. Poseban osvrt posvećen je sistemima za podršku u odlučivanju, ekspertnim sistemima, sistemima za menadžment dokumentima i informacionim sistemima za kreiranje znanja. Poglavlje se završava analizom koncepta organizacije koja uči, jer se u savremenoj globalnoj i digitalizovanoj ekonomiji, efektivno korišćenje znanja nametnulo kao najizdašniji i postojan izvor konkurentske prednosti svake kompanije. I na kraju, kritički se određujemo prema sistemu poslovne inteligencije jer u sebi obuhvata elemente strategije, upravljačkog računovodstva, poslovne analize, marketinga i informacione tehnologije kako bi se izvršilo prikupljanje, analiza, distribucija i delovanje na osnovu poslovnih informacija, radi lakšeg rešavanja upravljačkih problema i donošenja najboljih poslovnih odluka u kompanijama.

U petom poglavlju u smislu korišćenja znanja opisan je proces rudarenja podataka/Data Mining, jer kao takvo tretira važnost i ulogu otkrivanja znanja u poslovnoj inteligenciji svake kompanije. Dat je kratak pojam rudarenja podataka kroz zadatke – probleme rudarenja podataka. Predstavljen je odnos rudarenja podataka i otkrivanja znanja kroz kritički osvrt i analizu koraka u procesu otkrivanja znanja. Pored toga, analizirana je priprema podataka za rudarenje kroz procesuiranje, analiza relevantnih atributa i završni postupci. Poseban akcenat stavljen je na tehnike rudarenja podataka u kome su kritički razmatrane metoda regresije, klasifikacione metode, metode klasterovanja, neuronske mreže, stablo odlučivanja, metode za analizu veza i genetski algoritmi. Ovo poglavlje disertacije završava se kroz zaključno predstavljanje načina na koji se koristi znanje koje je otkriveno u procesu rudarenja podataka i predstavlaju se područja u kojima je moguća primena alata za rudarenje podataka.

Šesto poglavlje predstvlja drugu celinu disertacije i obrađuje memoriju organizacije kao fenomen i potrebu svake kompanije koja želi da uspostavi sisteme poslovne inteligencije i osvoji svoju konkurentnost na međunarodnom tržištu. Date su kritičke osnove definicije memorije organizacije. Predstavljene su tipologije i informatičke pretpostavke prilikom formiranja memorije organizacije koja bi u zavisnosti od svojih potrebnih funkcija bazirala na dokumentima, na menadžmentu znanja, bila zasnovana na slučajevima, ili pak bila distribuirana ili predstavljala kombinaciju raznih drugih tehnika. Poseban kritički osvrt stavljen je na probleme upravljanja sa velikom količinom podataka, a odnosi se na: Big Data sisteme, sisteme za planiranje poslovnih resursa – ERP sisteme, Data Warehouse sisteme, Računarstvo u oblaku – Cloud Computing sisteme i Hadoop sisteme, jer korist za sebe iz ove digitalne revolucije mogu da izvuku samo one kompanije koje su sposobne da podacima efikasno upravljaju i da iz njih izvuku zaključke koji vode efikasnim poslovnim odlukama.

Sedmo poglavlje predstavlja uvod u treću celinu doktorske disertacije i posvećeno je optimizaciji zaštite memorije organizacije. Najpre je razmatrano opšte stanje u oblasti istraživanja kroz analizu pretnji i ranjivosti memorije organizacije uz objašnjenje sofistikacije malvera i raznih vrsta napada. Završni deo ovog poglavlja disertacije analizira zaštitu kontejner tipa kroz opis antivirusne i Firewall zaštite, odnosno daje pregled koncepata IDS/IPS sistema i slojevite zaštite. Objašnjene su faze reagovanja na napad i dat je pregled sistema za sprečavanje upada. U završnom delu poglavlja kritički su analizirani koncept sistema reaktivne i proaktivne

zaštite i predložene su organizacione mere zaštite kroz politiku bezbednosti informacija, procenu rizika, identifikaciju resursa i bezbednosnih mera za zaposlene

Osmo poglavlje posvećeno je kriptografiji i logički je nastavak treće celine disertacije koji obrazlaže teorijske osnove istraživanja. Uvidom u veliki broj naučnih radova, navedene su prepoznate prednosti osnovnih šifarskih sistema, kao i njihov značaj na polu zaštite privatnosti i informacija. Predstavljeni su simetrični i asimetrični šifarski sistemi, kao i Diffie-Hellman protokol za razmenu ključeva. Poseban osvrt dat je na digitalnom potpisu i upravljanju ključevima. Osim već poznatih rezultata na polju zaštite privatnosti, kriptografska rešenja daju nam i nove ideje o mogućnostima upravljanja ključevima. Razmatraju se i novi principi kao i pristupi u okviru servisa za autentifikaciju, naročito u segmentu odvojene optimizacije pojedinih podsistema u kompanijama. Analizira se i RSA algoritam, digitalni potpis kao i sertifikati i infrastruktura javnih ključeva.

U devetom poglavlju se kritički analizira studiju slučaja kriptografskog rešenja zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije. Prikazana je studija slučaja, sa jednim hipotetičkim pristupom sa aspekta jake kontrole pristupa i višeslojne arhitekture zaštite memorije organizacije. Skup podataka i metodologija istraživanja u ovoj studiji slučaja dovodi do profilisanja sertifikata koji će se upotrebljavati u PKI sistemu. Vrši se izdvajanje atributa koji regulišu upotrebu korporativnih identifikacionih kartica u informacionom sistemu kompanije. Predlaže se višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije u korišćenju resursa memorije organizacije. Predložen je testiran model jake kontrole pristupa i mehanizmi zaštite informacionog sistema – memorije organizacije koja obuhvata mehanizme zaštite baza podataka i sprečava curenje podataka iz analitičkih sistema. Na kraju, dat je kritički osvrt na rešenje i predložene su smernice za eventualna dalja istraživanja, odnosno hipotetičko rešenje datog problema.

Deseto poglavlje je zaključak gde su jasno izdvojeni naučni i stručni doprinosi ove doktorske disertacije i predloženi pravci daljih istraživanja. Sumirani su svi ciljevi koji su postavljeni na početku istraživanja. Predstavljeni su i ostvareni rezultati i doprinosi u radu. Izvršeno je razmatranje moguće oblasti u kojima se predloženo rešenje kriptografske zaštite može primeniti. Kao osnovne oblasti primene identifikovani su većina kriptosistema koji egzistiraju u kompanijama, prvenstveno oni sistemi koji su od velike važnosti za informacionu bezbednost kako velikih kompanija, tako i državnih institucija

Na kraju rada dat je spisak literature koja je korišćena prilikom izrade ove doktorske disertacije. Takođe, dat je i spisak slika i spisak tabela predstavljenih u ovoj doktorskoj disertaciji.

6. Postignuti rezultati i naučni doprinos doktorske disertacije

U doktorskj disertaciji se predlaže generalizovani model zaštite u oblasti informcionih tehnologija sa predlogom kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja, čime bi se značajno povećala bezbednost komunikacije unutar memorije organizacije i ujedno izvršilo poboljšanje performansi za upravljanje i zaštitu znanja kompanije (kroz integraciju sistema organizovanja dokumenata, pretraživanja, analizu, čuvanje, i hijerarhijsko upravljanje dokumentima u memoriji organizacije).

Stručni doprinos ove doktorske disertacije odnosi se na predlog primene kriptografskih mehanizama zaštite i upotrebe svih dostupnih mogućnosti koje pruža memorija organizacije zasnovana na menadžmentu znanja u jednoj kompaniji. Osim toga, dat je pregled tehnologija, alata, softverskih rešenja i vodećih baza podataka koje se mogu pogodno koristiti za razvoj i

unapređenje memorije organizacije kroz integrisano automatizovano upravljanje, kao i pregled međunarodnih standarda za bezbednost informacija kroz definisanu poverljivost, integritet i pristup informacijama u kompaniji. Pored toga, predložen je razvoj kriptografskih rešenja zaštite integrisanog automatizovanog procesa upravljanja memorije organizacije zasnovane na menadžmentu znanja, kroz rešenja za upravljanje i zaštitu dokumenata, kroz integraciju sistema organizovanja dokumenata, pretraživanja, analize, čuvanja, i hijerarhijskog upravljanja dokumentima. I na kraju izvršena je analiza primera korišćenja standardne metodologije i alata za softversko modelovanje za implementiranje otvorenih standarda i omogućavanje njihove integracije sa drugim aplikativnim rešenjima za poslovno odlučivanje, kao što su ERP sistem, e-mail sistem, aktivni direktorijum.

Naučni doprinos ovog istraživanja obuhvata pregled, analizu i klasifikaciju postojećih kriptografskih rešenja u zaštiti integrisanog automatizovanog sistema upravljanja memorije organizacije, kao najznačajnijeg resursa svake kompanije. Doprinos ove doktorske disertacije odnosi se na poboljšanje nivoa zaštite integrisanog automatizovanog procesa upravljanja memorije organizacije u savremenom poslovnom odlučivanju, kroz pregled, analizu, klasifikaciju i kriptografsku zaštitu svih segmenata organizacije u skladu sa savremenim zahtevima poslovanja. Isto tako, predložena realizacija kriptografskih rešenja zaštite integrisanog automatizovanog upravljanja memorijom organizacije, obezbeđuje se jedinstvena sredina za rad sa dokumentima, kao i brz, kontrolisan i bezbedan pristup na svim nivoima. Dat je predlog smernica za dalji razvoj pristupa kriptografskoj zaštiti integrisanog automatizovanog upravljanja memorijom organizacije na bazi menadžmenta znanja.

Može se diskutovati i kolika je upotrebna vrednost ovakvih kompleksnih rešenja. Predložena, rešenja mogu biti nepraktična i komplikovana za upotrebu. Kod takvih rešenja odziv sistema može biti veoma spor. Ukoliko se šifruju svi podaci i sve komunikacije, kao i pristup i kontrola resursima organizacije, upotreba takvih sistema je veoma složena, teška i sigurno vema spora. Dakle, primenom maksimalne kriptografske zaštite u svim segmentima u radu jedne organizacije dovodi do usporavanja i do neefikasnosti u komunikacijama. Ipak, kada su informacije od izuzetnog značaja one moraju da se štite. Upravo je stvar kod upravljanja ovakvim sistemima, pa i kod projektovanja i realizacije, da se odredi prava mera potrebnih kriptografskih rešenja, kompleksnosti nosećih tehnologija, potrebnoj dužini i veku važenja kriptografskih ključeva i sl.

Rezultati rada se mogu koristiti za široki spektar komercijalnih potreba i rešenja za kriptografsku zaštitu memorije organizacije. Od korisnika takvih rešenja se ne zahteva profesionalno poznavanje kriptografije. Ostvarena komunikacija sa memorijom organizacije obezbeđuje visok stepen tajnosti za aplikacije koje koriste simetrične i asimetrične kriptografske ključeve. Za profesionalne sisteme zaštite, ostvareni rezultat se može posmatrati kao korak više u zaštiti kada se posmatraju kombinovana rešenja sa nadšifrovanjem i sakrivanjem šifrovanog materijala

7. Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Dragana Savića po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanja i donetim zaključcima zadovoljava kriterijume zahtevane za doktorsku disertaciju, te se može prihvatiti kao podobna za javnu odbranu.

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Dragana Savića pod nazivom „Kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja“, predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

Beograd, 22/02/2021.

Članovi komisije:

prof. dr Mladen Veinović, mentor,
Redovni profesor, Univerzitet Singidunum

prof. dr Milan Milosavljević, član,
Redovni profesor, Univerzitet Singidunum

prof. dr Petar Spalević, član,
Redovni profesor, Univerzitet u Prištini
sa privremenim sedištem u Kosovskoj Mitrovici