Sveučilište u Zagrebu

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Aleksandar Klaić

# METODA MODELIRANJA POLITIKA INFORMACIJSKE SIGURNOSTI TEMELJENA NA UPRAVLJANJU ZNANJEM

DOKTORSKI RAD

Zagreb, 2014.

Sveučilište u Zagrebu

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ALEKSANDAR KLAIĆ

# METODA MODELIRANJA POLITIKA INFORMACIJSKE SIGURNOSTI TEMELJENA NA UPRAVLJANJU ZNANJEM

DOKTORSKI RAD

Mentor:

Izv. prof. dr. sc. Marin Golub

Zagreb, 2014.

University of Zagreb

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Aleksandar Klaić

# KNOWLEDGE MANAGEMENT BASED METHOD FOR MODELLING OF INFORMATION SECURITY POLICIES

DOCTORAL THESIS

Supervisor:

Associate Professor Marin Golub, Ph.D.

Zagreb, 2014

Doktorski rad izrađen je na Sveučilištu u Zagrebu,
Fakultetu elektrotehnike i računarstva,
Zavodu za elektroniku, mikroelektroniku, računalne i inteligentne sustave

Mentor:
Izv. prof. dr. sc. Marin Golub

Doktorski rad ima: 238 stranica

Doktorski rad br.:_____

## O mentoru:

Marin Golub rođen je u Varaždinu 1968. godine. Diplomirao je, magistrirao i doktorirao u polju računarstva na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva (FER), 1992., 1996. odnosno 2001. godine.

Od srpnja 1993. godine radi na Zavodu za elektroniku, mikroelektroniku, računalne i inteligentne sustave FER-a. U lipnju 2010. godine izabran je u zvanje izvanrednog profesora. Sudjelovao je na šest znanstvenih projekata Ministarstva znanosti, obrazovanja i sporta Republike Hrvatske. Trenutno sudjeluje u Europskom COST istraživačkom programu projektne suradnje na projektu „Pouzdana proizvodnja i uporaba sigurnosnih uređaja". Objavio je više od 50 radova u časopisima i zbornicima konferencija u području evolucijskog računanja i sigurnosti računalnih sustava.

Član je strukovnih udruga IEEE i MIPRO. Sudjeluje kao recenzent u nekoliko znanstvenih časopisa.

## About the Supervisor:

Marin Golub was born in Varaždin in 1968. He received B.Sc., M.Sc. and Ph.D. degrees in computer science from the University of Zagreb, Faculty of Electrical Engineering and Computing (FER), Zagreb, Croatia, in 1992, 1996 and 2001, respectively.

From July 1993 he is working at the Department of Electronics, Microelectronics, Computer and Intelligent Systems at FER. In June 2010 he was promoted to Associate Professor. He participated in 6 scientific projects financed by the Ministry of Science, Education and Sports of the Republic of Croatia. Currently he participates European COST cooperation framework in the action „Trustworthy Manufacturing and Utilization of Secure Devices". He published more than 50 papers in journals and conference proceedings in the area of evolutionary computation and computer system security.

He is a member of IEEE and MIPRO. He is also a technical reviewer for various international journals.

*Zahvaljujem mentoru, profesoru Marinu Golubu*

*Zahvaljujem na beskrajnom strpljenju svojoj obitelji*
*Mislavu, Luki i Đurđi*

***SAŽETAK:***

*Politike i norme informacijske sigurnosti prisutne su već desetljećima u poslovanju različitih organizacijskih entiteta u državnim sektorima zemalja i međunarodnim organizacijama, a tijekom tog razdoblja postale su redovita praksa i u poslovnim sektorima. Dosadašnji razvoj politika i normi informacijske sigurnosti uglavnom je bio usmjeren prema različitim, usko profiliranim sektorskim pristupima, što je rezultiralo slabom povezanošću znanja na široj domenskoj razini. Za razliku od srodnih istraživanja koja analiziraju pojedine politike i norme informacijske sigurnosti ili neke uže domenske segmente, u ovom radu pristupilo se analizi šireg domenskog područja.*

*Provedena je analiza s ciljem šire domenske sistematizacije i integracije različitih pristupa i zahtjeva globalnog i lokalnog okruženja te dominantnih suvremenih politika i normi informacijske sigurnosti. Predložena je metoda modeliranja kojom se obuhvaća sustavski prikaz životnog ciklusa politike informacijske sigurnosti u globalnom okruženju, transformiran u hijerarhijsku domensku taksonomiju, uz pomoć koje se ostvaruje sadržaj modela u obliku domenskog rječnika, kategorizacije i hijerarhijskih odnosa koncepata te međusobnih relacija i atributa koncepata. Konceptualni metamodel ostvaren je kao okvir za upravljanje i komuniciranje znanjem kojim se povezuje postojeće heterogeno i slabo povezano domensko znanje iz dominantnih politika i normi informacijske sigurnosti. Formalna specifikacija konceptualnog metamodela (rječnik, sintaksa i semantika), temelj je za ostvarenje programskog ontološkog metamodela koji se koristi za provjeru valjanosti konceptualnog metamodela te za provjeru svojstava koja se postižu njegovom primjenom. Studijama slučajeva koje su ostvarene programskim ontološkim modelima, potvrđena su tražena svojstva jednostavnosti, dosljednosti, sveobuhvatnosti i učinkovitosti upravljanja životnim ciklusom politika informacijske sigurnosti modeliranih predloženom metodom.*

***Ključne riječi:*** *informacijska sigurnost, politika informacijske sigurnosti, norma, domena, taksonomija, metoda modeliranja, sustavski pristup, upravljanje znanjem, konceptualni metamodel, programski ontološki model.*

***ABSTRACT: KNOWLEDGE MANAGEMENT BASED METHOD FOR MODELLING OF INFORMATION SECURITY POLICIES***

*Information security policies and standards are present for decades within the business operations of different organizational entities in government sectors and international organizations. During that period of time, different security policies and standards became also the best practice in various business sectors. Past experience in the development of the security policies and standards is that they were mostly oriented towards narrowly specialized approach of each of the various sectors. The result of such approach is very weak correlation of the knowledge on the wider level of information security domain. This research is aimed at the wider level of information security domain in difference to some related researches that analyse certain standards, policies within certain business sectors, or some narrow functional domain segments.*

*The goal of this research is to correlate mutually different approaches in different sectors on the wider level of information security domain. The research comprises the chosen security policies and standards in the contemporary practises of different government and business sectors that are dominant in the global environment. The key research questions are: can the conceptualisation of the information security domain correlate existing heterogeneous and weakly related domain knowledge, and whether the lifecycle management of the security policies based on such conceptualisation will be simpler, more consistent, more comprehensive, and more efficient.*

*The first chapter "Introduction" describes the research field, motivation and the research goals, as well as the research questions. Chapter 2 "Modelling of Information Security Policies" explains the various methods and techniques used within the proposed method for modelling of security policies, such as conceptualisation, ontology methods, system approach, and domain taxonomy. Chapter 3 "Overview of Related Researches" analyses the state of play in the research field of information security and the related researches.*

*Chapter 4 "Analysis of Information Security Policies and Standards" analyses the wider level of information security domain in order to systematize and integrate the approaches of different sectors, different requirements from the global and local environments, and different characteristics of dominant information security policies and standards. Based on this analysis, and the process of abstraction and generalization of related concepts typical for dominant*

*security policies and standards, common domain concepts are proposed as the general domain vocabulary shown in annex A.*

*Chapter 5, "Knowledge Management Based Method for Modelling of Information Security Policies", proposes the method for modelling of security policies. The method comprises the system scheme of the security policies lifecycle shown in the global environment. Using the appropriate transformation, the scheme is realized in the way that is more appropriate for the elaboration of hierarchical domain taxonomy and for creating of subsystems of the conceptual metamodel. The proposed structure of the conceptual metamodel comprises of four organizational levels of this complex system with 18 subsystems. The metamodel structure is verified against the chosen dominant security policies and standards. Further elaboration of the metamodel content is done with the use of ontology methods for shaping the concepts and subconcepts. The elaborated hierarchical domain taxonomy is shown in annex B.*

*Chapter 6 "The Realization of the Conceptual Metamodel of Information Security Policies", based on the hierarchical domain taxonomy and further elaboration of attributes and mutual relations of domain concepts, describes the realization of conceptual metamodel using UML (Unified Modelling Language). This conceptual metamodel correlates the existing heterogeneous and weakly related domain knowledge. It also realizes the framework for the management and communication of the domain knowledge that comprises different approaches within different sectors, based on the chosen dominant security policies and standards. The conceptual model developed in UML has high level of clearness, comprehensibility, and visualization of the domain concepts, which makes it very appropriate for the communication among different security officers and other responsible persons within the different organizations. The conceptual model developed in UML also offers the formal specification consisted of vocabulary (domain taxonomy), syntax (categories and hierarchies of the classes representing concepts), and semantics (attributes and mutual relations of the classes). Besides UML notation, in annex C there is the table of the descriptions of all the relations defined among the classes of the metamodel. The formal specification is intended for software based development of the conceptual metamodel.*

*Chapter 7 "The Realization of the Software Based Ontology Model" describes the realization of the software based ontology model developed using Protégé Frames. Ontology model is used for the verification of the research results obtained by the proposed method and realized conceptual metamodel in UML. The verification is based on the case studies that comprise of*

*the security policy modelling of the organizational entities from government sector and from business sector. Third case study presents the solution for adapting modelled security policies of these two different organizations from different sectors for mutual business cooperation and sensitive information sharing (classified contract). Using the developed software based ontology metamodel, necessary policies were modelled as ontology models elaborated from the same metamodel. These case studies verify that the lifecycle management of the security policies modelled using the proposed method become simpler, more consistent, more comprehensive, and more efficient. The case studies also verify that the proposed modelling method and the realised conceptual metamodel represent the comprehensive solution for the wider domain level. Chapter 8 "Conclusion" gives the conclusion and guidelines for the future research.*

*The thesis describes the analysis realised with the view to comprise wider domain systematization and integration of different approaches and requirements within the global and local environment and the dominant information security policies and standards. The proposed method of policy modelling comprises the system scheme of the security policies lifecycle shown in the global environment, and transformed into hierarchical domain taxonomy. Hierarchical domain taxonomy is used to realize the content of the model comprised of vocabulary, sintax, and semantics. Conceptual metamodel is realised as the framework for the management and communication of the wider domain knowledge that correlates existing heterogeneous and weakly related domain knowledge from the dominant information security policies and standards. Formal specification of the conceptual metamodel (vocabulary, sintax, and semantics) is the base for the realization of software based ontology metamodel. The ontology metamodel is used for the verification of the research results, proposed policy modelling method and realised conceptual metamodel. Case studies that are realised using the ontology metamodel verify the required characteristics of the lifecycle management of the security policies modelled using the proposed method. It is verified that the lifecycle management becomes simpler, more consistent, more comprehensive, and more efficient.*

***Keywords:*** *Information Security, Security Policy, Standard, Domain, Taxonomy, Modelling Method, System Approach, Knowledge Management, Conceptual Metamodel, Software Based Ontology Model.*

# SADRŽAJ:

# 1. UVOD

## 1.1. Područje istraživanja

Politike informacijske sigurnosti imaju sve veći značaj i ulogu u razvoju suvremenog društva. Osobito je to vidljivo tijekom posljednjih nekoliko desetljeća, u postupnom jačanju važnosti međunarodne suradnje i sve većem utjecaju formalnih oblika međunarodnog organiziranja (npr. Organizacija sjeverno-atlantskog ugovora - NATO) koje su pratili i odgovarajući zahtjevi za međusobnu razdiobu i zaštitu osjetljivih podataka. Iako su politike informacijske sigurnosti koje su nastale u tom razdoblju imale puno zajedničkih elemenata, istovremeno su sadržavale i značajne razlike u pristupu, najvidljivije usporedbom suvremenog pristupa informacijskoj sigurnosti u poslovnom i državnom sektoru [1]. Tradicionalni pristup politici informacijske sigurnosti u državnom sektoru (engl. *Security Policy*), nastao je prije razdoblja sveopće internetizacije, a temelji se na uspostavi minimalnih sigurnosnih mjera u definiranim područjima informacijske sigurnosti. Temeljni cilj politike informacijske sigurnosti državnog sektora postizanje je zajedničkih minimalnih sigurnosnih zahtjeva za zaštitu klasificiranih podataka u iznimno heterogenom i složenom sustavu organizacije državnog sektora. Složenost sigurnosnih zahtjeva u najvećoj mjeri proizlazila je iz vanjskih čimbenika, odnosno iz procesa društvenih promjena, a tako je i danas. Primjeri ovog utjecaja su: zahtjevi transparentnosti na proces klasificiranja podataka u državnom sektoru koji uključuju potrebu razlikovanja klasificiranih (tajnih) i označenih neklasificiranih (osjetljivih) podataka, zahtjevi prava na pristup informacijama (engl. *Freedom Of Information - FoI*), zahtjevi zaštite osobnih podataka, liberalizacija telekomunikacija, potrebe i zahtjevi javno-privatnog partnerstva u različitim područjima poput zaštite kritične infrastrukture, te u novije vrijeme i cjelokupni kibernetički prostor s nizom povezanih, tehnološki i društveno isprepletenih sigurnosnih pitanja i problema.

Nasuprot tome, ozbiljniji utjecaj poslovnog sektora na razvoj područja informacijske sigurnosti, postaje primjetniji tek u drugoj polovini devedesetih godina prošlog stoljeća. Ključni proces koji je doveo do toga bila je inicijativa za izradu najbolje sigurnosne prakse britanskog Ministarstva trgovine i industrije (engl. *Department of Trade and Industry - DTI*) koja je 1995. g. rezultirala britanskom normom BS 7799:1995, a nekoliko godina kasnije preuzeta je međunarodnom normom ISO/IEC 17799:2000 i danas je detaljnije razrađena u

paleti međunarodnih normi ISO/IEC 27000 te se široko koristi i u poslovnom i u državnom sektoru. Za razliku od zaštite klasificiranih podataka u državnom sektoru i minimalnih sigurnosnih zahtjeva državnog sektora, ciljevi primjene informacijske sigurnosti u poslovnom sektoru postavljeni su šire i uključuju procijenjene poslovne vrijednosti i imovinu, a prevladavajući sigurnosni pristup usmjeren je na metode upravljanja rizikom. Brzi razvoj informacijske i komunikacijske tehnologije te širenje Interneta na prijelazu stoljeća, bili su ključni vanjski utjecaji koji su oblikovali pristup informacijskoj sigurnosti u poslovnom sektoru [2]. Stoga se informacijska sigurnost poslovnog sektora isprva usko usmjeravala na sigurnost informacijske tehnologije (IT) i imala vrlo malo doticaja sa sveukupnom poslovnom i sigurnosnom strategijom tvrtki. Sve veća ovisnost poslovnih procesa o tehnologiji i razvoj internetskog tržišta, počinju utjecati na sustavni pristup informacijskoj sigurnosti u poslovnom sektoru te na integraciju IT sigurnosti u širi skup mjera informacijske sigurnosti.

Područje istraživanja ovog rada usmjereno je na današnje stanje i trendove razvoja politika informacijske sigurnosti, njihove zahtjeve i način korištenja te oblike pojavnosti politika informacijske sigurnosti u državnom i poslovnom sektoru, kako u nacionalnom, tako i u međunarodnom okruženju. U okviru ovog istraživanja politiku informacijske sigurnosti definiramo kao skup procedura kojima se planira, ostvaruje, provodi i preispituje informacijska sigurnost u određenom opsegu primjene, što predstavlja životni ciklus politike informacijske sigurnosti.

## 1.2. Motivacija istraživanja

Područje politika informacijske sigurnosti suočava se danas s problemom sve veće složenosti sigurnosnih zahtjeva koji se postavljaju u različitim sektorima društva (npr. financijski sektor, sektor davatelja elektroničkih usluga i sl.), ali i globalno, u okvirima međunarodnih organizacija (npr. NATO, EU) i različitim oblicima međudržavne i poslovne suradnje (npr. međunarodne mirovne vojne misije, klasificirani ugovori). Složenost sigurnosnih zahtjeva, osim već spomenutog utjecaja niza vanjskih čimbenika, proizlazi iz različitih načina njihovog propisivanja i utvrđivanja koje uobičajeno obuhvaća zakonske i podzakonske akte, unutarnje pravne akte poslovnih organizacija, norme, smjernice, etičke kodekse i sl. [3]. Pri tome, doseg primjene neke od spomenutih vrsta akata koji utvrđuju sigurnosne zahtjeve ponekad nije lako utvrditi, jer može biti povezan s međunarodnom organizacijom, državom, sektorom poslovanja, vlasništvom pravne osobe ili, primjerice, s državom registracije pravnog subjekta.

Složenost sigurnosnih zahtjeva dodatno uzrokuje i njihova uska profiliranost na ciljani sektor i određeno područje primjene [4]. Posljedica toga je slaba međusobna koordinacija različitih stupova sigurnosnih zahtjeva (npr. zaštita klasificiranih podataka, osobnih podataka, poslovne tajne, kritične infrastrukture, kao i različiti oblici obvezujuće provedbe norme ISO/IEC 27001 i sl.). Ovi problemi slabe koordinacije provedbe različitih stupova sigurnosnih zahtjeva uočljivi su u procesima planiranja sektorskih politika informacijske sigurnosti u nadležnim institucijama, u procesima provedbi politika informacijske sigurnosti u različitim organizacijama iz državnog ili poslovnog sektora koje su obveznici određenih sigurnosnih zahtjeva, kao i u okviru različitih procesa nadzora provedbe mjera informacijske sigurnosti.

Ako se promatra uloga politika informacijske sigurnosti u širem kontekstu današnjeg stanja i razvoja suvremenog društva, potrebno je uzeti u obzir obilježja koja su vidljiva kao trendovi razvoja i koja dodatno traže određenu prilagodbu pristupa u suvremenim politikama informacijske sigurnosti. Ključne promjene i prilagodbe pristupa, potrebne su prvenstveno zbog razvoja globalne komunikacijske i informacijske infrastrukture (kibernetički prostor) i zbog nužnosti njenog zajedničkog korištenja i u državnom i u poslovnom sektoru, odnosno u društvu u cjelini [5].

Svakim danom prisutni su sve širi zahtjevi sigurnosne suradnje i međusobne razdiobe osjetljivih i tajnih podataka između različitih tvrtki, sektora, država i međunarodnih organizacija. Postoji čitav niz regulativnih i poslovnih razloga međusobne i međunarodne sigurnosne suradnje različitih pravnih osoba iz javnog i privatnog sektora, kao što je multilateralna međunarodna suradnja (npr. EU, NATO, međunarodne mirovne vojne misije), bilateralna međunarodna suradnja (npr. granična, policijska, ili pravosudna međudržavna suradnja), javno-privatna suradnja (npr. nacionalna ili EU kritična infrastruktura, klasificirani projekti, regulacija pojedinih gospodarskih sektora kao što su sektor elektroničkih komunikacija, ili financijski sektor), poslovna sektorska suradnja (npr. udruživanje tvrtki za velike projekte na nacionalnoj, međudržavnoj i međunarodnoj razini), kao i tržište elektroničkih usluga i projekti elektroničke državne uprave, odnosno suradnja državna uprava – gospodarstvo - građanstvo u najširem smislu (engl. *Government – Bussines – Citizens, GBC*).

Trendovi korištenja zajedničke globalne infrastrukture i sve češći i složeniji zahtjevi razdiobe osjetljivih podataka između organizacija koje pripadaju različitim sektorima i državama, nužno utječu na sve veću potrebu usklađivanja različitih stupova sigurnosnih zahtjeva i traže sve veće međusobno razumijevanje i usklađivanje različitih pristupa i sadržaja politika informacijske sigurnosti u organizacijama koje moraju međusobno surađivati i organizirati razdiobu osjetljivih i tajnih podataka. Nedostatak općenitijeg pristupa području informacijske sigurnosti na široj domenskoj razini, koji bi obuhvatio i međusobno približio različite sektorske pristupe i usko profilirane sigurnosne zahtjeve, predstavlja ključnu motivaciju ovog rada.

## 1.3. Istraživački problem

Općenitiji pristup području informacijske sigurnosti traži sistematizaciju i integraciju šire domenske razine koja bi u dovoljnoj mjeri poopćila i međusobno povezala određeni broj ključnih pojmova i koncepata iz područja informacijske sigurnosti, kako bi se obuhvatili i međusobno približili sadašnji, vrlo različiti sektorski pristupi i usko profilirani sigurnosni zahtjevi. Stoga se u ovom istraživanju težište stavlja na pristup široj domenskoj razini informacijske sigurnosti koja se predstavlja uz pomoć odabranih dominantnih politika i normi prepoznatih u suvremenoj praksi.

Problem povezivanja domenskog znanja mora obuhvatiti različite aspekte domene informacijske sigurnosti. Potrebno je uzeti u obzir značaj ključnih čimbenika informacijske sigurnosti, kako tradicionalno korištenih čimbenika: osoba, tehnologije i procesa, tako i danas široko prihvaćenih i prepoznatih utjecaja organizacijskog čimbenika [6]. Nadalje, potrebno je na odgovarajući način sistematizirati i povezati utjecaje globalnog i lokalnog okruženja neke organizacije koja provodi politiku informacijske sigurnosti i osigurati povezivanje različitih faza životnog ciklusa politika informacijske sigurnosti [7].

Temeljno pitanje na koje se želi dati odgovor u ovom radu jest:

- Može li se konceptualizacijom domene informacijske sigurnosti povezati postojeće heterogeno i slabo povezano domensko znanje iz dominantnih politika i normi informacijske sigurnosti?

Konceptualizacija provedena razvojem zajedničkog rječnika domene te sistematizacijom i formalizacijom ključnih obilježja dominantnih politika i normi informacijske sigurnosti, temelj je za ostvarenje konceptualnog metamodela domene. Na taj način može se ostvariti općenitiji pristup potreban za širu normizaciju domene politika informacijske sigurnosti. Ostvarenjem konceptualnog metamodela dominantnih politika i normi otvaraju se mogućnosti programskog ostvarenja ontoloških modela politika informacijske sigurnosti za potrebe različitih organizacija i sektora, zasnovanih na zajedničkoj domenskoj specifikaciji.

Sljedeće ključno pitanje na koje se želi dati odgovor u ovom radu jest:

- Hoće li upravljanje životnim ciklusom politika informacijske sigurnosti uporabom konceptualnog metamodela domene biti jednostavnije, dosljednije, sveobuhvatnije i učinkovitije?

Normizacija šireg domenskog područja politika informacijske sigurnosti, kao i razvoj odgovarajuće metode modeliranja za ostvarenje konceptualnog metamodela politika informacijske sigurnosti, usmjereni su u okviru ovog istraživanja prvenstveno prema pronalaženju rješenja za rastuće probleme upravljanja i komuniciranja znanjem u vrlo heterogenoj i složenoj domeni informacijske sigurnosti.

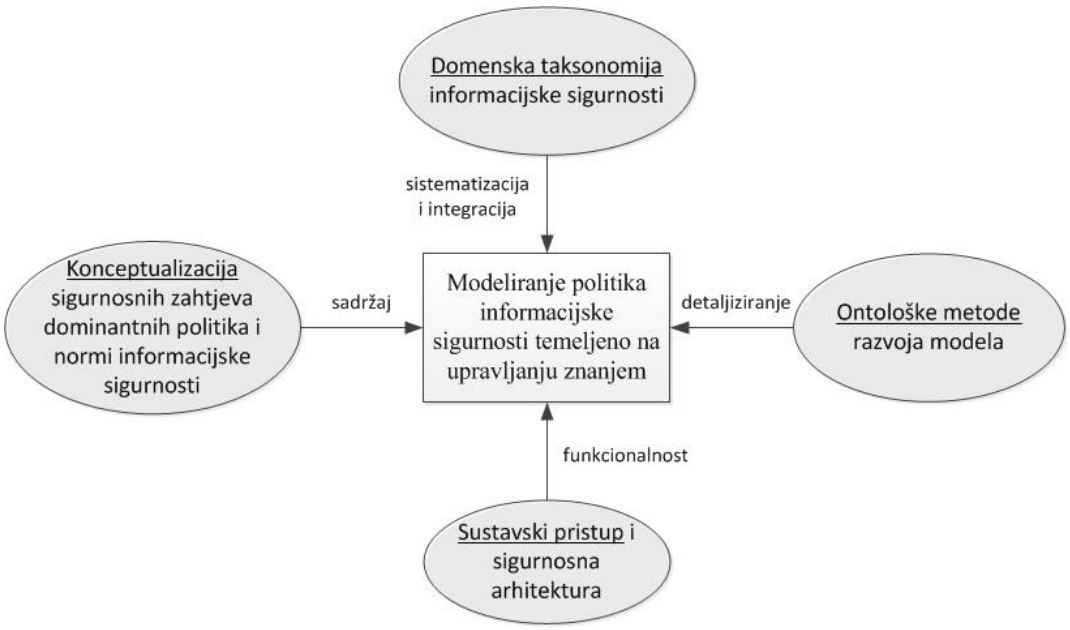
## 1.4. Organizacija rada

Rad je podijeljen na osam poglavlja. Prvo poglavlje je uvod. U drugom poglavlju opisuje se pristup modeliranju politika informacijske sigurnosti koji se koristi u ovom radu te se definiraju ključni pojmovi u predloženoj metodi modeliranja politika informacijske sigurnosti: konceptualizacija, domenska taksonomija, ontologija i sustavski pristup, kao i njihova osnovna uloga u procesu modeliranja. U trećem poglavlju prikazan je pregled srodnih istraživanja. Četvrto poglavlje opisuje sistematizaciju i integraciju šireg domenskog područja informacijske sigurnosti analizom značenja temeljnih pojmova, opisom nastajanja važnijih koncepata informacijske sigurnosti tijekom njezinog formativnog razdoblja, kao i ključnim obilježjima politika informacijske sigurnosti u dva najvažnija sektora društva: državnom i poslovnom sektoru. Tako se dolazi do analitičkih preduvjeta za ostvarenje predložene metode modeliranja politika informacijske sigurnosti. Peto poglavlje definira okvire istraživanja ovoga rada i daje prikaz predložene metode modeliranja politika informacijske sigurnosti temeljene na upravljanju znanjem. U ovom poglavlju uvode se pretpostavke i ograničenja

modeliranja, daje se prikaz potrebne transformacije modela životnog ciklusa politika informacijske sigurnosti u hijerarhijski model domenske taksonomije te se koriste ontološke metode oblikovanja koncepata. U šestom poglavlju detaljno je prikazan konceptualni metamodel politika informacijske sigurnosti, ostvaren u UML-u (engl. *Unified Modelling Language - UML*), s opisom 18 podsustava metamodela te namjene i načina korištenja metamodela. U sedmom poglavlju prikazuje se programski ontološki metamodel ostvaren uz pomoć programskog razvojnog okruženja *Protégé Frames*. Opisano je korištenje programskog ontološkog metamodela, način ostvarenja instanci klasa metamodela te unos i korištenje podataka za potrebe specifičnih instanci ontoloških modela u odabranim studijama slučajeva. Prikazane su tri studije slučajeva na temelju kojih se provodi provjera valjanosti konceptualnog metamodela, te je dana rasprava o dobivenim rezultatima predložene metode modeliranja na bazi rezultata modeliranja u ovim primjerima. Rad završava zaključkom i smjernicama budućih istraživanja. U prilozima A, B i C u cijelosti su tablično prikazani dobiveni rezultati općeg domenskog rječnika informacijske sigurnosti, hijerarhijske domenske taksonomije dominantnih politika i normi informacijske sigurnosti te relacije između klasa definiranih u konceptualnom UML metamodelu zasnovanom na hijerarhijskoj domenskoj taksonomiji.

# 2. MODELIRANJE POLITIKA INFORMACIJSKE SIGURNOSTI

Općenitiji pristup području informacijske sigurnosti, nužan za rješavanje postavljenih istraživačkih problema u poglavlju 1.3, traži pojmovnu i konceptualnu razradu šire domenske razine. Takva razrada može u zadovoljavajućoj mjeri poopćiti i međusobno povezati određeni broj ključnih pojmova i koncepata iz područja informacijske sigurnosti, kako bi se obuhvatili i međusobno približili sadašnji, vrlo različiti sektorski pristupi i uskonamjenski sigurnosni zahtjevi. Težište ovog istraživanja stoga je na široj domenskoj razini informacijske sigurnosti, koja se predstavlja uz pomoć odabranih dominantnih politika i normi prepoznatih u suvremenoj praksi. Povezivanje domenskog znanja mora se osigurati na širokom opsegu pojavnosti domene informacijske sigurnosti. Pri tome je potrebno sustavno obuhvatiti niz različitih pojmova prisutnih u domenskom znanju, oblikovati koncepte koje ovi pojmovi predstavljaju te ih međusobno povezati u model. Model treba na odgovarajući način pridonijeti rješavanju problema uočenih i opisanih u motivaciji ovog istraživanja i definiranih preko istraživačkog problema. Ključni pojmovi i prateća teorijska područja koja se koriste u predloženoj metodi modeliranja politika informacijske sigurnosti temeljenoj na upravljanju znanjem, kao i njihova osnovna uloga u procesu modeliranja provedenom u okviru ovog rada, prikazani su na slici 2.1.




**Slika 2.1:** Ključni pojmovi koji se koriste u predloženoj metodi modeliranja politika informacijske sigurnosti te njihova osnovna uloga u procesu modeliranja

## 2.1. Konceptualizacija

Postoje četiri različita pristupa konceptima koja se koriste u različitim znanstvenim područjima [8]:

- psihološki pristup - definira koncepte kao mentalne entitete, analogno idejama ili uvjerenjima;
- lingvistički pristup - definira koncepte kao značenje općih pojmova;
- epistemologija - filozofska teorija znanja koja promatra koncepte kao jedinice znanja, na sličan način kako se to danas široko koristi u različitim vidovima „predstavljanja znanja“;
- ontološki pristup - koncepte definira kao apstrakciju vrste i obilježja nekog pojavnog entiteta.

U današnjim primjenama konceptualizacije u računalnoj znanosti, moguće je pronaći mješavinu svih ovih pristupa [9]. Pri tome su osnovni načini tvorbe pojmova apstrakcija, generalizacija i specijalizacija. Apstrakcija je tvorba pojmova koja nastaje tako što se na osnovi određenog broja primjera izdvaja ono svojstvo koje im je zajedničko, a ostala svojstva se zanemaruju (apstrahiraju). Generalizacija je oblik tvorbe pojmova u kojemu se već usvojenom pojmu, oduzima neko obilježje te se takvim postupkom može dobiti novi pojam koji će biti općenitiji od početno usvojenog pojma. Specijalizacija je oblik tvorbe pojmova u kojemu se već usvojenom pojmu dodaje novo obilježje te se takvim postupkom može dobiti novi pojam koji će biti manje općenit, odnosno posebniji od početno usvojenog pojma. Postupci apstrakcije, generalizacije i specijalizacije, koriste se u ovom radu za potrebe usporedne analize dominantnih politika i normi informacijske sigurnosti, u kojima se u svrhu stvaranja šireg domenskog rječnika, moraju prepoznati osnovna zajednička obilježja, odnosno pojmovi, kojima bi se na jedinstven način opisalo šire domensko područje.

Konceptualizacija općenito predstavlja formalno opisivanje različitih fizičkih i društvenih pojavnosti u svrhu boljeg i lakšeg razumijevanja i komunikacije među ljudima [10]. Konceptualizacija se bavi značenjem pojmova i namijenjena je prvenstveno ljudima u svrhu komunikacije i boljeg razumijevanja domene koja se konceptualizira. To znači da je cilj konceptualizacije uvođenje apstrakcije, odnosno odgovarajuće razine poopćavanja, koja će osigurati smanjivanje složenosti određene pojavnosti s ciljem boljeg razumijevanja ljudi i lakšeg komuniciranja među ljudima o toj pojavnosti. Analiziranje odnosa poslovnih procesa i tehnologije korištenjem konceptualnih modela, pokazalo se vrlo uspješnom metodom pristupa

složenom području upravljanja i informatizacije poslovnih procesa [10]. Prednost konceptualizacije je jasan prikaz semantike određene aplikacije ili projekta uz pomoć formalnog zapisa. Loša strana je to što su rezultati prvenstveno namijenjeni za potrebe čovjeka te u smislu programskog ostvarenja mogu poslužiti samo kao specifikacija zasnovana na formalnom zapisu konceptualizacije [11].

Područje u kojem se konceptualizacija danas široko koristi jest područje metamodeliranja [11, 12]. Metamodel je općenito model kojim se definira jezik za opisivanje izvedenih modela. Konceptualizacija se koristi u metamodeliranju upravo zbog mogućnosti specificiranja intuitivnog jezika za komuniciranje ljudi o različitim modelima, primjerice između stručnjaka različitog strukovnog profila. U tom smislu, konceptualni model nekog sustava treba zadovoljiti osnovne zahtjeve kao što su:

- poboljšano razumijevanje tako modeliranog sustava;
- učinkovita mogućnost razdiobe informacija o modelu između zainteresiranih strana;
- osiguravanje odgovarajuće specifikacije sustava za projektante i programere;
- dokumentiranje sustava u svrhu njegovog održavanja i unaprjeđenja, odnosno općenito, u svrhu bolje međusobne suradnje korisnika koji mogu imati različite uloge i načine korištenja neke složene domenske razine.

Prikazani osnovni zahtjevi konceptualizacije predstavljaju i razlog korištenja konceptualizacije u ovom istraživanju. Domenu informacijske sigurnosti obilježava složeno, heterogeno i slabo povezano domensko znanje. Konceptualizacijom se stoga definira sadržaj pojedinih segmenata domene predstavljene dominantnim politikama i normama informacijske sigurnosti, odnosno značenje takvog sadržaja korisnicima (različiti sektori društva, različiti profili stručnjaka i korisnika). Konceptualizacijom se provode usporedbe i prepoznavanje pojedinih općenitih koncepata (procesi, objekti, kontrole, ključni čimbenici politika informacijske sigurnosti i sl.), kao i atributa i relacija između koncepata. U tom smislu, konceptualni model predstavlja središnju točku procesa modeliranja (razvoj, specifikacija, održavanje, dorade i proširenja), ali s druge strane, predstavlja i okvir koji omogućava komuniciranje o sadržajima konceptualizirane domene, čime doprinosi boljoj općoj razini međusobnog razumijevanja stručnjaka različitih profila koji surađuju u području informacijske sigurnosti.

Osnovna obilježja konceptualizacije značajna za ovaj rad su:

- primarno je namijenjena ljudima u svrhu boljeg razumijevanja i razvoja međusobne komunikacije;
- koristi rječnik pojmova sa odgovarajućom specifikacijom i međusobnim relacijama između koncepata predstavljenih pojmovima;
- koristi vizualni način zapisa radi jasnoće i razumljivosti.

Konceptualizacija u ovom radu prvenstveno osigurava sadržaje za proces modeliranja politika informacijske sigurnosti temeljen na upravljanju znanjem (slika 2.1). Uvođenje sadržaja u procesu modeliranja provodi se uz pomoć odabira pojmova kojima se definira sadržaj i kontekst primjene, odnosno pojmova koji su pridruženi pripadnim konceptima, definiranim u kontekstu domene od interesa, a to je domena informacijske sigurnosti. Pri tome se kategorije ovako odabranih pojmova protežu od jednostavnih prema složenima, te od konkretnih prema apstraktnima, osiguravajući na taj način, zahtjev općenitosti nužan za opis šire domenske razine s jedne strane, a s druge strane, zahtjev praktične primjenjivosti nužan za modeliranje konkretnih organizacijskih okruženja koja provode politiku informacijske sigurnosti.

## 2.2. Domenska taksonomija

Taksonomija se u ovom radu promatra kao klasifikacijska shema koja strukturira znanje u domeni od interesa i stvara rječnik domene [13]. Na taj način opisuju se pojmovi u određenoj domeni te se definiraju odnosi među pojmovima, odnosno, stvara se osnovna hijerarhijska struktura pojmova (klasa - podklasa). Ovakva hijerarhijska domenska taksonomija, uvodi u odabrani rječnik domene osnovnu vezu specijalizacije. Različite domenske kategorije pri tome predstavljaju grananja taksonomije unutar kojih se razvijaju daljnje hijerarhije pojmova. Rječnik koji se koristi u taksonomiji predstavlja pojmove koji imaju jedinstveno, zajedničko značenje za domenu i kontekst u kojem se primjenjuju, kao primjerice u [14]. U slučaju domene informacijske sigurnosti izbor pojmova koristi se u širokom rasponu njihove zastupljenosti u dominantnim politikama i normama informacijske sigurnosti. Prethodno pojašnjeni pristup konceptualizaciji kao metodi za razvoj metamodela, omogućava korištenje općenitog domenskog rječnika za razinu metamodela, istovremeno zadržavajući mogućnost proširenja, korištenjem specifičnog rječnika za razinu modela nekog ciljanog okruženja u kojem se želi modelirati određena politika informacijske sigurnosti. Ovakav pristup odabran je i u ovom istraživanju i opisuje se u okviru ovog rada.

Taksonomija mora osigurati različite kategorije hijerarhijski strukturiranih pojmova. Uvjeti koji se postavljaju na odabir i razradu kategorija i pojmova taksonomija prema [13] su:

1. međusobno isključivanje, odnosno međusobno nepreklapanje kategorija;
2. iscrpnost, odnosno uključivanje svih mogućnosti;
3. nedvosmislenost i jasnoća;
4. ponovljivost klasifikacije i pristupa pojmovima;
5. prihvatljivost u logičkom i intuitivnom smislu u cilju opće prihvaćenosti;
6. korisnost razdiobe u smislu jasnoće uvida u područje od interesa.

Primjer razrade kategorija i pojmova koji se koriste u domeni informacijske sigurnosti u ovom radu prikazan je na slici 2.2 na primjeru kategorija pojmova iz segmenta nadzora informacijske sigurnosti.

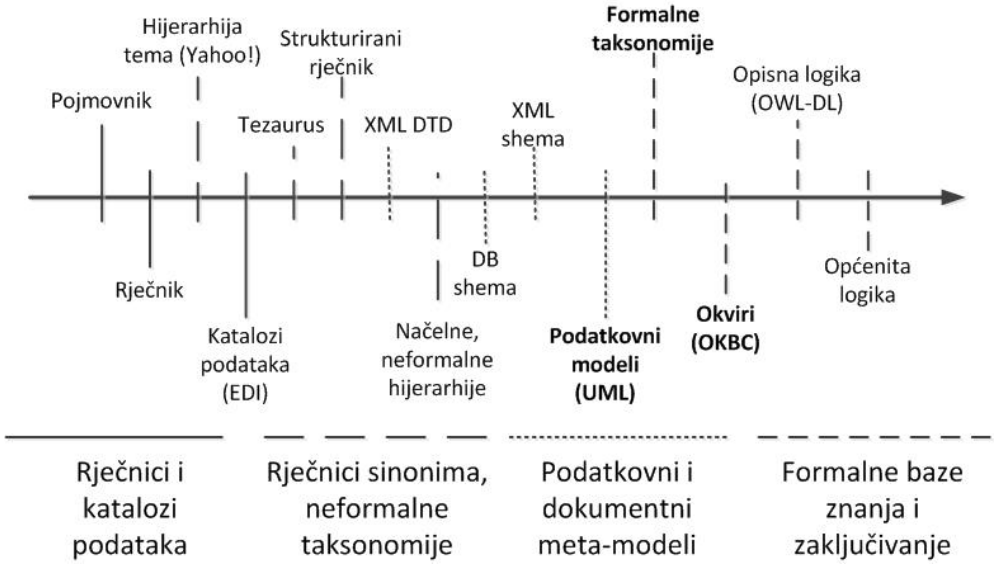

**Slika 2.2:** Primjer razrade kategorija i pojmova koji se koriste u domeni informacijske sigurnosti na primjeru nadzora informacijske sigurnosti

Strukturirani pojmovi u primjeru na slici 2.2 predstavljaju konceptualizirane pojmove iz dominantnih politika i normi, apstrahirane i generalizirane na razinu procedura i pojmova, prepoznatljivih u različitim sigurnosnim zahtjevima te se uz pomoć razrade domenske taksonomije mogu specijalizirati za posebne zahtjeve i primjene u različitim okruženjima u kojima se provodi politika informacijske sigurnosti. Tako dobivene instance klasa modela nasljeđuju opća obilježja klasa u svojoj hijerarhijskoj vertikali, a mogu se dodatno specijalizirati unosom podataka koji opisuju obilježja konkretnog organizacijskog okruženja. Ostvarenjem domenske taksonomije u procesu modeliranja politika informacijske sigurnosti, provodi se sistematizacija i integracija prethodno konceptualiziranih pojmova iz domene (slika 2.1).

## 2.3. Ontologija

Ontologija postoji od doba Aristotela kao filozofska disciplina koja proučava prirodu postojanja. Ontologija u računalnim znanostima koristi se u novije vrijeme te se i ovdje odnosi na sustav kategorija, ili referentni okvir, koji se tiče određenog pogleda na svijet. Ontologija označava „sustavski razlog postojanja“ te je neovisna o prirodnom jeziku, ali je ovisna o određenom filozofskom nazoru [15]. Svaka osoba posjeduje neke koncepte u svom mentalnom sklopu, neovisne od jezika kojim se izražava. Ova razlika obično se označava kao leksičko znanje (pojam koji se koristi prilikom referiranja na koncept) i neleksičko znanje (samo značenje koncepta) [9, 16].

Razvoj ontologija kao eksplicitnih, formalnih specifikacija pojmova u domeni i odnosa između njih [15], proširio se iz područja umjetne inteligencije u kojem je izvorno nastao, u čitav niz znanstvenih disciplina i strukovnih domena. Tradicionalne forme klasifikacija i pojmovnika nalikuju ontologijama tako što definiraju koncepte i međuodnose pojmova na sustavan način, ali su manje opisne u značenjima pojmova i manje formalne u specifikaciji tog značenja, osobito za potrebe različitih računalnih primjena. Na slici 2.3 prikazane su različite vrste ontologija, odnosno načina izražavanja znanja kakvi se danas mogu susresti u najrazličitijim primjenama [17]. Sličnost svih ovih pristupa prikazanih na slici 2.3 u tome je što koriste određeni način prikaza međusobno logički povezanih pojmova (sintaksa), a temeljna razlika između ovih pristupa je u načinu specificiranja značenja prikazanih logički povezanih pojmova (semantika). Prikazane vrste ontologija, odnosno načini izražavanja značenja pojmova, razvrstane su u četiri grupe prema srodnosti pristupa sintaksi i semantici opisa pojmova: rječnici i katalozi podataka; rječnici sinonima i neformalne taksonomije; podatkovni i dokumentni metamodeli; formalne baze znanja i zaključivanje. S lijeve strane prikaza na slici 2.3 nalaze se načini izražavanja značenja pojmova koji popise pojmova prikazuju s vrlo slabom specifikacijom značenja pojmova. S desne strane prikaza na slici 2.3 nalaze se logičke teorije s formalnim specifikacijama koje u sebi obuhvaćaju uvedenu definiciju ontologije. Gledajući s lijeva na desno primjere istaknute na slici 2.3, razina opisnosti značenja pojmova i stupanj formalnosti takve specifikacije rastu. Na taj način se smanjuje neodređenost i višeznačnost pojmova te se omogućava bolja podrška za automatizirano zaključivanje. Na slici 2.3, istaknuti su načini izražavanja značenja pojmova koji se primarno koriste u ovom radu: podatkovni modeli (UML), formalne taksonomije i okviri (OKBC), gdje pripada i programsko razvojno okruženje *Protégé Frames*.




**Slika 2.3:** Vrste ontologija, odnosno načini izražavanja značenja pojmova [17] (istaknuti načini primarno se koriste u ovom radu)

Ontologija osigurava zajednički rječnik za stručnjake i istraživače koji žele razmjenjivati informacije u nekoj domeni, a uključuje i računalno primjenjive definicije osnovnih koncepata u domeni i odnosa između njih. Mogući razlozi za razvoj određene ontologije, odnosno prednosti korištenja ontologija prema [18] su:

- razmjenjivanje uzajamnog razumijevanja i komuniciranje o određenoj strukturi informacija između ljudi ili računalnih sustava, odnosno programskih aplikacija;
- omogućavanje ponovnog korištenja domenskog znanja koje je netko uobličio u ontologiju kao i nadopunjavanje takvih ontologija daljnjim razvojem;
- stvaranje eksplicitnih domenskih pretpostavki koje mogu predstavljati bazu i temelj nekog budućeg programskog ostvarenja, jer su ontološki modeli lako primjenjivi i kada se znanje o domeni promijeni, a također vrlo pogodni za učenje znanja domene;
- razdvajanje domenskog i operativnog znanja, čime se lako postiže višestruka primjenjivost domenskog znanja za različite operativne probleme (npr. domena politika informacijske sigurnosti i modeli politika za konkretna organizacijska okruženja - opći pojmovi u klasama općeg ontološkog modela, a specifični u instancama klasa za konkretni model);
- analiziranje domenskog znanja koje opisuje ontologija u svrhu ponovnog korištenja, proširenja, uključenja u veće ontologije i sl.

Ontologija je eksplicitna, formalna specifikacija dijeljene konceptualizacije [15]. Eksplicitna specifikacija znači da su koncepti eksplicitno definirani, a nisu implicitno sadržani. Formalna specifikacija pretpostavlja da bi ontologija trebala biti programski čitljiva. Dijeljena specifikacija odražava ideju da ontologija obuhvaća znanje koje je prihvaćeno od interesne zajednice u određenom području na koje se ontologija odnosi. Konceptualizacija podrazumijeva apstraktni i pojednostavljeni model neke pojave, zasnovan na identificiranju svojstava ključnih za namjenu ontologije. Ontologija sadrži rječnik pojmova, definiciju pojmova koja pojašnjava pojmovima pridružene koncepte i daje domenski valjanu interpretaciju koncepata, zatim sadrži modeliranje domene od interesa s ciljem predstavljanja relacija između koncepata te odgovarajuće prihvaćene definicije pojmova i strukture domene za pretpostavljenu zajednicu korisnika.

Na temelju navedenih definicija i opisa proizlazi da ontologija u velikoj mjeri predstavlja nadgradnju prethodno opisanih pojmova konceptualizacije i domenske taksonomije. Odgovor na ključno istraživačko pitanje o jednostavnosti, dosljednosti, sveobuhvatnosti i učinkovitosti upravljanja životnim ciklusom politika informacijske sigurnosti uporabom konceptualnog metamodela domene, traži odgovarajuće, programski podržano, ostvarenje modela. U tom smislu, upravo programski podržani ontološki model predstavlja važan rezultat ovog istraživanja. Osnovna obilježja takvog ontološkog modela koja su bitna za ovaj rad su:

- namijenjen je ljudima i programskim aplikacijama u svrhu boljeg razumijevanja i komunikacije;
- koristi rječnik pojmova sa odgovarajućom specifikacijom i međusobnim relacijama;
- koristi zapis modela prilagođen čitljivosti i za programske aplikacije i za ljude.

Dakle, za razliku od osnovnih obilježja konceptualizacije, prikazanih u poglavlju 2.1, koja su bila primarno namijenjena ljudima i okrenuta odgovarajućem vizualnom zapisu, osnovna obilježja ontološkog modela postavljaju zahtjeve za programsku čitljivost, kao i za čitljivost, bolje razumijevanje i međusobnu komunikaciju ljudi. U okviru metode modeliranja predložene ovim radom, uloga ontoloških metoda prvenstveno je u detaljiziranju sadržaja modela, odnosno u razradi atributa i relacija koncepata (slika 2.1).

## 2.4. Sustavski pristup

Temelj razvoja teorije sustava zasnovan je na drevnoj Aristotelovoj spoznaji da je cjelina više od zbroja svih njenih dijelova. Na taj način su stari Grci prvi shvatili postojanje razumljivog reda u praktičnom svijetu, kojim se može upravljati uz pomoć logičkih aktivnosti. Ta ideja ostala je prihvaćena kao činjenica, kako za žive organizme, tako i za društvene grupe, a u novije vrijeme poopćena je i na različite složene sustave u kojima se interakcija događa među različitim vrstama živih i neživih elemenata.

Temelje opće teorije sustava [19] postavio je Von Bertalanffy početkom dvadesetog stoljeća, pojašnjavajući da je fundamentalno obilježje živih bića njihova organizacija te da analiza pojedinačnih elemenata i procesa ne može osigurati potpuno razumijevanje složenijih pojava. Razlog je u tome što takva analiza ne daje informacije o međusobnoj koordinaciji i utjecajima između pojedinih elemenata i procesa u sustavu. Upravo zbog toga glavno istraživačko usmjerenje u pristupu složenim sustavima mora biti otkrivanje zakona sustava i to na svim razinama organizacije u sustavu. Budući da sustav obilježava međusobna interakcija njegovih komponenata i formalne specifikacije sustava moraju se prvenstveno temeljiti na međusobnim odnosima elemenata i procesa, tj. na formi i uređenosti relacija koje ih povezuju. Analogija s modeliranjem politika informacijske sigurnosti može se lako postaviti, jer se i ovdje radi o složenom sustavu s heterogenim elementima i procesima, koji se nalaze u stalnoj međusobnoj interakciji. Ovu interakciju potrebno je opisati na svim razinama organizacije. Dakle, modeliranje treba obuhvatiti elemente sustava, procese koji se odvijaju unutar sustava ili u interakciji sustava i okoline, te međusobne interakcije elemenata i procesa na različitim organizacijskim razinama sustava. Na temelju ovog razmatranja, za područje modeliranja politika informacijske sigurnosti, može se reći da su prisutni svi bitni razlozi za korištenje sustavskog pristupa:

- duboka povezanost problematike sa okolinom i vanjskim svijetom, pri čemu problematiku nije moguće u potpunosti izolirati (npr. regulativni aspekti ili kibernetički prostor);
- složenost sustava koji je potrebno promatrati iz više aspekata, pazeći na međusobne utjecaje pojedinih elemenata i procesa (npr. fizička sigurnost, sigurnost informacijskih sustava ili sigurnost osoblja);
- multidisciplinarnost problematike koja usko povezuje heterogene čimbenike kao što su osobe, procesi, tehnologija i organizacija u okviru koje djeluju.

Sustav je skup od dva ili više povezanih elemenata koji imaju sljedeća svojstva [20]:

1. svaki element sustava sudjeluje u funkcioniranju cjeline sustava;
2. na svaki element sustava utječe barem jedan drugi element sustava;
3. svi mogući podsustavi imaju prva dva svojstva.

U ovom radu definicija sustava primjenjuje se na modeliranje politika informacijske sigurnosti, odnosno na širu domensku razinu dominantnih politika i normi informacijske sigurnosti, koje se promatraju kao složeni sustav. Model je pri tome, apstraktno, pojednostavljeno predstavljanje stvarnog sustava, u svrhu njegovog boljeg razumijevanja, daljnjeg proučavanja odnosno eksperimentiranja. Nadalje, metamodel je model koji služi za izgradnju drugih modela, što se u ovom radu koristi za modeliranje šire domene informacijske sigurnosti u kojoj mogu biti prisutne različite politike informacijske sigurnosti, koje su za ovaj proces modeliranja stvarni sustavi, te predstavljaju više ili manje izdvojeni dio stvarnoga svijeta koji čini funkcionalnu cjelinu.

Prema opisu iz poglavlja 2.1, metamodel predstavlja konceptualizaciju pogodnu za raspravu složenih heterogenih koncepata domene politike informacijske sigurnosti između različitih profila stručnjaka koji rade u tom području (vizualizacija, jasnoća, jednostavnost). Konceptualizacija, uz obilježja jasnoće i vizualizacije, daje i formalnu specifikaciju koja olakšava programski razvoj ontoloških modela opisanih u poglavlju 2.3. Ontološki model izgrađen prema specifikaciji metamodela služi za ispitivanje svojstava i mogućnosti primjene metamodela i istovremeno osigurava računalno čitljiv model s potporom za izradu konkretnih politika informacijske sigurnosti – instanci modela. Specifikacija ovog procesa modeliranja sastoji se od pojmova pridruženih formalno specificiranim domenskim konceptima, koji imaju jasno i jednoznačno definirano značenje u domeni informacijske sigurnosti. Na taj način formalna specifikacija temelji se na međusobnim odnosima elemenata i procesa, tj. na formi i uređenosti i pri tome mora obuhvatiti sve razine organizacije sustava.

Pojmovi u domeni strukturirani su odgovarajućom domenskom taksonomijom. Domenski koncepti na koje se pojmovi odnose formalno su specificirani i predstavljaju domensko znanje, konceptualizirano analizom informacija iz odabranih dominantnih politika i normi informacijske sigurnosti. U procesu stvaranja instanci modela za konkretna organizacijska okruženja u kojima se primjenjuje određena politika informacijske sigurnosti koriste se podatci u obliku dokumenata, evidencija i drugih zapisa. Na taj način se u procesu

modeliranja prati hijerarhija pojmova u kojoj znanje predstavlja organizirane informacije na domenskoj razini, informacije predstavljaju podatke u kontekstu pojedinih politika ili normi informacijske sigurnosti, a podatci su zapisi u obliku dokumenta ili nekom drugom obliku koji koriste konkretne politike koje se modeliraju. U ovu hijerarhiju pojmova: podatak – informacija – znanje, može se dodati i mudrost kao najviši pojam. Mudrost je viša razina razumijevanja o tome koje znanje se koristi s kojom namjerom, odnosno podrazumijeva dvije razine znanja, razinu poznavanja i razinu razumijevanja. Promatrajući stanje politike informacijske sigurnosti u okviru šireg domenskog prostora, može se uočiti da je stanje razvoja došlo do faze znanja u kojem je velik broj informacija uobličen u odgovarajuće proceduralne naputke za postupanje (organizirane informacije na domenskoj razini - znanje), no viša razina mudrosti u smislu poznavanja svih tih procedura i razumijevanja njihovog korištenja, gledano iz kuta različitih domenskih sigurnosnih zahtjeva, odnosno primjene znanja u širem i sveobuhvatnom domenskom smislu i prostoru djelovanja na različite organizacijske sustave i u različitim uvjetima, nalazi se početnoj fazi istraživanja. Upravo ova nepovezanost, odnosno slaba međusobna koordinaciju različitih stupova sigurnosnih zahtjeva, kako je to naglašeno u poglavlju 1.2, predstavlja motivaciju ovog istraživanja.

Ontologija kao formalna specifikacija predstavlja proces opisivanja sustava i njegovih svojstava. Formalna specifikacija izražava se jezikom čiji su rječnik, sintaksa i semantika formalno definirani. Poluformalne specifikacije usmjerene su primarno na sintaksu, dok neformalne specifikacije nastoje kvalitativnim pristupom, dobrim planiranjem i jasnoćom izražavanja postići zadovoljavajući stupanj razumijevanja i pouzdanosti. U području informacijske sigurnosti, norme i politike pisane su prirodnim jezikom u nestrukturiranom obliku dokumenata i predstavljaju neformalne specifikacije. Poluformalni pristup tipičan je samo za neke segmente politike informacijske sigurnosti, primjerice tehničke politike vezane za prava pristupa korisnika informacijskom sustavu. Upravo stoga, uvođenje formalizacije pristupa u šire područje politika informacijske sigurnosti predstavlja veliki istraživački izazov.

U okviru procesa modeliranja u ovom radu, uloga sustavskog pristupa prvenstveno je u osiguravanju željenih funkcionalnosti modela, odnosno u prilagodbi pojmova, koncepata te atributa i međusobnih relacija konceptualiziranih pojmova u domeni, potrebnom načinu koordinacije i međusobnog utjecaja elemenata i procesa prisutnih u stvarnom sustavu, što je vidljivo na slici 2.1.

# 3. PREGLED SRODNIH ISTRAŽIVANJA

U radovima [7, 21] analizirano je stanje razvoja u području informacijske sigurnosti, osobito s obzirom na trendove razvoja na široj domenskoj razini i na korišteni metodološki pristup. Prema [21], u aktualnim rješenjima za upravljanje informacijskom sigurnošću i dalje su primarno prisutna taktička i reaktivna obilježja informacijske sigurnosti, naročito vidljiva pri velikim sigurnosno povezanim krizama (npr. događanja iz 2001.g.: teroristički napad na SAD 9/11, s nizom posljedica kao što je primjerice kontinuitet poslovanja tvrtki, ili propast korporacije Enron povezana s problemima revizije i odgovornosti uprave tvrtke), što uzrokuje stanje u kojem su sigurnosne mjere u stalnom kašnjenju za izvorima prijetnji. Stoga je velik dio razvojnih napora u području upravljanja informacijskom sigurnošću usmjeren prema višedimenzijskom shvaćanju politike informacijske sigurnosti (međupovezanost područja i temeljnih čimbenika politika informacijske sigurnosti). Prvenstveni cilj ovog smjera istraživanja je uvođenje strateških i proaktivnih obilježja u politike i norme informacijske sigurnosti. Drugi važan smjer razvoja usmjeren je prema uključenju novih temeljnih čimbenika politika informacijske sigurnosti koji se u tradicionalnom pristupu informacijskoj sigurnosti nisu posebno analizirali, kao što je organizacijska kultura i struktura. Pored ovih smjerova, prisutni su i značajni istraživački napori vezani za pokušaj smanjivanja utjecaja subjektivnosti metoda upravljanja rizikom, primjerice istraživanjem sigurnosne metrike.

U ovom radu primarno se usmjerava na prva dva opisana smjera razvoja, nastojeći prijedlogom nove metode modeliranja politika informacijske sigurnosti omogućiti s jedne strane, sveobuhvatniji pristup politikama informacijske sigurnosti, a s druge strane, pristup koji će biti više strateški usmjeren i proaktivan u suvremenom sigurnosnom okruženju. Razlog takvom pristupu su suvremeni poslovni zahtjevi koje, kao što je u motivaciji ovog istraživanja u poglavlju 1.2 opisano, obilježava sve veća potreba povezanosti i međusobne poslovne suradnje organizacija iz različitih sektora društva. Sigurnosno okruženje, uslijed niza globalnih utjecaja, postaje sve promjenjivije i složenije. Gledajući s metodološke strane, najveći broj aktualnih istraživanja u području informacijske sigurnosti oslanja se na teoriju sustava i primjenu ontologije [7] te se neki važniji primjeri koji su utjecali na ovo istraživanje, posebno opisuju.

## 3.1. Sustavski pristup modeliranju u području informacijske sigurnosti

Komparativnim pregledom literature u [7] i prethodnim istraživanjem u [1] i [21], došlo se do više zaključaka o aktualnom razvoju područja politika i normi informacijske sigurnosti. Jedan od zaključaka je da se aktualna istraživanja u području politike informacijske sigurnosti velikim dijelom oslanjaju na teoriju sustava kao primjerice u [6, 22, 23, 24, 25].

Vrlo utjecajan primjer u novijem istraživanju je sustavski model upravljanja informacijskom sigurnošću prema [6], koji u pristupu upravljanju informacijskom sigurnošću uključuje dodatni temeljni čimbenik informacijske sigurnosti – organizaciju, odnosno njeno oblikovanje i strategiju. Ovo je proširenje u odnosu na tradicionalni pristup koji je zasnovan na osobama, procesima i tehnologiji, kao temeljnim čimbenicima politika informacijske sigurnosti. Pored toga, sustavski model upravljanja informacijskom sigurnošću, prikazan na slici 3.1, uključuje i dinamičke međuodnose između ova četiri temeljna čimbenika informacijske sigurnosti. Sustavski model upravljanja u osnovi predstavlja primjenu teorije sustava, odnosno sveobuhvatnog pristupa problematici informacijske sigurnosti na najvišoj organizacijskoj razini, s ciljem provođenja upravljanja informacijskom sigurnošću na osnovi ulaznih veličina proizašlih iz poslovnih ciljeva.


**Slika 3.1:** Sustavski model upravljanja informacijskom sigurnošću [6]

Najvažnija novina koju uvodi ovaj model jasno je izražavanje stanovišta da informacijsku sigurnost čine dinamički povezane i višedimenzijske aktivnosti, u odnosu na tradicionalno korištene skupove izdvojenih i nezavisnih sigurnosnih problematika (tzv. područja informacijske sigurnosti, kao što su sigurnost osoblja ili fizička sigurnost). Model se sastoji od spomenuta četiri glavna elementa (temeljni čimbenici informacijske sigurnosti), povezana međusobno sa šest dinamičkih poveznica (ljudski faktor, organizacijska kultura, nastajanje, usmjeravanje, arhitektura, omogućavanje i podrška). Ovakav model, vrlo općenitom razinom koncepata kojima je ostvaren, osigurava kontekst u koji se uklapaju postojeće norme kao što je CoBIT [26], ali i druge norme poput ISO/IEC 27001 [27], koje organizacije koriste u planiranju i ostvarenju svojih sigurnosnih programa i primjeni najboljih praksi. Na taj način stvara se s jedne strane, sustavni i sveobuhvatni, a s druge strane dinamički pristup, koji osigurava svojstvo proaktivnosti cjelokupnog sigurnosnog programa. Ovakav model ne zamjenjuje izvore najbolje prakse sigurnosnih programa, ali nudi pogled na aktivnosti informacijske sigurnosti u puno širem kontekstu. Taj kontekst omogućava integraciju različitih segmenata politika informacijske sigurnosti koji bi se inače koristili nepovezano, iako svojim međusobnim utjecajima i djelovanjima čine jedinstvenu organizacijsku cjelinu.

Primarna namjena sustavskog modela upravljanja informacijskom sigurnošću bila je otvaranje rasprave u stručnim i znanstvenim krugovima o potrebnim promjenama pristupa u ovom multidisciplinarnom području, razvoj svijesti o novim sigurnosnim potrebama i edukacija. Model je optimiziran za vizualnu prezentaciju ove problematike i prati ga nestrukturirani tekstualni opis elemenata modela te nije formalno specificiran za potrebe ostvarenja nekim programskim alatom. Ipak, zbog spomenute sveobuhvatnosti modela u koju se lako uklapaju neke druge norme, kao što je spomenuta norma CoBIT [26], globalna strukovna udruga revizora informacijske sigurnosti ISACA (engl. *Information Systems Audit and Control Association - ISACA*), odlučila je kupiti prava na daljnji razvoj ovog modela te ga je nastavila razvijati pod imenom poslovni model informacijske sigurnosti (engl. *The Business Model for Information Security – BMIS*) [24]. Cilj daljnjeg razvoja ISACA-e bio je prilagoditi model za poslovne namjene i ostvarenje različitih normi potrebnih u poslovanju, prvenstveno za upravljanje informacijskom tehnologijom. ISACA je u daljnjem razvoju BMIS modela nadograđivala osnovni model iz [6] na način koji omogućava mapiranje određenog koncepta iz željene norme (sigurnosni zahtjev, kontrola), na elemente i dinamičke poveznice BMIS modela, koristeći pri tome ontološke metode ostvaranjem koncepata i relacija koje ih

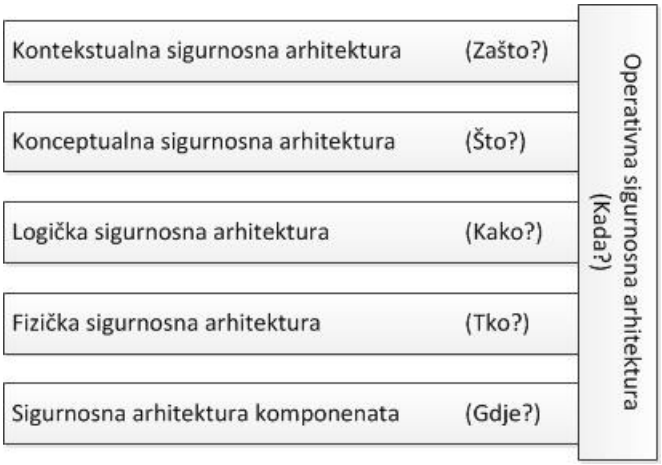
povezuju s vršnim konceptima temeljnog modela, usmjeravajući se primarno na problematiku upravljanja informacijskom tehnologijom u okruženju poslovnog sektora.

Metoda modeliranja politika informacijske sigurnosti predložena u ovom radu, ima sličan pristup u tome što se usmjerava na širi domenski pogled na područje informacijske sigurnosti. Za razliku od sustavskog modela informacijske sigurnosti u [6], namijenjenog primarno za znanstveno-stručnu raspravu i razvoj sigurnosne svijesti te stoga neformalno specificiranog, u ovom radu ciljevi modeliranja usmjereni su puno dublje i detaljnije te se na bazi šire domenske taksonomije ostvaruje detaljno razrađen i formalno specificiran višerazinski model politika informacijske sigurnosti, primjenjiv za široki spektar organizacijskih okruženja. U odnosu na BMIS pristup, čiji je osnovni model za praktičnu primjenu puno općenitiji te traži znatno veći napor u modeliranju konkretnih organizacijskih okruženja, modelske instance metamodela predloženog u ovom radu, relativno jednostavnim konfiguriranjem konkretnih podataka o određenoj organizaciji mogu predstavljati detaljan model politike informacijske sigurnosti ciljane organizacije.

SABSA model (engl. *Sherwood Applied Bussiness Security Architecture* - *SABSA*) prema [23], je model koji se fokusira na zaštitu definiranih poslovnih vrijednosti – atributa, koje dijeli u sedam područja (korisnički, upravljački, operativni, upravljanje rizikom, pravno-regulativni, tehnička strategija, poslovna strategija) s ukupno 85 identificiranih atributa. Na taj način se poslovni rizici promatraju kao prijetnje definiranim atributima koji zahtijevaju zaštitu. Taksonomija atributa izvedena je iz poslovnih pokretača koji predstavljaju općenite poslovne potrebe neke poslovne organizacije. Poslovni pokretači u konkretnoj primjeni mogu se pridruživati jednom ili više definiranih atributa. Odabrani atributi su željena obilježja poslovnih vrijednosti kojima je potrebno upravljati i u tu svrhu ih odgovarajuće mjeriti. Ovako se modelom istovremeno provodi usmjeravanje poslovnih ciljeva i upravljanje sigurnosnim programom jer definirani atributi obuhvaćaju šire područje od sigurnosnih zahtjeva (poslovna strategija, tehnička strategija i sl.). Jednako kao i prethodno spomenuti modeli, SABSA model je sveobuhvatan na razini poslovnog organizacijskog sustava i u primjeni može uspješno koristiti postojeće norme za područje upravljanja informacijskom sigurnošću ili informacijskom tehnologijom.

Pored teorije sustava na koju se oslanja, SABSA model koristi i slojeve sigurnosne arhitekture prema slici 3.2, koji osiguravaju kompletnost sigurnosnih zahtjeva, ali i poslovno opravdanje

planiranja različitih sigurnosnih elemenata. Na taj način objedinjavaju i puno širu funkcionalnost upravljanja sigurnosnim projektom na najvišoj razini cjelokupne poslovne organizacije.




**Slika 3.2:** SABSA model slojeva sigurnosne arhitekture [23]

SABSA model sigurnosne procese usko povezuje s poslovnim procesima, jer mu je i namjena ostvarenje sigurnosne arhitekture poduzeća [23]. Time se iskoristivost sigurnosnog modela sužava na uski poslovni profil potencijalnih organizacija – korisnika modela. Nasuprot tome, predloženi model u ovom radu, usmjeren je na modeliranje šire domenske razine informacijske sigurnosti, ne limitirajući se pri tome na profil organizacije koja ga koristi, već naprotiv, nastojeći omogućiti što šire korištenje istog modela i pokazati prednosti takvog pristupa modeliranju politika informacijske sigurnosti. U segmentu razrade funkcionalnosti modela, u ovom radu koristimo model slojeva sigurnosne arhitekture prema slici 3.2 u svrhu provjere kompletnosti sigurnosnih funkcionalnosti pri razvoju modela.

Sustavski pristup koristi se u području informacijske sigurnosti već niz godina, primjerice preko uspostave sustava upravljanja informacijskom sigurnošću u normi ISO/IEC 27001. Najvažniji rezultat istraživanja u području sustavskog pristupa u novije vrijeme svakako je svijest o unutarnjoj povezanosti temeljnih čimbenika i područja informacijske sigurnosti. Takvo, višedimenzionalno shvaćanje informacijske sigurnosti znači da se, primjerice, sigurnost osoblja promatra u kontekstu procesa u kojima osobe sudjeluju, ali i u kontekstu tehnologije, fizičkog prostora, ili podataka koje osobe koriste.

## 3.2. Primjena ontologije u području informacijske sigurnosti

Komparativnim pregledom literature u [7] i prethodnim istraživanjem u [1] i [21], došlo se i do zaključaka o primjeni ontologije u istraživanju mogućnosti modeliranja politika informacijske sigurnosti. Primjena ontologije može se smatrati jednim od najvažnijih i najproduktivnijih pravaca istraživanja u ovom području. Najveći broj istraživačkih radova pri tome je usmjeren na tehničke, uskonamjenske sigurnosne politike, najčešće u području kontrole pristupa, prijetnji ili ranjivosti informacijskih sustava [7]. Rad u [28] primjerice predlaže uvođenje ontologije u problematiku upravljanja ranjivošću, a s ciljem doprinosa automatizaciji programa informacijske sigurnosti te korištenja postojećih repozitorija podataka o ranjivostima. Rad u [29] bavi se problematikom usmjeravanja prometa na okosnici velikih računalnih mreža, pri čemu se razvija sigurnosni okvir u kojem se značenje određene mrežne komunikacije pojedinih mrežnih entiteta koristi u izboru i primjeni odgovarajuće politike informacijske sigurnosti, koja se automatski konfigurira na mrežnim elementima. Rad u [30] usmjeren je na područje kibernetičke forenzike i sustavnim pristupom nastoji povezati problematiku ranjivosti i prijetnji, kao i specifičnosti različitih sektora društva s obzirom na kibernetičku sigurnost. Razrađuje se taksonomija pojedinih pojmova i predlaže ontološki model za područje kibernetičke forenzike. Nadalje, rad u [31] analizira i predlaže arhitekturu sustava upravljanja sigurnošću informacijskih sustava zasnovanu na ontologiji. Kao i u većini drugih radova usmjerenih na sigurnosnu ontologiju i ovdje se ukazuje na važnost korištenja postojeće najbolje prakse i nužnost njenog nadopunjavanja prednostima koje daje formalizirani pristup i konceptualizacija znanja, kako u svrhu ponovnog korištenja, tako i u svrhu interoperabilnosti informacijskih sustava. U tom smislu, primjena ontologije predstavlja okvir za prikupljanje i upravljanje znanjem o sigurnosti. Razvijena ontologija usmjerena je na procjenu rizika te je pokazana mogućnost ekstrakcije sigurnosnih informacija iz odredbi politike informacijske sigurnosti visoke razine, s ciljem primjene usklađenih protumjera zasnovanih na procjeni rizika informacijskog sustava. Ontologija se u svim ovim radovima promatra prema definiciji danoj u poglavlju 2.3., kao eksplicitna specifikacija konceptualizacije i predstavlja znanje u formalnom i strukturiranom obliku prema [15].

Usporednom analizom raspoloživih prijedloga sigurnosnih ontologija u literaturi [32] može se zaključiti da je najveći dio predloženih sigurnosnih ontologija fokusiran na usko definirano područje sigurnosti, a sveobuhvatna primjena ontologije u području informacijske sigurnosti očekuje se kao smjer budućeg razvoja. Jedan od zaključaka rada u [32] jest da zbog

složenosti, područje sigurnosti nije moguće formalizirati jedinstvenim konceptom te stoga definicija kompletne sigurnosne ontologije nije jedinstveni problem već predstavlja nužnost povezivanja čitavog niza novih koncepata koji se razrađuju u istraživačkoj zajednici. Također se zaključuje da je najveći broj radova u području sigurnosne ontologije u ranoj fazi razvoja i da u predloženim ontologijama nedostaje formalnih svojstava za zaključivanje, odnosno da u ovoj fazi razvoja nisu dovoljno dobro dorađene za ponovno korištenje i proširenje, te za nužan konačni cilj razdiobe znanja. Nedostatak ontologija koje obuhvaćaju cjelokupnu domenu informacijske sigurnosti uočen je i u [33], gdje se ukazuje na to da su prepoznata samo dva istraživačka projekta sa širom vizijom pristupa [34, 35].

Istraživanje opisano u [34] predlaže ontologiju zasnovanu na analizi rizika i detaljnoj razradi odabranih vršnih koncepata: imovine, prijetnji, ranjivosti i kontrola. Povezivanjem ovih općih koncepata s njihovim međusobnim relacijama ostvarena je jezgra ontologije koja predstavlja prikaz domene informacijske sigurnosti na kontekstno nezavisan i aplikacijski neutralan način. S ciljem praktične iskoristivosti, jezgra ontologije popunjena je domenski specifičnim tehničkim rječnikom koji se povezuje s ključnim konceptima i relacijama. Dobiveni rezultati ovako formirane ontologije u [34], ograničeni su malim brojem vršnih koncepata ontologije, koji opisuju izvršni dio politika informacijske sigurnosti, primarno povezan s lokalnim okruženjem modeliranog organizacijskog entiteta. Za razliku od ovog pristupa, u metodi modeliranja predloženoj u ovom radu, ne ograničava se broj vršnih koncepata. Broj vršnih koncepata tako se prilagođava potrebi željene razine opisa globalnog i lokalnog okruženja, nužnog za postizanje sveobuhvatnosti opisa politika informacijske sigurnosti u prethodno određenim okvirima domenske definicije (pojednostavljenje u okvire dominantnih politika i normi informacijske sigurnosti). Pri tome se postavljaju slični ciljevi kao u radu [34], vezano za kontekstno nezavisan i aplikacijski neutralan pristup.

Modeliranje šireg dijela domene informacijske sigurnosti u odnosu na [34], obilježje je rada u [35], koji se pri tome zasniva na konceptualizaciji nekih postojećih normi informacijske sigurnosti (npr. *ISO/IEC 27001, Common Criteria, IT Grundschutz, NIST CS Handbook, EBIOS*). U ovom istraživanju kombinira se korištenje postojećih najboljih praksa i normi informacijske sigurnosti s ontološkim metodama. Postavljeni su ciljevi razvijanja unificiranih i formalnih modela znanja, zasnovani na konceptualizaciji odabranih normi informacijske sigurnosti i postavljeni u okvire šireg istraživačkog projekta usmjerenog na područje upravljanja sigurnosnim rizicima [36]. Proces mapiranja znanja iz odabranih normi usmjeren

je na eksplicitno znanje izraženo i uobličeno specifikacijama normi (sigurnosni zahtjevi i kontrole), koje se konceptualizira i ontološki modelira. Pri tome se u radu koristi sljedeća kategorizacija znanja koje, prema već uvedenoj definiciji iz poglavlja 2.4, predstavlja organizirane informacije na domenskoj razini:

1. deklarativna vrsta znanja (engl. *Know-about Knowledge*) - znanje o nečemu, što se predstavlja ontološkim modelom koncepata;
2. proceduralna vrsta znanja (engl. *Know-how Knowledge*) - znanje kako nešto napraviti, a osigurava se uz pomoć opisa prirodnim jezikom pohranjenih uz pripadajuće ontološke koncepte;
3. relacijska vrsta znanja (engl. *Know-with Knowledge*) - povezivanje deklarativnog tipa znanja, koje se predstavlja relacijama između ontološki modeliranih koncepata.

Prednost pristupa iz [35] je što znanje koje je izraženo određenom normom (neformalni oblik specifikacije nestrukturiranim tekstualnim dokumentom) postupkom ontološkog modeliranja dobiva pogodniji oblik programski čitljive i formalne specifikacije zapisa koji je moguće na različite načine dalje koristiti i obrađivati. Ograničenje pristupa je u tome što nema novog i dodatnog znanja ili povezivanja znanja iz konceptualiziranih normi s nekim drugim širim konceptima te se, konceptualizirajući samo znanje eksplicitno izraženo normama, ostaje u okvirima znanja formuliranog i izraženog takvom normom. Na taj način nije moguće doći do općenitijeg rješenja za modeliranje šire domenske razine. Ovaj problem je prepoznat u radu te se kao cilj daljnjeg istraživanja postavlja usmjeravanje na uključivanje implicitno sadržanog znanja u široj domeni koje je puno teže izraziti i formalizirati od eksplicitnog znanja, izraženog zahtjevima i opisanog dokumentima pojedinih normi.

U procesu modeliranja predloženom u ovom radu, šira domenska razina informacijske sigurnosti konceptualizira se pristupom preko implicitno sadržanog domenskog znanja, a ne samo preko eksplicitno izraženog znanja u dominantnim politikama i normama informacijske sigurnosti. Prema poglavlju 2.4, u kojem je pojašnjena hijerarhija pojmova (podatak – informacija – znanje – mudrost), implicitno izraženim znanjem domene informacijske sigurnosti smatra se viša razina koncepata kojima se definira „znanje o znanju“, odnosno najviši pojam ove hijerarhije – mudrost. To znači da, sukladno definiciji pojma mudrosti, model u ovom radu razrađuje i koncepte poznavanja eksplicitnog znanja (zahtjevi dominantnih normi i politika informacijske sigurnosti), ali i koncepte razumijevanja implicitnog znanja (međusobne sličnosti koncepata različitih normi i politika, njihovih

zahtjeva te načina i potreba njihove primjene na široj domenskoj razini). Na modelskoj razini, to znači međusobnu povezanost konceptualiziranih pojmova iz dominantnih politika i normi, kao i njihovu povezanost s višim i općenitijim konceptima šireg domenskog područja kojima mogu pripadati, što je ilustrirano i slikom 2.2 u poglavlju 2.2. o domenskoj taksonomiji. Koncept deklarativne, proceduralne i relacijske vrste znanja u odnosu na domenu informacijske sigurnosti, primjenjuje se u ovom radu na sličan način kao i u [35].

Ciljevi primjene ontologije u području modeliranja informacijske sigurnosti su bolje komuniciranje o sigurnosnim problemima, sustavno organiziranje i ponovno korištenje znanja, kao i ostvarivanje određenog napretka u zaključivanju o sigurnosnim problemima [7]. Razvoj metoda za potporu procesa planiranja, ostvarenja, provođenja i preispitivanja politike informacijske sigurnosti, najvećim dijelom oslanja se na teoriju sustava. Uskonamjenski segmenti politika informacijske sigurnosti, kao što je primjerice kontrola pristupa informacijskom sustavu ili problematika ranjivosti sustava, i dalje prevladavaju u istraživanjima, ali zahtjevi za razvoj novih pristupa, metoda i alata u području organizacije i upravljanja, a osobito u okviru sveobuhvatnog pristupa politici informacijske sigurnosti i primjeni ontologije, dobivaju sve više na značaju. Razvoj u ovom području sveobuhvatnog pristupa politici informacijske sigurnosti još je uvijek u ranoj fazi istraživanja i uglavnom se odvija u znanstveno-istraživačkoj zajednici. Aplikacije u praktičnoj primjeni tek se očekuju, jednako kao i više koordiniranih napora u svrhu suradnje između istraživača u znanstveno-istraživačkom sektoru i stručnjaka iz državnih i privatnih institucija na problematici od zajedničkog interesa.

# 4. ANALIZA POLITIKA I NORMI INFORMACIJSKE SIGURNOSTI

Opisom područja istraživanja u poglavlju 1.1., naglašeno je kako politika informacijske sigurnosti kao područje istraživanja obuhvaća vrlo široko i multidisciplinarno područje. Kako bi se moglo sistematizirati i integrirati obilježja suvremenog stanja ovog područja koje predstavlja domenu istraživanja rada, ali i domenu u kojoj se provodi konceptualizacija, potrebno je pravilno razlučiti i povezati niz pojmova te na odgovarajući način specificirati njihovo značenje u širem domenskom kontekstu. Značenje pojedinih pojmova ovisi o kontekstu njihovog korištenja koje je u području informacijske sigurnosti iznimno raznoliko, kako s obzirom na vrste organizacija koje provode sigurnosne mjere, njihovu pripadnost državnom ili poslovnom sektoru, odnosno pojedinom usko specijaliziranom sektoru gospodarstva, tako i s obzirom na moguće poslovne aktivnosti u nacionalnom ili međunarodnom okruženju, ali i na sva druga ograničenja koja iz prethodnog konteksta proizlaze (primjerice, složenost regulativnih zahtjeva, različitost potreba korištenja komunikacijske i informacijske tehnologije, odnosno razina složenosti poslovnih procesa neke organizacije). Upravo ova složenost i multidisciplinarnost domene otežava njezinu konceptualizaciju koja se u dosadašnjim istraživanjima, prikazanim u poglavlju 3., uglavnom temeljila na pristupu pojedinim uskonamjenskim domenskim segmentima, ili na konceptualizaciji pojedinih normi iz područja informacijske sigurnosti. Stoga se, u cilju sistematizacije i integracije šire domene, u ovom poglavlju provodi analiza najvažnijih općih pojmova, analiza najvažnijih koncepata informacijske sigurnosti, kao i konteksta njihove primjene tijekom formativnog razdoblja politika informacijske sigurnosti, te se analiziraju i ključna obilježja koncepata informacijske sigurnosti koji se primjenjuju u dva najvažnija sektora primjene, državnom i poslovnom sektoru. Nadalje, daje se prikaz najvažnijih koncepata vezanih za regulativni okvir informacijske sigurnosti, odnosno pregled izravno i neizravno povezane regulative s područjem informacijske sigurnosti. Na temelju navedenog opisa provodi se i dodatna analiza dominantnih normi i politika informacijske sigurnosti, odnosno njihovih ključnih koncepata, kao i sličnosti između tih koncepata.

Pojam „politika“ u ovom radu koristi se u smislu značenja koje ima engleski pojam *„Policy“*. Prema [37], pojam *„Policy“* u engleskom jeziku označava skup ideja ili plan aktivnosti u određenoj situaciji, koji je prethodno usuglašen od grupe ljudi, poslovne organizacije, vlade

neke države ili neke političke stranke. U hrvatskom jeziku, ovaj isti pojam „politika“ koristi se i kao hrvatski prijevod za drugi engleski pojam *„Politics“*, koji prema [37] označava aktivnosti vlade neke države, članova zakonodavnih tijela ili drugih osoba koje utječu na način upravljanja državom. Prema [38] pojam „politika“ u hrvatskom jeziku označava:

1. djelatnost koja teži uređenju društva u najširem smislu, uređenju nekih dijelova, institucija ili projekata društva i odnosa među njima;
2. umijeće i način vladanja državom, gradom, kompanijom, institucijom;
3. opće usmjerenje, planiranje i način upravljanja djelatnošću nekog posebnog područja društvenog, državnog, privrednog, kulturnog itd. života;

te ima još neka značenja koja nisu od interesa za ovo razmatranje. Prethodno pojašnjeno značenje engleskog pojma *„Policy“*, najbliže je značenju hrvatskog pojma „politika“ navedenom pod brojem 3.: opće usmjerenje, planiranje i način upravljanja djelatnošću nekog posebnog područja društvenog, državnog, privrednog, kulturnog itd. života.

Postoji veliki broj definicija pojma „informacijska sigurnost“. Prema normi ISO/IEC 27001 [27], informacijska sigurnost je očuvanje povjerljivosti, cjelovitosti i raspoloživosti podataka, a dodatno mogu biti uključena i druga svojstva, kao što su autentičnost, odgovornost, neporecivost i pouzdanost. Prema Zakonu o informacijskoj sigurnosti [39], informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera zaštite te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade tih mjera. Sve češće se u praksi koristi i pojam osiguravanje informacija (engl. *Information Assurance*), često kao zamjena za pojam informacijska sigurnost, prvenstveno zbog preširokog i neodređenog značenja pojma sigurnost. Osiguravanje informacija u tom je smislu međudjelovanje između tehnologije koja osigurava uvjete sigurnosti, procesa koji osnažuju djelovanje tehnologije i ljudi koji omogućavaju rad tehnologije u operativnoj uporabi [40].

Općenito, pojam sigurnosti predstavlja dihotomiju, tj. temelji se na dva oprečna stanja (sigurno je / nije sigurno), koja su rezultat osobne percepcije i predstavljaju subjektivni osjećaj ili doživljaj sigurnosti. Upravo ova psihološka komponenta doživljavanja sigurnosti, čest je cilj i pozitivnih pristupa (npr. programi pripravnosti za neka sigurnosna događanja), ali i negativnih pristupa (npr. marketinško iskorištavanje potencijalnih kupaca zastrašivanjem katastrofičnim mogućnostima). Za razliku od pojma sigurnosti koji ima samo dva oprečna stanja, pojam povjerenja (engl. *Trust*), već se intuitivno doživljava u više kvalitativnih razina.

S obzirom da je povjerenje zasnovano na iskustvu, ovakav pristup je usko povezan s procjenjivanjem rizika, koje se i u našem svakodnevnom životu dijelom provodi intuitivno, a dijelom svjesno. Kao što se i u svakodnevnom životu povjerenje stječe ili gubi određenim životnim iskustvom, slična situacija je i u politikama informacijske sigurnosti, gdje se preko različitih oblika nadzora, certifikacije, akreditacije ili ugovornih obaveza, na određeni način utvrđuju i provjeravaju sigurnosni zahtjevi koji trebaju biti provedeni, te se na taj način osigurava tražena ili propisana razina povjerenja.

Pojam sigurnosti (engl. *Security*) tradicionalno u politikama informacijske sigurnosti označava aktivnosti ili osobe koje nekome pružaju zaštitu od moguće štete ili pokušavaju spriječiti neku kriminalnu radnju. Primjerice uz pojam sigurnosti vezuje se čuvar, odnosno zaštitar (engl. *Security Guard*) ili sigurnost zračne luke (engl. *Airport Security*). Usko povezan s pojmom sigurnosti je i pojam zaštite (engl. *Safety*), koji označava stanje sigurnosti ili opremu koja nekoga čini zaštićenim, primjerice sigurnosni pojas (engl. *Safety Belt*) ili sigurnost na cestama (engl. *Road Safety*). Kao što je vidljivo iz prikazanih primjera na hrvatskom i engleskom jeziku, u hrvatskom jeziku ne postoji potpuna dosljednost u primjeni pojmova sigurnost i zaštita u odnosu na engleski jezik, ali su pojmovi uglavnom jasni u smislu njihovog značenja. Ako se promatra ove pojmove iz kuta primjene politika informacijske sigurnosti, može se uočiti još jednu povezanost ova dva pojma, odnosno mogućnost da pojedine zaštitne mjere ostvarene u nekom organizacijskom okruženju, mogu biti provedene u okviru procesa zaštite na radu, a da pri tom istovremeno služe i kao sigurnosna kontrola u kontekstu politike informacijske sigurnosti (npr. vatrodojava).

Sljedeći, usko povezani pojam s kontekstom politika informacijske sigurnosti je „sustav upravljanja informacijskom sigurnošću“ (engl. *Information Security Management System – ISMS*), kao dio sveukupnog sustava upravljanja nekom organizacijom, zasnovan na pristupu upravljanju rizicima s ciljem uspostavljanja, provođenja, praćenja, revidiranja, održavanja i unaprjeđivanja informacijske sigurnosti [27, 41]. Međunarodna udruga za normizaciju (engl. *International Standardization Organization - ISO*) u zahtjevima normi, utvrđuje obvezu korištenje procesa planiranja, provedbe, provjere i dorade (engl. *Plan, Do, Check, Act – PDCA*), što je slučaj i pri uspostavi i korištenju ISMS-a. Često se koristi i pojam „sigurnosni program“, koji se uspostavlja u svrhu provođenja politike informacijske sigurnosti te, jednako kao i ISMS, uključuje planiranje, provedbu, provjeru i doradu, odnosno trajno upravljanje temeljnim čimbenicima informacijske sigurnosti (osobe, procesi i tehnologija), koji utječu na

aspekte sigurnosti u okviru cijele organizacije [23]. Postoje različiti izvori sigurnosnih normi koje se mogu koristiti pri razvoju sigurnosnih programa, odnosno ISMS-a pojedine organizacije [27, 42]. Sukladno vrlo sličnim definicijama, pojmovi kao što su sigurnosni program i ISMS u praksi, na široj domenskoj razini, mogu se promatrati kao različitost rječnika pojedinih normi, odnosno iz kuta gledanja domenske taksonomije kao različita sintaksa sadržajno srodnih koncepata.

## 4.1. Značenje pojma „politika informacijske sigurnosti“

Pojam „politika informacijske sigurnosti“, koristi se u ovom radu kao hrvatski zamjenski pojam za engleski pojam „*Security Policy“*, koji se može naći u većini literature, regulative i normi u engleskom govornom području. U hrvatskom jeziku izravno prevedeni pojam „sigurnosna politika“, ima  šire značenje koje je vezano za područje nacionalne sigurnosti. Tako su prema [43], sigurnosne politike u širem značenju definirane kao djelatnosti za pripremu osiguravanja od izvora budućih prijetnji u prirodi, društvu i među društvima, dok u užem značenju one predstavljaju zbroj svih mjera, djelatnosti i postupaka namijenjenih uspostavljanju i djelovanju sustava nacionalne sigurnosti.

U tom smislu, prema [3], politika informacijske sigurnosti predstavlja dokumente kojima se utvrđuju mjere informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka te raspoloživosti i cjelovitosti informacijskih sustava u kojima se ti podatci obrađuju, pohranjuju ili prenose. U užem smislu, dokument politike informacijske sigurnosti predstavlja izjavu ili očitovanje najodgovornijih osoba (uprava tvrtke ili čelnik državnog tijela) o uvjerenjima, ciljevima i razlozima te općenitim načinima kako doći do željenih postignuća u području informacijske sigurnosti i to u obliku kratkog i konciznog dokumenta na općenitoj razini, bez specifičnosti i detaljnih opisa (vršni dokument). U širem smislu, dokumenti politike informacijske sigurnosti predstavljaju hijerarhijski strukturiran skup propisa (slika 4.1) koji se, pored opisanog vršnog dokumenta, uobičajeno sastoji i od razine normi (obvezujući zahtjevi), razine procedura (obvezujući postupci) te od razine smjernica ili naputaka (preporučeni načini ostvarivanja normi i procedura) [3, 44].


**Slika 4.1:** Hijerarhijske razine u skupu dokumenata politike informacijske sigurnosti

Iako postoji više definicija pojma „informacijska sigurnost“, odnosno pojma „politika informacijske sigurnosti“, prisutna je velika sličnost među tim definicijama. Sličnost je u korištenju elemenata kao što su:

1. željeno stanje - povezuje se s temeljnim kriterijima informacijske sigurnosti (povjerljivost, cjelovitost i raspoloživost);
2. štićene vrijednosti - predstavljaju podatke i drugu važnu materijalnu i nematerijalnu imovinu;
3. sigurnosne mjere ili kontrole - primjenjuju se za zaštitu štićenih vrijednosti, odnosno kao protumjere procijenjenih rizika.

Slijedom ovog razmatranja, politiku informacijske sigurnosti definiramo kao skup procedura kojima se planira, ostvaruje, provodi i preispituje informacijska sigurnost u određenom opsegu primjene.

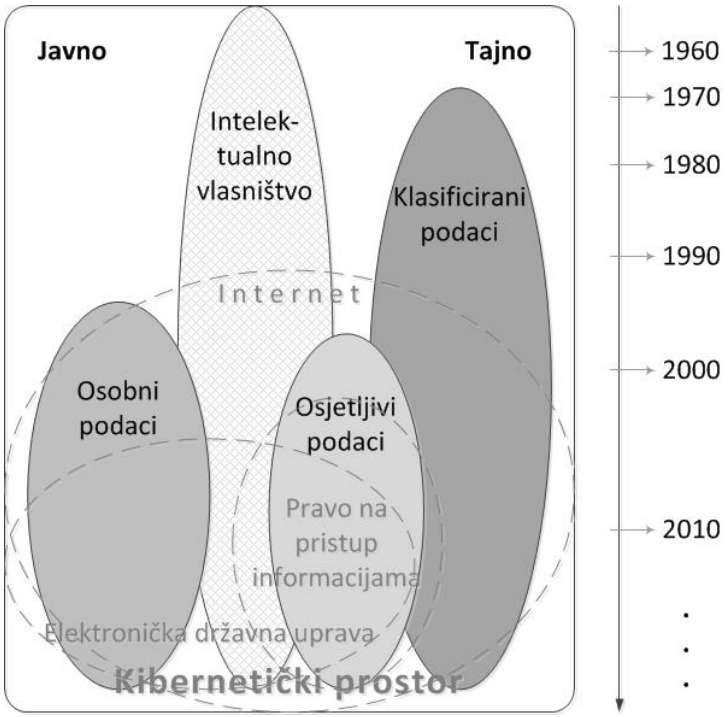
## 4.2. Razvoj politike informacijske sigurnosti

Razvoj politike informacijske sigurnosti usko je povezan s razvojem informacijskog prostora. Informacijski prostor predstavlja virtualnu globalnu okolinu međusobno povezanih javnih i privatnih informacijskih sustava, u kojoj nastaju i prenose se različite vrste podataka, ali i specifični podatci koji su dominantni s obzirom na propise i zahtjeve informacijske sigurnosti [3]. Slijedom toga potrebno je primijeniti odgovarajuće mjere informacijske sigurnosti propisane za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i

cjelovitosti informacijskih sustava u kojima se ti podatci obrađuju, pohranjuju ili prenose. Ova definicija usko je povezana sa sve više korištenim pojmom kibernetičkog prostora. Kibernetički prostor, kibernetička sigurnost, kibernetički terorizam, izvedenice su nastale u engleskom jeziku iz prefiksa *„cyber-“*, kojim se tvori riječ *„cybernetics“*, odnosno kibernetika [5]. Kibernetika je znanost o sustavima automatskog upravljanja te općenito procesima upravljanja u biološkim, tehničkim, ekonomskim i drugim sustavima. U području informacijskih sustava iz ovog prefiksa proizlazi i termin kibernetički prostor [45]. Pojam kibernetičkog prostora odgovara prethodnoj definiciji informacijskog prostora, te se može reći da kibernetički prostor označava suvremeno stanje informacijskog prostora prema slici 4.2 [2], koje uključuje široko korištenje informacijskih i komunikacijskih sustava, kao i povezivanje različitih informacijskih sustava i pohranjenih podataka u elektroničkom obliku preko Interneta.

Pojam informacijski prostor, prema slici 4.2 koristi se za daljnju analizu u puno širem značenju od suvremenog kibernetičkog prostora, odnosno proširuje se na sve načine komuniciranja i zapisa informacija koji su se koristili tijekom formativnog razdoblja politika informacijske sigurnosti. Na taj način se pokazuje kako ova uska povezanost politika informacijske sigurnosti i informacijskog prostora nije samo rezultat tehnološkog razvoja, već i rezultat čitavog niza društvenih procesa koji su se događali tijekom ovog formativnog razdoblja, ali i društvenih procesa kakvi se nastavljaju i danas uz svekoliku tehnološku potporu.

Suvremeni informacijski prostor prema slici 4.2 oblikovao se tijekom posljednjih pedesetak godina [2]. U tom razdoblju čitav niz različitih trendova utjecao je na formiranje suvremenog stanja informacijskog društva i pripadajućeg informacijskog prostora. Važnost razvoja informacijskog prostora je u tome što koncepti politika informacijske sigurnosti i njihov razvoj kroz povijest, u velikoj mjeri prate razvoj informacijskog prostora. Isto se može reći i za suvremene potrebe u području politika informacijske sigurnosti i suvremeni kibernetički prostor. Stoga će se razvoj zahtjeva i koncepata politika informacijske sigurnosti, koji je u najvećoj mjeri nastao u spomenutom vremenskom razdoblju od posljednjih pedesetak godina, promatrati paralelno s promjenama koje su se u tom razdoblju događale u informacijskom prostoru i koje su vremenom postajale sve veće i učestalije, što je i vidljivo sa simbolički prikazane vremenske skale na desnoj strani slike 4.2.




**Slika 4.2:** Stvaranje suvremenog informacijskog prostora

### 4.2.1. Informacijski prostor i domene podataka

Analizom razdoblja od posljednjih pedesetak godina mogu se utvrditi neke tipične faze kroz koje je oblikovanje informacijskog prostora prolazilo, kao što je prikazano na slici 4.2. U razdoblju do sedamdesetih godina prošlog stoljeća, informacijski prostor obilježavala je izrazita segmentacija na informacijske prostore pojedinih država, kao i vrlo oštra granica između javnog i tajnog informacijskog prostora [2, 3]. Ova oštra granica u to je vrijeme bila dodatno naglašena diskrecijskom mogućnošću odlučivanja državnih tijela o granicama između javnog i tajnog dijela informacijskog prostora te je samim time bilo nepoznato ne samo što je tajno, već u velikoj mjeri i što se uopće može utvrditi kao tajno. Tajni prostor u to vrijeme pripadao je u potpunosti državnom sektoru u užem smislu, odnosno najvećim dijelom sigurnosno-obavještajnom, policijskom i vojnom dijelu tog sektora, a pravila klasificiranja podataka bila su u najvećoj mjeri nedostupna široj javnosti.

Nužnost vojne, ali i obavještajno-sigurnosne suradnje između različitih država - saveznika, sve više je oblikovala i ujednačavala postupke klasificiranja podataka kojima se utvrđuje potreba tajnosti nekog podatka. Tako se na prijelazu sedamdesetih u osamdesete godine prošlog stoljeća sve jasnije određuju koncepti kasnije široko prihvaćene, većinom četvero-stupanjske klasifikacije tajnosti podataka u državnom sektoru razvijenih zemalja. Postupci

klasificiranja zasnovani su na procjeni stupnja štete od mogućeg neovlaštenog otkrivanja klasificiranog podatka. Bitna komponenta ovog koncepta bila je jasna veza između stupnja tajnosti određenog klasificiranog podatka i skupa sigurnosnih mjera kojima treba zaštititi svaki podatak određenog stupnja tajnosti.

Sve jasniji zahtjevi politike informacijske sigurnosti u šezdesetim i sedamdesetim godinama prošlog stoljeća, potaknuli su stvaranje sigurnosnih modela za provedbu ciljeva politike informacijske sigurnosti na informacijskim sustavima [46]. Tako su nastali rešetkasti model (Lattice Model) i Bell-La Padula model, formalni sigurnosni modeli koji se bave kontrolom pristupa podatcima na informacijskom sustavu, odnosno sigurnosnim kriterijem povjerljivosti tih podataka, ili primjerice Biba model koji je usmjeren na kriterij cjelovitosti podataka. Sigurnosnim modelima na formalni, matematički način, arhitektura informacijskih sustava prilagođavala se ciljevima politike informacijske sigurnosti. S obzirom da je sastavni dio informacijskog sustava u primjeni i njegovo okruženje, koje uz tehnički sustav i podatke na sustavu obuhvaća i korisnike sustava, nužan daljnji korak bili su sigurnosni načini rada informacijskih sustava. Kako je to bilo razdoblje u kojemu su korišteni zatvoreni informacijski sustavi koji nisu bili povezani s vanjskim svijetom, okruženje je obuhvaćalo samo korisnike sustava. Sigurnosni načini rada informacijskih sustava utvrđeni kao: namjenski (engl. *Dedicated*), na razini sustava (engl. *System High*), razdijeljeni (engl. *Compartmented*) i višerazinski (engl. *Multilevel*), povezuju stupanj tajnosti klasificiranih podataka koji se koristi na informacijskom sustavu, razinu sigurnosnih certifikata osoba koje pristupaju informacijskom sustavu, nužnost pristupa klasificiranom podatku u okviru djelokruga rada osobe (engl. *Need-to-Know*), kao i formalno odobrenje za pristup podatcima na informacijskom sustavu [47]. Zanimljivo je da se sigurnosni načini rada i danas primjenjuju u svojoj izvornoj formi, iako se može reći da više gotovo i ne postoje zatvoreni informacijski sustavi za kakve su prvotno kreirani, no koncepti sigurnosnih mjera prema korisnicima klasificiranih informacijskih sustava ostali su uglavnom isti.

Iz ovoga je vidljivo da uspostava sustava povjerenja prema osobama tradicionalno čini vrlo bitan i nužan element u provedbi politike informacijske sigurnosti. Tako se, primjerice, u državnoj upravi, osobama koje pristupaju klasificiranim podatcima, na temelju sigurnosne provjere izdaje sigurnosno uvjerenje (certifikat) odgovarajućeg stupnja tajnosti, usklađeno sa stupnjem tajnosti klasificiranih podataka kojima trebaju pristupati u okviru svojih poslovnih zaduženja. Postupak sigurnosne provjere inicira državno tijelo - poslodavac, za svog

zaposlenika, koji u okviru djelokruga svog radnog mjesta ima potrebu pristupa određenim kategorijama klasificiranih podataka. Korištene kategorije klasificiranih podataka mogu biti vezane na međunarodne klasificirane podatke kao što su primjerice NATO ili EU klasificirani podatci, ili na pojedine nacionalne kategorije klasificiranih podataka, kao što su primjerice, podatci o klasificiranim ugovorima u okviru nabave ili neka druga klasificirana aktivnost ili projekt. Izdavanjem sigurnosnog certifikata osobi te potpisivanjem izjave osobe o tome da je svjesna svojih prava i obaveza u području tajnosti podataka, rukovoditelji pojedinih ustrojstvenih cjelina državnog tijela izdaju zaposleniku formalno odobrenje za pristup određenoj kategoriji klasificiranih podataka ili odobravaju pristup na neformalnoj razini, dodjelom svakog pojedinog klasificiranog podatka osobi koja ima odgovarajući certifikat i odgovarajuće poslovno zaduženje.

Ovakav koncept provedbe politike informacijske sigurnosti razvio se u državnom sektoru tijekom sedamdesetih i osamdesetih godina prošlog stoljeća, isprva u najrazvijenijim državama, a kasnije i u ostalim državama koje su surađivale kao partneri u različitim oblicima suradnje. Tako dolazi do stvaranja jasne i javnosti dostupne regulative vezane uz načela klasificiranja podataka, čime se zatvoreni i tajni dio tadašnjeg informacijskog prostora, transformirao u znatno otvorenije i jasno ograničeno područje, odnosno u domenu klasificiranih podataka koja je u takvom obliku prisutna i danas. S obzirom da su načela klasificiranja postala slična u različitim državama i pri tome javno propisana, stvoreni su preduvjeti za učinkovitu međunarodnu razmjenu klasificiranih podataka i suradnju različitih država na problematici koja zahtijeva razmjenu klasificiranih podataka, kao što je vojna suradnja ili borba protiv suvremenih prijetnji, kao što je terorizam. Međusobno povjerenje država zasnovano je na jasnim načelima klasificiranja i zaštite klasificiranih podataka, odnosno na primjeni odgovarajuće, međusobno usklađene politike informacijske sigurnosti. Tako se razvila praksa uzajamnog potpisivanja bilateralnih i multilateralnih međunarodnih sigurnosnih ugovora (engl. *General Security Agreements – GSA*), odnosno ugovora o uzajamnoj razmjeni i zaštiti klasificiranih podataka, kao što je primjerice [48].

Unatoč otvaranju opisanih mogućnosti međunarodne razmjene klasificiranih podataka preko međunarodnih sigurnosnih ugovora, segmentacija informacijskog prostora u nacionalnim granicama, ostala je snažno prisutna i tijekom osamdesetih godina prošlog stoljeća. Tek iznimno brz razvoj informacijske i komunikacijske tehnologije te brzo širenje Interneta, započeto na prijelazu osamdesetih i devedesetih godina prošlog stoljeća, ublažava ovu

nacionalnu segmentaciju informacijskog prostora, sve više povezujući nacionalne informacijske prostore različitih država u zajednički globalni informacijski prostor, koji se u prvom desetljeću ovog stoljeća počinje i sustavno izgrađivati [49]. U takvim okolnostima društvo postaje sve više svjesno potrebe zaštite od ugroza povezanih s rastućom i globalnom informacijskom tehnologijom. Tako sredinom devedesetih godina prošlog stoljeća, napose u Europskoj uniji [50], započinje doba sustavnog pristupa regulaciji koncepata privatnosti, odnosno zaštite osobnih podataka. Zaštita osobnih podataka ubrzo postaje globalni obrazac postupanja razvijenog svijeta. Na taj je način domena osobnih podataka sa slike 4.2 postala posebno značajna u informacijskom prostoru, jer su korisnici osobnih podataka i državna tijela i druge pravne osobe, a osobni podatci često se razmjenjuju i u okviru međunarodne suradnje različitih država, ali i u okviru svakodnevnih aktivnosti, kao što je primjerice sigurnost zračnog prometa.

Koncepti privatnosti fizičkih osoba potaknuli su razvoj analognog pristupa na razini pravnih osoba. U poslovnom sektoru tradicionalno se primjenjuje koncept zaštite intelektualnog vlasništva, pa je kao jedan od mogućih mehanizama, uz autorsko pravo i patent, prisutan i koncept poslovne tajne. Ipak, ovaj koncept u poslovnom sektoru predstavlja tajnost, odnosno podatke koje obilježava kriterij povjerljivosti. Stoga je postojala široka potreba za domenom podataka koji nisu tajni, već su namijenjeni isključivo za službenu uporabu. Razlog ovakvim potrebama, koje uglavnom nastaju tijekom druge polovine devedesetih godina prošlog stoljeća, bio je ponajviše u sve većoj uporabi komunikacijsko-informacijske tehnologije i u globalizaciji Interneta. Politike informacijske sigurnosti u području tajnih podataka bile su u to vrijeme nedovoljno prilagođene korištenju nove globalne komunikacijske tehnologije te je stvaranje nove domene podataka koja je na slici 4.2 označena kao osjetljivi podatci (engl. *Sensitive Information*), bilo učinkovito rješenje za integriranje segmentiranih nacionalnih informacijskih prostora u globalni informacijski prostor koje se u to vrijeme ubrzano događalo. Domena osjetljivih podataka omogućila je uvođenje kategorija podataka samo za službenu, odnosnu poslovnu uporabu. U ovoj domeni postoje vrlo raznolika rješenja kao i način označavanja ovakvih kategorija podataka, no zajedničko za kategorije podataka iz ove domene je da nemaju svojstvo tajnosti, da dijele dosta sličnosti s osobnim podatcima u smislu sigurnosnih mjera koje se postavljaju za njihovu zaštitu, te da je s takvim podatcima moguće komunicirati s drugim osobama u okviru službene ili poslovne suradnje koristeći primjerice, službeno potvrđene javne adrese elektroničke pošte i bez korištenja posebnih sigurnosnih mjera (npr. kriptiranje), što sa klasificiranim podatcima nije moguće.

Iako pod različitim nazivima i oznakama (npr. „*NATO Unclassified*“, „*EU Limitee*“, „*For Official Use Only*“ ili „Neklasificirano“), domena osjetljivih, odnosno označenih neklasificiranih podataka, krajem devedesetih godina postaje gotovo nezaobilazna domena podataka u velikom broju država, osobito u zemljama članicama NATO-a i EU-a. Slijedeći temeljne koncepte privatnosti, označene neklasificirane podatke u državnoj upravi obilježava osjetljivost u smislu poslovnih ili službenih odnosa, pri čemu ti podatci nemaju svojstvo tajnosti te kao takvi ne mogu biti klasificirani stupnjem tajnosti. Ovakvi podatci koji moraju biti označeni propisanom oznakom, predstavljaju mjeru kojom se može, primjerice, spriječiti uvid javnosti u situacijama kada bi takav uvid otežavao daljnju provedbu aktivnosti na koju se odnosi sadržaj ovakvog podatka. Jedan od najboljih primjera za korištenje osjetljive domene podataka jest planiranje i priprema budućih zakonskih akata u državnoj upravi, koji u fazi razrade mogu nositi oznaku osjetljivosti, kako bi se izbjeglo prerano javno komentiranje različitih opcija koje razmatra radna grupa zadužena za izradu prijedloga. Takav način korištenja oznake osjetljivosti ničim ne pretpostavlja kasniju proceduru, primjerice, preko javne rasprave ili prijedloga vlade za upućivanje pravnog propisa na donošenje u parlament. U svim tim slučajevima oznake osjetljivosti predstavljaju oznake za podatke koji nisu tajni, ali su namijenjeni isključivo za službeno postupanje ovlaštenih osoba (engl. *Need-to-Know*) i pri tome nije dopušteno njihovo objavljivanje bez suglasnosti vlasnika podataka. Na taj način uvedena je još jedna označena kategorija podataka koja osigurava primjereno postupanje s podatcima koji nisu tajni, ali nisu namijenjeni drugoj uporabi, osim u službene svrhe. Uvođenje ove domene osjetljivih podataka, iako posložnjuje planiranje politike informacijske sigurnosti, u osnovi predstavlja poticaj državnom sektoru za smanjenje broja klasificiranih podataka i samim time veću transparentnost rada.

### 4.2.2. Povezanost segmenata informacijskog prostora

Procesi demokratizacije društva tijekom devedesetih godina dvadesetog stoljeća uvode u regulativnu praksu koncept poznat kao pravo na pristup informacijama (engl. *Freedom of Information - FOI*) [2, 3]. Krajem devedesetih, mnoge razvijene demokratske države, osobito članice EU-a, uvode ovaj koncept u svoju nacionalnu regulativu [51]. Cilj ovog koncepta bio je pomiriti međusobno suprotstavljene zahtjeve državne uprave za klasificiranjem podataka te zahtjeve javnosti za transparentnošću rada državne uprave. U tom smislu važno je napomenuti da ovaj koncept nije u koliziji s podatkovnim domenama informacijskog prostora, kao što su

domena klasificiranih i osjetljivih podataka sa slike 4.2, već se ovim konceptom osigurava dodatna kontrola podataka kojima se bavi državna uprava – kontrola javnosti. Načelo prava na pristup informacijama tako obuhvaća mogućnost uvida u neki dokument državne uprave ili dobivanja informacije o određenoj temi, ali pod propisanim uvjetima (pisani zahtjev, utemeljeni razlog i sl.). Pri tome za domenu osjetljivih podataka, državna tijela koja su vlasnici podataka obavezna su osigurati uvid u takve podatke prema propisanoj proceduri.

Što se tiče klasificiranih podataka, oni su uglavnom izuzeti od izravne primjene ovog načela, ali se u većini država propisuju i dodatna načela nezavisne arbitraže između vlasnika podataka i tražitelja informacije, odnosno zakonske odredbe koje vlasnika klasificiranih podataka obvezuju na ocjenjivanje razmjernosti, između interesa javnosti i zaštite vrijednosti koje su klasificiranjem određenog podatka zaštićene. Najčešći organizacijski model primijenjen u različitim državama je model organizacije parlamentarnog povjerenika za informacije, zaduženog za arbitražu između tražitelja podatka, koji potraživanje temelji na načelu prava na pristup informacijama te vlasnika klasificiranih podataka, koji zaštitu podatka temelji na načelu tajnosti podataka državne uprave.

Stvaranjem globalnog informacijskog prostora (kibernetički prostor), zasnovanog na rasprostranjenosti i sveprisutnosti Interneta, javlja se potreba za učinkovitijim pristupom cjelokupnom informacijskom prostoru u odnosu na pristup koji proizlazi iz korištenja i načela pojedinih podatkovnih domena informacijskog prostora kao što je, primjerice, domena klasificiranih podataka. Pored nezaustavljive integracije nacionalnih informacijskih prostora u globalni informacijski prostor, međunarodne i nacionalne potrebe za komuniciranjem nameću promjenu i prilagodbu politika informacijske sigurnosti i prakse komuniciranja s različitim vrstama podataka, kao što su osobni podatci ili klasificirani podatci. Takve promjene nije moguće postići bez opsežne i koordinirane prilagodbe kompleksne regulative u području tajnosti i privatnosti podataka. Upravo to se posljednjih desetak godina i događa te se, počevši od globalno korištenog koncepta elektroničke državne uprave, preko šireg pojma informacijskog društva, prilagođava čitav niz komponenti nacionalnog zakonodavstva povezanih s konceptima tajnosti i privatnosti, kao što je primjerice u [52]. Takve prilagodbe, zbog iznimno velikog tehnološkog iskoraka u području komunikacijske i informacijske tehnologije te sveprisutnosti Interneta, kao i posljedično stvorene nove društvene situacije – globalizacije, sežu u čitav niz zakona kojima se regulira područje rada davatelja elektroničkih komunikacijskih usluga, utvrđuju elektroničke inačice dokumenata i potpisa, postavljaju

načela zaštite klasificiranih podataka, osobnih i drugih podataka, propisuju mjere zaštite podataka, odnosno potiče normizacija, kako u tehnološkom, tako i u sigurnosnom smislu.

Prema opisanim povijesnim procesima razvoja može se vidjeti da se utjecaj informacijskog prostora na politike informacijske sigurnosti prenosi preko dva ključna koncepta:

1. različitih domena podataka - od kojih se i danas sastoji informacijski prostor (klasificirani podatci, osjetljivi podatci, osobni podatci, intelektualno vlasništvo), a koje se ovdje promatraju u njegovom širem povijesnom značenju pojašnjenom u poglavlju 4.2.; ove domene podataka (slika 4.2) nastajale su na opisani način, tijekom formativnog razdoblja politika informacijske sigurnosti, a razlozi nastanka ovih domena i pravila korištenja podataka iz tih domena u najvećoj mjeri su prisutna i danas (kriterij dominantnosti s obzirom na zahtjeve informacijske sigurnosti);
2. globalne komunikacijsko-informacijske infrastrukture - koja je u procesima koji su se odvijali tijekom protekla dva do tri desetljeća gotovo u potpunosti integrirana s domenama podataka iz točke 1. (uključuje i klasificirane podatke) te je danas pojmovno praktično nedjeljiva od informacijskog prostora i domena podataka pod točkom 1., a pojam kibernetičkog prostora, upravo na temelju ovog razmatranja, dobiva svoje puno značenje i smisao, kao i povezanost i ulogu u okviru šire domene informacijske sigurnosti i suvremenih politika informacijske sigurnosti.

## 4.3. Obilježja politika informacijske sigurnosti u državnom i poslovnom sektoru

Politika informacijske sigurnosti ima najdužu tradiciju u državnim sektorima razvijenih zemalja [53]. Temeljni cilj politike informacijske sigurnosti državnog sektora danas, u osnovi je isti kao i prije nekoliko desetaka godina: osigurati minimalne sigurnosne mjere prilikom postupanja s klasificiranim podatcima u državnim tijelima.

### 4.3.1. Tradicionalna politika informacijske sigurnosti državnog sektora

Tipičan način kako se osiguravaju minimalne sigurnosne mjere je uvođenje metode klasificiranja podataka, procedure koja je danas u velikom broju zemalja metodološki gotovo unificirana. Metoda klasificiranja uobičajeno se sastoji od četiri stupnja tajnosti, definirana u smislu štete koju bi prouzročilo neovlašteno otkrivanje tako označenih podataka. Ovu metodu detaljnije će se prikazati na temelju primjera iz hrvatske regulative, Zakona o tajnosti

podataka [54]. Metodu klasificiranja uobičajeno prati i sustav mjera informacijske sigurnosti za svaki stupanj klasificiranja, koji je u Republici Hrvatskoj propisan Zakonom o informacijskoj sigurnosti [39] i njegovim podzakonskim aktima. Time je uveden novi pristup klasificiranju podataka, sukladan zahtjevima NATO-a i EU-a za zemlje članice. Ključna novina sastoji se u ukidanju prijašnjih vrsta tajnosti (državna, vojna, službena) te uvođenju jedinstvenog četvero-stupanjskog sustava klasifikacije, neovisno o tome je li sadržaj klasificiranog podatka vojne ili civilne naravi, već isključivo procjenjujući razinu štete koju bi neovlašteno otkrivanje takvog podatka prouzročilo za zakonom zaštićene vrijednosti. Zakonom su uvedena određena ograničenja pa se tako klasificirati mogu samo podatci iz djelokruga državnih tijela u područjima obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva, ali samo ako su od sigurnosnog interesa za Republiku Hrvatsku. Određivanje stupnja štete od neovlaštenog otkrivanja definira stupanj tajnosti:

1. „Vrlo tajno“ (VT) - neovlašteno otkrivanje nanijelo bi nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske;
2. „Tajno“ (T) – neovlašteno otkrivanje teško bi naštetilo nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske;
3. „Povjerljivo“ (POV) – neovlašteno otkrivanje naštetilo bi nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske;
4. „Ograničeno“ (OGR) – neovlašteno otkrivanje naštetilo bi djelovanju i izvršavanju zadaća državnih tijela u okviru obavljanja poslova u područjima u kojima je zakonom omogućeno klasificiranje podataka.

U okviru nacionalne sigurnosti i vitalnih interesa RH, definirane su osobito sljedeće vrijednosti:

1. temelji Ustavom utvrđenog ustrojstva Republike Hrvatske;
2. neovisnost, cjelovitost i sigurnost Republike Hrvatske;
3. međunarodni odnosi Republike Hrvatske;
4. obrambena sposobnost i sigurnosno-obavještajni sustav;
5. sigurnost građana;
6. osnove gospodarskog i financijskog sustava Republike Hrvatske;
7. znanstvena otkrića, pronalasci i tehnologije od važnosti za nacionalnu sigurnost Republike Hrvatske.

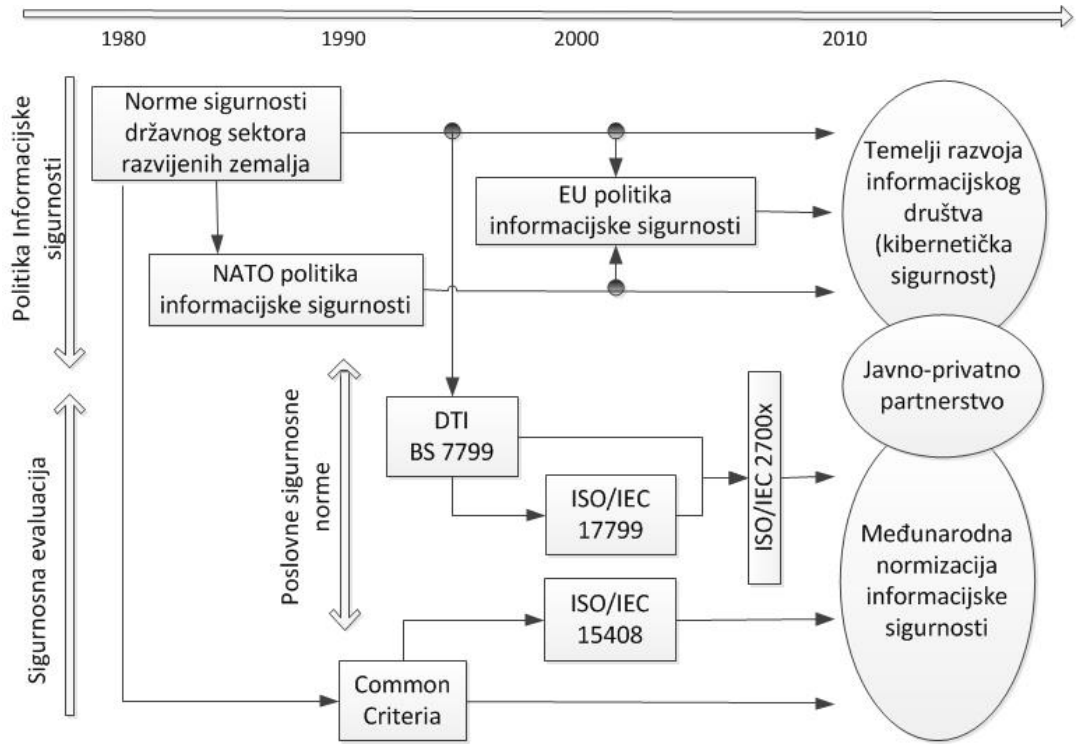
Klasificiranje podataka provode zakonom ovlaštena državna tijela kada u okviru poslova iz svoje nadležnosti, utvrde moguću štetu od neovlaštenog otkrivanja podataka za vrijednosti definirane zakonom. U okviru procesa klasificiranja državna tijela su podijeljena u dvije skupine: skupinu koja može klasificirati svim stupnjevima tajnosti i skupinu koja može klasificirati samo stupnjevima tajnosti POV i OGR. Pri tome, ostala tijela državne uprave, kao i tijela lokalne vlasti i pravne osobe s javnim ovlastima, mogu biti samo primatelji, tj. korisnici klasificiranih podataka. Za znanstvene ustanove, zavode i druge pravne osobe koje rade na projektima, pronalascima, tehnologijama i drugim poslovima od sigurnosnog interesa za Republiku Hrvatsku, klasificiranje provode zakonom ovlaštena državna tijela, nadležna po određenoj problematici.

### 4.3.2. Razvoj suvremene politike informacijske sigurnosti

Opisani koncept klasificiranja podataka temelji se na metodi široko prihvaćenoj u demokratskim državama svijeta u razdoblju tijekom šezdesetih i sedamdesetih godina prošlog stoljeća. Unificiranim pristupom klasificiranju, koji je nastao širokim prihvaćanjem ovakve metode klasificiranja zasnovane na stupnju štete od neovlaštenog otkrivanja klasificiranog podatka, otvorio se prostor za sadržajno usklađivanje odredbi politike informacijske sigurnosti u različitim državama. Proces sadržajnog usklađivanja politike informacijske sigurnosti vremenom je doveo do korištenja pet danas gotovo isključivo primjenjivanih područja informacijske sigurnosti u državnom sektoru: sigurnost osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost poslovne suradnje [39]. Područje sigurnosti informacijskih sustava, za koje se dugo vremena koristio naziv INFOSEC, nastalo je u okviru brzog razvoja tehnologije na prijelazu stoljeća, spajanjem tradicionalnih tehničkih sigurnosnih područja: COMSEC (engl. *Communication Security*), TECSEC (engl. *Technical Security*) i COMPUSEC (engl. *Computer Security*). Aktualnim izmjenama politike informacijske sigurnosti u NATO-u, EU i zemljama članicama, nastoji se ovo područje informacijske sigurnosti na odgovarajući način proširiti, kako bi u kombinaciji s nacionalnim strategijama i drugom regulativom, osiguralo potporu rastućim zahtjevima kibernetičke sigurnosti te se u NATO terminologiji prešlo na pojam „*Comunication and Information System Security*“, a u EU se koristi pojam „*Information Assurance*“.

Ovaj proces sustavne razrade, sadržajnog oblikovanja i normiranja politike informacijske sigurnosti u državnom sektoru, započet još sedamdesetih godina prošlog stoljeća, utjecao je

na niz drugih procesa koji su u konačnici rezultirali nekim od danas široko primjenjivanih međunarodnih normi, kao što su paleta normi informacijske sigurnosti ISO/IEC 27000 ili norma ISO/IEC 15408 za sigurnosnu evaluaciju informacijske tehnologije, što je prikazano na slici 4.3 [1].




**Slika 4.3:** Razvoj politika i normi informacijske sigurnosti

Problematika razvoja politika informacijske sigurnosti, ali i metoda sigurnosne evaluacije, od samog početka normizacije područja informacijske sigurnosti u državnom sektoru, bile u središtu interesa najrazvijenijih država. Normizacija nacionalne politike informacijske sigurnosti u razvijenim državama uvelike je utjecala na zajedničku, političko-obrambenu organizaciju tih država – NATO. Suvremena politika informacijske sigurnosti NATO-a, koja je potpuno revidirana tijekom devedesetih godina prošlog stoljeća, utjecala je u najvećoj mjeri i na politiku informacijske sigurnosti EU-a, čiji je ozbiljniji razvoj započet na prijelazu stoljeća.

Najveći utjecaj na međunarodnu normizaciju informacijske sigurnosti u širem smislu od državnog sektora, imao je razvoj politike informacijske sigurnosti u Velikoj Britaniji koji je, iako proizašao iz državnog sektora, uvelike nadilazio njegove okvire. Taj razvoj je sredinom devedesetih godina prošlog stoljeća rezultirao dokumentom najbolje prakse informacijske

sigurnosti koji je Ministarstvo trgovine i industrije Velike Britanije (engl. *Department of Trade and Industry – DTI*), uz pomoć britanskog nacionalnog tijela za normizaciju (engl. *British Standards Institute*), 1995.g. utvrdilo kao britansku nacionalnu normu BS 7799-1. Već pet godina kasnije, Međunarodna normizacijska udruga ISO/IEC je ovu normu prihvatila kao međunarodnu normu ISO/IEC 17799:2000. Time je otvoren put za šire prihvaćanje ove norme, što se kasnije ponovilo i sa drugim dijelom britanske norme BS 7799-2 koji sadržava specifikaciju sustava upravljanja informacijskom sigurnošću (ISMS) i predstavlja osnovu za certificiranje prema ovoj normi.

Na sličan način su nastale norme za sigurnosnu evaluaciju IT proizvoda i sustava (engl. *Common Criteria for Information Technology Security Evaluation - CC*), čiju je izradu na temelju europske ITSEC norme te nekih nacionalnih normi uključenih zemalja, inicirala grupa razvijenih zemalja svijeta (Francuska, Kanada, Nizozemska, Njemačka, Velika Britanija i SAD). ISO/IEC preuzeo je ovu normu i objavio ju 1999.g. kao međunarodnu normu ISO/IEC 15408:1999 koja se sastoji iz tri dijela [55].

Pored navedenih izravnih utjecaja pri razvoju spomenutih međunarodnih normi informacijske sigurnosti, suvremena politika informacijske sigurnosti suočava se i s procesima razvoja informacijskog društva. Pri tome oba ključna utjecaja za razvoj informacijskog društva, brzi razvoj komunikacijske i informacijske tehnologije, kao i globalizacija društva i sveprisutnost Interneta, sa svim svojim utjecajima na posebne vrste podataka koje su od značaja za informacijsku sigurnost, otvaraju čitav niz novih inicijativa prikazanih na desnoj strani slike 4.3. Opisana međunarodna normizacija područja informacijske sigurnosti svakako je jedna od najznačajnijih inicijativa. Nadalje, tu su inicijative koje su nužne pri razvoju temelja informacijskog društva i kojima se nastoje postići sigurnosni uvjeti svojstveni za tradicionalno društvo, odnosno problematika kibernetičke sigurnosti. Činjenica da informacijsko društvo obuhvaća sva tri čimbenika suvremenog društva: državni sektor, poslovni sektor i građanstvo u cjelini, uvodi još jednu nužnu komponentu: javno-privatno partnerstvo. Upravo u programima EU-a ovakve inicijative su najvidljivije [49].

### 4.3.3. Minimalne sigurnosne mjere i upravljanje rizikom

Tradicionalna politika informacijske sigurnosti, koja je nastajala u državnim sektorima razvijenih zemalja u razdoblju do devedesetih godina prošlog stoljeća, redovito je bila zasnovana na dva ključna elementa:

1. klasificiranje podataka propisanim stupnjevima tajnosti - uobičajeno četvero-stupanjski sustav klasificiranja, zasnovan na stupnju štete od neovlaštenog otkrivanja za zakonom zaštićene vrijednosti;
2. utvrđeni skup minimalnih mjera informacijske sigurnosti - za svaki pojedini stupanj tajnosti klasificiranog podatka.

To znači da utvrđeni stupanj tajnosti klasificiranog podatka određuje minimalni skup zaštitnih mjera (engl. *Baseline Approach*) koji se mora primjenjivati na tako označeni klasificirani podatak. Na taj način svaki vlasnik klasificiranih podataka kao i svaki korisnik klasificiranog podatka, mora primjenjivati iste i ujednačene mjere informacijske sigurnosti (skup minimalnih sigurnosnih mjera), propisane na razini cijelog državnog sektora, a po potrebi i šire, u okviru međunarodne razmjene klasificiranih podataka.

Jedan od najranijih pokušaja uvođenja upravljanja rizicima informacijske sigurnosti datira iz sedamdesetih godina prošlog stoljeća, kad je Nacionalni zavod za norme SAD-a (danas poznat pod nazivom *National Institute of Standards and Technology – NIST*), objavio FIPSPUB-31, „Fizička sigurnost i upravljanje rizicima u automatskoj obradi podataka“ (1974.g.). Ipak, tek tijekom devedesetih godina prošlog stoljeća, u područje informacijske sigurnosti u uporabu se sve više uvode različite metode upravljanja rizikom informacijske sigurnosti. Najveći utjecaj na norme u području upravljanja rizikom imao je financijski sektor. To je prvenstveno proizašlo iz činjenice da je financijski sektor tehnološki prednjačio u uvođenju internetskih usluga i u internetskom poslovanju. Na taj način su i mjere informacijske sigurnosti u financijskom sektoru morale sustavno obuhvatiti, ne samo tradicionalno prisutne aspekte ljudi i fizičke sigurnosti, već i visoko zastupljenu informacijsku tehnologiju o kojoj ovisi cjelokupni poslovni proces svake financijske institucije. S druge strane, metode upravljanja rizicima tradicionalno se koriste u poslovanju financijskih institucija pa su se prirodno proširile sa financijskih na operativne rizike, važne za problematiku informacijske sigurnosti. Za razliku od državne uprave koja uobičajeno klasificira podatke sa četiri stupnja tajnosti, financijski sektor kao i općenito poslovni sektor u cjelini, klasifikaciju provodi na znatno jednostavniji način. Tako se najčešće razlikuju samo

vrste podataka, kao što su osobni podatci, poslovna tajna (usporediva s klasificiranim podatkom) ili primjerice, osjetljivi podatci. S druge strane, ovisnost financijskih institucija o kontinuitetu poslovnih procesa barem je jednako značajna kao i povjerljivost podataka u državnoj upravi. Takvi različiti zahtjevi, inherentni samim poslovnim ciljevima koji su bitno različiti u poslovnom sektoru od onih u državnoj upravi, doveli su i do različitih smjerova razvoja informacijske sigurnosti u državnoj upravi i poslovnom sektoru.

Upravljanje rizicima informacijske sigurnosti tako se nametnulo kao značajan zahtjev kojim se odgovara na svojstvo raspoloživosti, a ne samo povjerljivosti, kako informacijskih sustava tako i podataka, odnosno na kontinuitet poslovanja i činjenicu da je poslovni sektor više usmjeren na poslovne procese, a manje na pojedine vrste tajnih podataka. To znači da za razliku od državnog sektora u kojem je temeljni objekt zaštite klasificirani podatak, poslovni sektor štiti informacijsku imovinu i poslovne procese u širem smislu. Upravljanje rizikom u području informacijske sigurnosti povezano je se s pojmom operativnog rizika. Iako ne postoji jedinstvena definicija operativnog rizika, najčešće se primjenjuje definicija nastala u okviru Basel II norme [56] koja opisuje operativni rizik kao rizik gubitka nastao zbog neodgovarajućih unutarnjih poslovnih procesa ili procesa u kojima postoje slabosti ili pogreške, odnosno zbog ljudskog faktora i tehničkih sustava ili zbog vanjskog događaja. Definicija operativnog rizika kao rizika od gubitka izdvaja ga od tipičnih financijskih rizika koji su spekulativne prirode, odnosno rizika koji se poduzimaju u smislu ostvarivanja dobiti (npr. kreditni rizik, valutni rizik). Nadalje, povezanost operativnog rizika s unutarnjim poslovnim procesima, osobama, sustavima i vanjskim događajima može se staviti u određeni odnos s temeljnim konceptima pristupa politici informacijske sigurnosti, odnosno upravljanju informacijskom sigurnošću. Metode upravljanja rizicima u okviru suvremenog pristupa informacijskoj sigurnosti, temelje se na identificiranoj imovini koju treba zaštititi, zatim na identificiranim prijetnjama za tu imovinu, identificiranim ranjivostima koje bi ove prijetnje mogle iskoristiti (vektor napada) te na procjeni utjecaja koje gubitak povjerljivosti, cjelovitosti ili raspoloživosti može imati na imovinu. Sigurnosne kontrole (zaštitne mjere) štite identificiranu imovinu, tj. vrijednosti koje je organizacija identificirala kao važne za poslovanje i koje se nalaze u opsegu primjene metode upravljanja rizikom. U osnovi, ovako definirani operativni rizici predstavljaju sveobuhvatno viđenje prijetnji bilo da nastaju u okviru unutarnjih slabosti organizacije, ili zbog prirodnih nepogoda ili drugih vanjskih prijetnji, te uslijed namjernog ili nenamjernog postupanja ljudi.

S druge strane, tradicionalna politika informacijske sigurnosti državnog sektora formirala je svoje temelje u doba hladnog rata kada je sustav prijetnji bio definiran blokovskom podjelom svijeta i simetričan po svojoj prirodi, jer je imao jednostavnu podjelu na prijateljsku i neprijateljsku stranu, kao i jednostavna, zatvorena organizacijska i tehnološka okruženja, ali i znatno zatvorenije državne granice. Posljedica toga je da se promjene tradicionalne politike informacijske sigurnosti i postupno kombiniranje metoda minimalnih sigurnosnih mjera i procjene rizika, počinju postupno uvoditi tek na prijelazu stoljeća, kako bi se odgovorilo novim, asimetričnim prijetnjama, nastalim kao posljedica raspada blokovske podjele svijeta i nastupa društvene globalizacije, odnosno velikog tehnološkog razvoja i sveprisutnosti Interneta. Pojam asimetričnih prijetnji dolazi iz vojne doktrine. Asimetričnim se općenito smatra borba slabijeg i jačeg, odnosno netradicionalnog i tradicionalnog [57]. U teoriji ratovanja, asimetričnost je poznata odavno, kroz dugu povijest gerilskih ratova s asimetričnim vojnim snagama koje se sukobljavaju na specifičan gerilski način. Nakon završetka razdoblja hladnog rata, ova forma ratovanja postaje pretežita u svijetu. U isto vrijeme, terorističke prijetnje koje se šire svijetom, predstavljaju također asimetrične prijetnje i to u znatno širem smislu i obimu od vojnog, odnosno predstavljaju prijetnje nacionalnoj sigurnosti, ekonomskoj i društvenoj dobrobiti. Nadalje, ubrzani tehnološki razvoj, praćen sveprisutnim Internetom, pridružuje konceptu asimetričnih prijetnji i novu tehnološku, odnosno kibernetičku formu prijetnji, također asimetričnih obilježja, odnosno onu koja može nastati bilo gdje i bilo kada pa je pojavu prijetnje ekspertno-analitičkim pristupom nemoguće predvidjeti. Kibernetičke prijetnje nemaju samo obilježja prijetnji informacijama ili informacijskim resursima, već zbog sve veće ovisnosti društva, svih vrsta organizacija, te različite energetske i druge infrastrukture, o informacijskoj i komunikacijskoj tehnologiji, obilježja ovih kibernetičkih prijetnji postaju znatno šira. Postoji cijeli spektar kibernetičkih prijetnji, od različitih neželjenih izvršnih programa koji ometaju korisnike Interneta, preko krađa identiteta i računalnih financijskih prijevara, pa sve do prijetnji kritičnoj nacionalnoj infrastrukturi i potencijalnog ugrožavanja života ljudi [4, 5, 45].

Uvođenje procesa upravljanja rizicima u državnom sektoru najprimjetnije je u području sigurnosti informacijskih sustava. Već od kasnih devedesetih godina prošlog stoljeća više nije bilo moguće voditi politiku informacijske sigurnosti zasnovanu na zatvorenim informacijskim sustavima, na način kakav je bio koncipiran u šezdesetim godinama prošlog stoljeća. Ovakvi zatvoreni informacijski sustavi (engl. *Air-gap*), podrazumijevali su informacijsku infrastrukturu bez fizičke veze s vanjskim svijetom, odnosno s komunikacijskim vodovima

pod izravnom kontrolom vlasnika informacijskog sustava. Promjene u razvoju tehnologije, liberalizacija telekomunikacijskog sektora, kao i sveprisutnost Interneta, zauvijek su promijenile obilježja tradicionalnog pojma zatvorenih (klasificiranih) informacijskih sustava [58], te se danas u najvećem broju slučajeva koristi klasificirane informacijske sustave s fizičkim vezama preko Interneta, ali bez logičkih veza s vanjskim informacijskim servisima, ili s logičkim vezama koje su posebno kontrolirane ili ograničene (npr. jednosmjerne podatkovne diode). Takva promjena otvorila je niz ranjivosti današnjih klasificiranih informacijskih sustava (npr. problem programskih zakrpa), te ih u određenoj mjeri izložila suvremenim kibernetičkim prijetnjama (npr. računalni virusi i crvi).

Iako se kibernetičke prijetnje mogu svrstati u podjele prema skupinama otkaza, nezgoda i napada, specifičnost je da moramo jasno razlikovati dvije važne kategorije prijetnji informacijskih sustava, u odnosu na prijašnje poimanje tradicionalnih prijetnji: nestrukturirane prijetnje (hakeri, pojedinci) i strukturirane prijetnje (strane države, terorističke i kriminalne organizacije). Ove prijetnje potrebno je promatrati u kontekstu okolnosti nastalih nakon završetka hladnog rata, odnosno u kontekstu razvoja suvremenog kibernetičkog prostora bez državnih granica, s (uglavnom) anonimnim počiniteljima novih računalnih kaznenih djela, s brzim razvojem tehnologije praćenim unutarnjim ranjivostima komercijalnih proizvoda, te s danas lako dostupnim i rasprostranjenim alatima i tehnikama za iskorištavanje ovih ranjivosti i pokretanje automatiziranih metoda kibernetičkih napada. Sve ovo rezultira činjenicom da na ekspertno-analitičkoj razini nije moguće predvidjeti vjerojatnost kibernetičkih napada, niti općenito asimetričnih prijetnji kao što je to bio slučaj sa tradicionalnim, simetričnim sigurnosnim prijetnjama. Upravo ova činjenica, ključni je razlog najvećeg broja aktualnih promjena koje se događaju u revizijama pristupa politikama informacijske sigurnosti.

U takvoj situaciji tradicionalna politika informacijske sigurnosti u državnom sektoru, zasnovana na konceptu minimalnih sigurnosnih mjera koje su usko povezane sa stupnjevima tajnosti klasificiranih podataka, pribjegava selektivnoj primjeni metoda upravljanja rizikom. To znači da se upravljanje rizikom primjenjuje u okvirima područja informacijske sigurnosti (npr. sigurnost informacijskih sustava, fizička sigurnost, sigurnost podataka i sl.) ili na određenim razinama (npr. okosnica računalne mreže i najvažniji informacijski sustavi). Na taj način se selektivno primjenjuje metoda upravljanja rizikom, u kombinaciji s obaveznim i trajno prisutnim minimalnim sigurnosnim mjerama u svih pet područja informacijske

sigurnosti. S obzirom da je ažuriranje politike informacijske sigurnosti uobičajeno jedan do dva puta godišnje, pojedini sigurnosni elementi koji se kroz upravljanje rizicima pokažu kao dobra rješenja, uključuju se po potrebi u minimalne sigurnosne mjere pojedinih područja informacijske sigurnosti.

Ovakav koncept minimalnih sigurnosnih mjera poznat je i u poslovnom sektoru u obliku primjene najbolje prakse. Primjerice, danas najšire korištena paleta normi informacijske sigurnosti ISO/IEC 27000, nastala je 1995.g. kao BS 7799-1 (kasnije ISO 17799), odnosno kao skup najboljih praksi koji u početku i nije bilo moguće certificirati, jer je BS 7799-2, kao norma za provedbu certifikacije nastao 1998.g., a ISO/IEC ga je preuzeo 2005.g. Tek nakon preuzimanja i šire popularizacije ove norme namijenjene certificiranju preko ISO/IEC organizacije, sustavno je uveden formalni postupak certificiranja i broj certificiranih organizacija u svijetu počeo se polako povećavati. Tome treba dodati da zbog relativno visoke cijene formalnog postupka certificiranja prema ISO 27001, državni sektor gotovo redovito [59], kao i dio poslovnog sektora, koristi internu reviziju prema ISO/IEC 27001. Svi načini primjene ove palete normi u razdoblju nakon donošenja ISO/IEC 27001, obavezno se provode u okviru primjene metode upravljanja rizikom.

Potrebno je uočiti da koncept minimalnih sigurnosnih mjera ne ide za tim da rizike postavi u korelaciju s vrijednošću imovine, već umjesto toga traži identificiranje i postavljanje svih unaprijed definiranih sigurnosnih zahtjeva u procese. Postoje dva načina kako se unaprijed definirane sigurnosne mjere ili kontrole određuju. Eksplicitno propisivanje minimalnih sigurnosnih mjera s njihovim centraliziranim praćenjem i povremenim revidiranjem, uobičajeno je rješenje za politiku informacijske sigurnosti državnog sektora. Korištenje najbolje prakse bilo je češće u poslovnom sektoru, gdje se na temelju različitih normi najbolje prakse, kao što je opisani primjer s normom ISO 17799, odabiru sigurnosne kontrole koje se ostvaruju, a procjena se vrši usporedbom sa sličnim rješenjima u sektoru poslovanja kojim se određena tvrtka bavi.

Važan problem koji se u novije vrijeme pojavljuje i u državnom i u poslovnom sektoru je povjerenje u informacijsku tehnologiju, odnosno certificiranje uređaja, sustava i programske podrške. Ovdje postoji problem asimetričnih informacija poznat iz ekonomije [60], koji se manifestira u području informacijske sigurnosti u problemu sigurnosti proizvoda informacijske tehnologije. Paradoks leži u činjenici da nema široko prihvaćenog načina kojim

bi korisnici razlikovali sigurne od nesigurnih proizvoda te slijedom toga proizvođači nisu motivirani investirati u sigurnost proizvoda. Certifikacijske procedure kao što je *Common Criteria* (CC), bile su rani pokušaj odgovora na ovaj problem. Zbog dugotrajnog procesa certifikacije, povezanog s visokim troškovima, te nemogućnosti praćenja tražene dinamike tržišta novih proizvoda, tvrtke se rjeđe i samo za manji broj proizvoda, odlučuju upustiti u proces certificiranja po CC normi, odnosno normi ISO/IEC 15408:1999, koja je u međuvremenu nastala preuzimanjem ove norme na međunarodnoj razini. Spomenuta problematika asimetričnih informacija i posljedični paradoks, kao što je prikazani slučaj nepostojanja motivacije za proizvodnju sigurnih proizvoda, spada u područje sigurnosne ekonomije [61], grane koja povezuje problematiku sigurnosti i ekonomije i koja je tijekom desetljeća brzog razvoja tehnologije i Interneta izgubila na važnosti, ali se brzo i uspješno revitalizira posljednjih godina.

Složenost organizacije, tehnologije, kao i pravnih odgovornosti, čini suvremeno informacijsko društvo osjetljivim na čitav niz povezanih prijetnji i ranjivosti, koje se dinamički mijenjaju zajedno sa stalnom promjenom sigurnosnog okruženja [3]. Odgovore na ova pitanja suvremenih prijetnji i ranjivosti, uglavnom nije moguće dati isključivo tehnološkim, niti organizacijskim, a niti isključivo regulativnim rješenjima, već jedino kombinacijom svih ovih rješenja. Politike informacijske sigurnosti na različitim razinama, od međunarodnih organizacija kao što su NATO i EU, preko nacionalnih, do politika informacijske sigurnosti u ključnim poslovnim sektorima, mogu dati odgovarajuća rješenja, ali jedino ako su međusobno dobro koordinirane u svim povezanim aspektima organizacijskih, tehnoloških i regulativnih obilježja. Ovakvi problemi koji se mogu uočiti u praksi, usko su povezani s problematikom slabe koordinacije stupova sigurnosnih zahtjeva, izloženom u poglavlju 1.2., o motivaciji ovog istraživanja.

## 4.4. Regulativni okvir informacijske sigurnosti

Minimalne sigurnosne mjere, kao i upravljanje rizicima, usko su povezani s dva važna regulativna načela:

1. načelo primjerene pažnje (engl. *Duty of Care*);
2. načelo svijesti o rizicima poslovanja (engl. *Duty of Diligence*).

Pri tome, načelo primjerene pažnje podrazumijeva zakonsku odgovornost bilo koje pravne osobe za primjerenu pažnju u provedbi sigurnosnih propisa koja se dokazuje provedbom

relevantnih normi informacijske sigurnosti (npr. najbolje prakse), čime se izbjegava eventualna odgovornost pravne osobe za određenu povredu sigurnosti koja je rezultirala štetom po korisnike. Sustavno provođenje politike informacijske sigurnosti predstavlja najbolju interpretaciju zahtjeva o primjerenoj pažnji u provedbi sigurnosnih propisa. Načelo svijesti o rizicima poslovanja predstavlja zakonsku odgovornost pravne osobe za kontinuirano istraživanje i razumijevanje rizika s kojima se tvrtka suočava čime se propisuje izravna odgovornost osoba u upravi tvrtke za poslovanje tvrtke (tzv. regulativa korporativnog upravljanja), a obveza se ostvaruje primjenom odgovarajuće metode upravljanja rizicima na nivou poslovanja tvrtke (rizici poslovanja). Svrha ovog načela je zaštita svih zainteresiranih strana u poslovanju tvrtke (vlasnici, zaposlenici, kooperanti, korisnici, …). Slično kao i za načelo primjerene pažnje, može se i ovdje reći da sustavno provođenje upravljanja rizikom poslovanja predstavlja uspješnu interpretaciju zahtjeva poslovne odgovornosti u provedbi sigurnosnih propisa.

Načelo svijesti o rizicima poslovanja bitno je ne samo za upravu određene tvrtke već i za regulatorna tijela, odnosno nadležna državna tijela. Temeljno načelo u metodama upravljanja rizikom je pridruživanje odgovornosti organizacijskom entitetu koji može najprikladnije djelovati na upravljanje rizikom. Primjeri u praksi dobro pokazuju taj problem. Tako problem sigurnosti bankomata nije rješiv ukoliko se banke ne utvrde odgovornima za kartične prijevare povezane s bankomatima. Ukoliko je teret dokazivanja prijevara na krajnjem korisniku, banka nije motivirana za sigurnosna ulaganja u svoj sustav bankomata. Potrebno je napomenuti da na temeljno načelo pridruživanja odgovornosti organizacijskom entitetu koji je najbolje pozicioniran za upravljanje rizikom, bitno utječu i prijetnje. Tako u slučaju suvremenih elektroničkih kartica za financijske transakcije, koje koriste kombinaciju čip- i pin-zaštite, imamo primjer potencijalne ranjivosti (mogućnost provedbe transakcije karticom bez korištenja pina) prema [62], koja dodatno problematizira priznavanje šteta između trenutka nestanka kartice i poništenja kartice od banke koja ju je izdala, a na zahtjev korisnika. Ovo je vremenski prozor koji je u najvećem broju slučajeva u odgovornosti krajnjeg korisnika nestale kartice, a koji u opisanom slučaju, ne može utjecati na smanjenje rizika, odnosno na prijetnju. Praksa pokazuje da je mehanizam pravilnog određivanja odgovornosti za rizike (načelo svijesti o rizicima poslovanja) u mnogim slučajevima puno učinkovitiji od detaljnog obvezivanja tvrtki za provedbom određenih sigurnosnih mjera (načelo primjerene pažnje), osobito u dijelu posljedica rizika po korisnike njihovih usluga. Dobar primjer za ovo su trendovi razvoja regulative elektroničkih komunikacija u zemljama

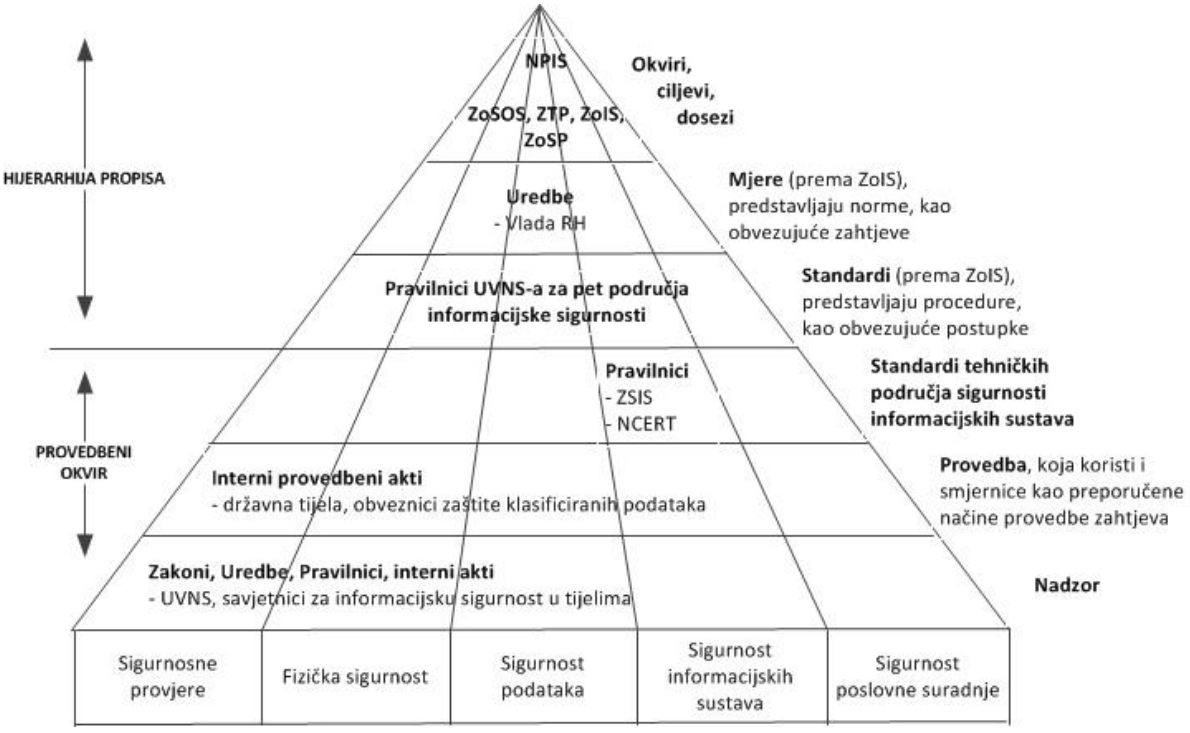
članicama EU-a, gdje se posljednjih nekoliko godina vidi sve veći pomak u postavljanju odgovornosti na operatore pojedinih javnih elektroničkih usluga, primjerice u obvezama filtriranja neželjene elektroničke pošte (engl. *Spam*).

Koncept regulativnog okvira informacijske sigurnosti temelji se na kombinaciji zakonodavnih propisa, međunarodnih i nacionalnih normi te unutarnjih propisa i ugovornih obaveza svake pojedine organizacije (državnog tijela ili pravne osobe, odnosno tvrtke) [3]. U posljednjih desetak godina složenost regulativnog okvira informacijske sigurnosti značajno je porasla. Razlozi tome leže u nizu čimbenika koji donose promjene u suvremenom društvu, kao što su društveno-politički procesi poslije hladnog rata, globalizacija, velik tehnološki napredak krajem dvadesetog stoljeća, sveprisutnost Interneta, velike sigurnosne krize poput terorističkog napada na SAD 11. rujna 2001. godine ili veliki gospodarski problemi poput propasti američke korporacije Enron iste godine, ali i zahtjevi demokratizacije poput načela prava na informaciju ili zaštite privatnosti. Sigurnost nije samoj sebi svrha, već je stanje koje se želi postići u društvu, odnosno unutar nekog sektora društva, primjerice zdravstva, financijskog sektora, gospodarstva, državnog sektora, građanstva itd. Kako su svi ti društveni sektori u današnjem društvu sve uže povezani, tako se i sigurnosni mehanizmi nužno dodiruju ili međusobno preklapaju u pojedinim slučajevima. Sve ovo uvelike otežava utvrđivanje primjenjivosti pojedinih zakona i nekih specifičnih zakonskih odredbi, a pogotovo međusobnih interakcija više različitih propisa. Općenito rečeno, identifikacija primjenjive zakonske regulative može biti prilično težak zadatak, osobito u slučajevima kada određena organizacija, državno tijelo ili pravna osoba, surađuje ili posluje u međunarodnim okvirima, što u današnjem svijetu postaje nužnost, a pri tome se složenost regulativnog okvira informacijske sigurnosti dodatno povećava.

### 4.4.1. Hijerarhija propisa

Zakonodavni propisi obuhvaćaju široku paletu međunarodnih i nacionalnih zakonskih propisa. Zakonski i podzakonski akti međusobno se hijerarhijski nadograđuju, polazeći od općih prema posebnim propisima, od funkcionalnih prema provedbenim, odnosno od organizacijskih prema tehničkim propisima. Tako razlikujemo međunarodne ugovore kao npr. [48], zakone kao npr. [39], čije donošenje redovito provode državni parlamenti odnosno zakonodavni stup vlasti pojedine države. Po hijerarhiji slijede uredbe kao npr. [59], koje su u nadležnosti izvršne vlasti, odnosno vlade svake pojedine države, te naposljetku pravilnici,

odluke, naputci i smjernice različitih državnih tijela. Pri tome razina pravilnika, odluka, naputaka i smjernica može predstavljati podzakonsku razinu i primjenjivati se na nacionalnoj razini kao npr. [63], ali može predstavljati i interne akte samih državnih tijela za provedbu pojedinih, zakonom propisanih obveza, unutar djelokruga samog državnog tijela kao npr. [64]. Naputci i smjernice kao npr. [65], služe opisivanju preporučenih načina zaštite, primjerice informacijskog sustava, a implementacija mjera definiranih ovakvim preporukama je poželjna, ali nije obvezujuća. U tom smislu dokumenti s preporukama čine fleksibilne elemente regulativnog okvira informacijske sigurnosti, tako da se često koriste na onim mjestima gdje sigurnost nije moguće, nije potrebno, ili nije poželjno strogo definirati. Na slici 4.4 prikazan je primjer nacionalne hijerarhije propisa informacijske sigurnosti u državnom sektoru Republike Hrvatske [3], a vrlo slični okviri regulative informacijske sigurnosti postoje i u primjerima drugih država, odnosno međunarodnih organizacija kao što su NATO ili EU.




**Slika 4.4:** Primjer nacionalne hijerarhije propisa informacijske sigurnosti u državnom sektoru Republike Hrvatske*****

***** kratice na slici 4.4:
NPIS – Nacionalni program informacijske sigurnosti [52],
ZoSOS - Zakon o sigurnosno-obavještajnom sustavu, NN 79/06,
ZTP – Zakon o tajnosti podataka [54],
ZoIS – Zakon o informacijskoj sigurnosti [39],
ZoSP – Zakon o sigurnosnim provjerama, NN 85/08,
UVNS – Ured Vijeća za nacionalnu sigurnost,
ZSIS – Zavod za sigurnost informacijskih sustava,
NCERT – Nacionalni CERT, CARNet

Zakon o informacijskoj sigurnosti [39], prema slici 4.4, koristi pojam „mjere“ za skup obvezujućih zahtjeva koji predstavljaju minimalne sigurnosne mjere u politici informacijske sigurnosti državnog sektora (poglavlje 4.3.3.). Ova razina regulative, prema slici 4.1, predstavlja „normu“, odnosno skup obvezujućih zahtjeva. Zakon prema slici 4.4 koristi i pojam „standardi“, za koji se u radu upotrebljava općenitiji pojam „procedure“ u smislu skupa obvezujućih postupaka za provedbu zahtjeva, odnosno norme (slika 4.1).

Norme općenito predstavljaju dokumente odobrene od mjerodavnog nacionalnog ili međunarodnog tijela za normizaciju koji za opću i višekratnu uporabu daju pravila, upute ili značajke za određenu vrstu aktivnosti ili njihove rezultate, a s ciljem postizanja najboljeg stupnja uređenosti u danom okruženju (prikladnost namjene, optimizacija ograničenjem raznolikosti, spojivost različitih proizvoda, promicanje prednosti za društvo kao što su sigurnost, zaštita zdravlja i okoliša, itd.) [66]. Stoga norme predstavljaju rješenje zajedničkih potreba državne uprave i gospodarstva za jedinstvenim sustavima u području informacijske sigurnosti [27] ili u području vrednovanja informacijske tehnologije [55]. Primjena normi je obvezujuća isključivo u slučajevima kada na njih upućuju odredbe nekog zakonskog ili podzakonskog propisa, kao što je to primjerice u članku 38. Uredbe o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04): „Mjere, postupci i osobe ovlaštene za osiguranje, pohranjivanje i zaštitu sustava određuju se, ostvaruju i provjeravaju prema planu kojeg donosi voditelj zbirke osobnih podataka u skladu s međunarodnim preporukama za to područje (ISO 17799)“. Primjerci međunarodnih i nacionalnih normi, u najvećem broju slučajeva se kupuju i podliježu zaštiti autorskih prava, a certificiranje po tim normama mogu provoditi samo institucije akreditirane od nadležnog normizacijskog tijela. Kao što je već pojašnjeno, internu reviziju najčešće obavljaju zaposlenici organizacije koja provodi normu, a takav pristup dosta je često prisutan u slučaju provedbe normi informacijske sigurnosti.

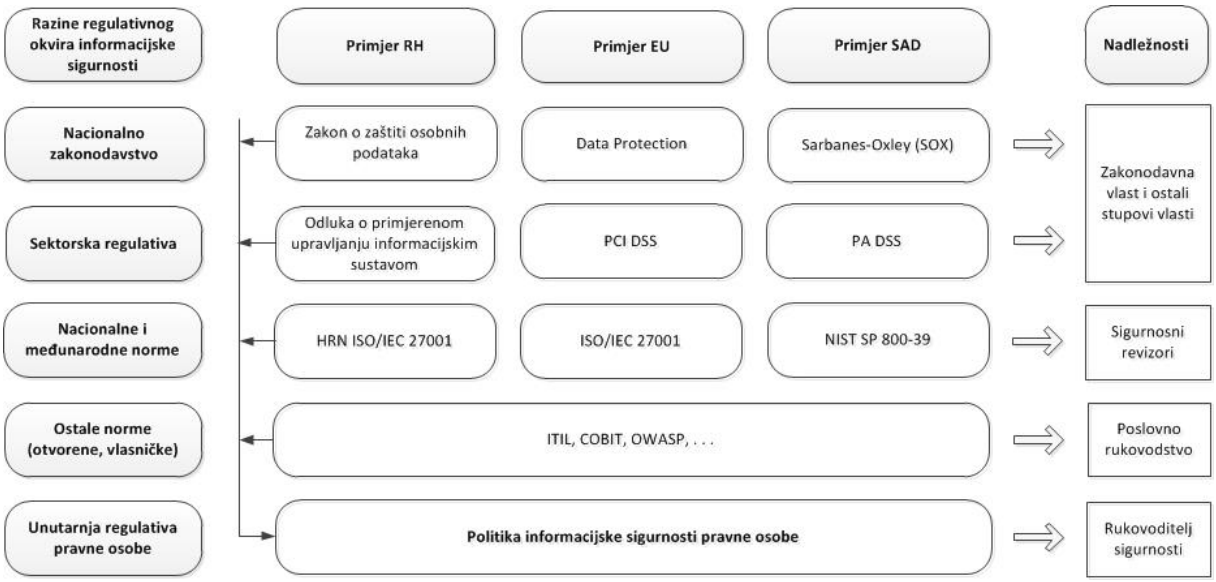
Osim međunarodnih i nacionalnih normi koje donose ovlaštena normizacijska tijela, postoje i interne norme koje predstavljaju dokumente pojedine organizacije ili skupine organizacija, namijenjene za bilo koju vrstu njihove unutarnje uporabe (npr. normiranje nekih unutarnjih ili zajedničkih poslovnih procesa). Nadalje, postoje i otvorene norme za slobodnu javnu uporabu (npr. IETF, RFC dokumenti) [67]. Otvorene norme sve su više prisutne u području informacijske tehnologije. Razlog tome je u iznimno velikoj dinamici razvoja, ali i složenosti informacijske tehnologije. Tradicionalni pristup normizaciji kroz proces usklađivanja u

tehničkim odborima normizacijskog tijela i kroz preuzimanje različitih međunarodnih normi u području informacijske tehnologije za nacionalnu uporabu (ISO, IEC, CEN, ETSI i druge), zbog dinamike razvoja informacijske tehnologije pokazao se nedostatnim. Stoga se u novije vrijeme u području informacijske tehnologije najčešće koriste različite otvorene norme, vlasničke norme (eng. *Proprietary*) ili *de-facto* norme, odnosno norme koje su se nametnule masovnim korištenjem nekog proizvoda. S obzirom da model vlasničkih normi počiva na interesnoj grupaciji tvrtki koje usuglašavaju ili preuzimaju zajedničku privatnu normu (npr. tehnologije nasljednici DVD medija: Blue-ray disk i HD-DVD), takav pristup može dovesti do tržišne polarizacije, selektivnosti i netransparentnosti, odnosno do ograničenja tržišnog natjecanja te je stoga poželjna inicijativa državnog sektora usmjerena na poticanje otvorenih normi i procesa normizacije kao npr. u [52].

Pored navedenih vrsta regulativnih propisa, potrebno je razlikovati i specifičnosti tzv. sektorske regulative ili regulative vertikale poslovanja, kojom se na određeni način reguliraju, odnosno postavljaju, zahtjevi koje moraju provesti sve pravne osobe koje se bave određenom vrstom djelatnosti, kao što je primjerice bankovni sektor ili sektor zaštitarske djelatnosti. Sektorsku regulativu mogu predstavljati neki od prethodno obrađenih slojeva u hijerarhiji propisa (zakoni, norme ili njihova kombinacija). Jedan od najreguliranijih sektora u smislu informacijske sigurnosti svakako je bankovni sektor. Može se reći da su vršni dokumenti sektorske regulative u bankovnom sektoru dokumenti Basel norme [56] koji u stvari predstavlja međunarodnu bankovnu normu koju je kreirao Bazelski odbor za bankovni nadzor (engl. *Basel Committee on Banking Supervision – BCBS*). BCBS se sastoji od predstavnika središnjih banaka i bankovnih regulatora iz nekoliko EU država, Japana i SAD-a, koji potiču međunarodnu kooperaciju banaka i izdaju smjernice za nadzor banaka. Iako aktualna inačica Basel norme nije zakon, njezini zahtjevi preuzimaju se u zakonodavstvima velikog broja država u svijetu (npr. EU direktive 2006/48/EC, 2006/49/EC, koje su obvezujuće za sve države članice EU) i propisuju se kroz različite nacionalne propise koji mogu biti zakoni, uredbe ili pravilnici, odnosno odluke središnjih banaka kao nadležnih tijela.

Važnost opisane hijerarhije propisa je u tome što primjenjivi propisi izravno utječu i na formu i na sadržaj politika informacijske sigurnosti koje se provode u određenim organizacijama, bilo u državnom, bilo u poslovnom sektoru. Na slici 4.5 prikazan je utjecaj različitih razina hijerarhije propisa, odnosno regulativnog okvira informacijske sigurnosti na lokalnu politiku informacijske sigurnosti neke pravne osobe [3]. Pri tome su uzeti u obzir neki tipični primjeri

regulative i normi koji su prikazani po različitim razinama za područja RH, EU i SAD. Na desnoj strani slike 4.5 pokazana je načelna organizacijska nadležnost za pojedine razine u hijerarhiji propisa.




**Slika 4.5:** Utjecaj različitih razina regulativnog okvira informacijske sigurnosti na razvoj lokalne politike informacijske sigurnosti neke pravne osobe u različitim okruženjima RH, EU i SAD-a*****

***** kratice na slici 4.5:
PCI DSS – Payment Card Industry Data Security Standard,
PA DSS – Payment Application Data Security Standard,
NIST – U.S. National Institute of Standards and Technology ,
ITIL – Information Technology Infrastructure Library,
COBIT – Control Objectives for Information Technology,
OWASP – Open Web Application Security Project

U poglavlju 4.1 već je pojašnjeno značenje pojma politika informacijske sigurnosti, te su na slici 4.1 prikazane tipične hijerarhijske razine skupa dokumenata politike informacijske sigurnosti. U smislu povezanosti politike informacijske sigurnosti sa širom hijerarhijom propisa pojašnjenja su dana u ovom poglavlju i na slici 4.5. Potreba donošenja dokumenata politike informacijske sigurnosti uobičajeno proizlazi iz zakonskih obaveza ili vlastite poslovne inicijative određene pravne osobe. Politika informacijske sigurnosti pri tome se najčešće raščlanjuje na više slojeva, pa prema [44] obično razlikujemo:

1. opće politike – na razini organizacije u cijelosti (npr. vršni dokument politike informacijske sigurnosti);
2. funkcionalne politike - po određenim područjima (npr. sigurnost osoblja), politike prihvatljivog korištenja (engl. *Acceptable Use Policy – AUP*) pojedinih resursa (npr. poslovno korištenje Interneta);

3. specifične politike - obrađuju određenu specifičnu problematiku ili aplikaciju (npr. povrede sigurnosti).

### 4.4.2. Etička načela

Informacijska sigurnost u velikoj se mjeri temelji na zakonskim i drugim propisima koji osiguravaju uređeni okvir za uspostavu i upravljanje sustavom informacijske sigurnosti u određenom okruženju [3]. Zbog složenosti ljudskog ponašanja i odnosa u društvu, propisi nisu uvijek odgovarajući način za rješavanje problematike postupanja osoba u nekim aspektima njihovog rada. Stoga sve aspekte sigurnosti niti je moguće u potpunosti regulirati, niti bi ih se u praktičnom smislu moglo pravno procesuirati, posebice u slučajevima kada pojedini propisi daju mogućnosti za različita tumačenja ili ostavljaju prostor nepotpuno uređenim u nekom poslovnom segmentu (npr. uporaba privatne programske podrške na poslovnim računalima, ili uporaba programske podrške koja ima licence za besplatno korištenje fizičkih osoba na računalima pravne osobe i sl.) [68]. U tom smislu, u određenim slučajevima koristi se etika, kao sustav vrijednosti i poželjnog ponašanja, te se definiraju opće norme prihvatljivog ponašanja, odnosno objektivno definirane norme dobrog i lošeg ponašanja – etički kodeks.

U osnovi postoje dva načina etičkog pristupa: pristup zasnovan na posljedici (teleologija) i pristup zasnovan na pravilu (deontologija), pri čemu oba načina mogu biti promatrana u individualnom kontekstu (osoba - egoizam) ili univerzalnom kontekstu (društvo - utilitarizam) [68]. Etički kodeksi obično se utvrđuju za određeni profil zaposlenika ili određenu organizaciju (npr. Etički kodeks državnih službenika, NN 49/06, ili etički kodeks u [69]), te predstavljaju kombinaciju etičkih pristupa prilagođenih kontekstu za koji su namijenjeni (u primjeru: državni službenici u Republici Hrvatskoj, odnosno strukovna udruga stručnjaka sigurnosti informacijskih sustava).

Sa stanovišta mogućih sankcija za različite vrste povreda sigurnosti (engl. *Breach of Security*), u regulativnom okviru razlikujemo:

- kršenje odredbi propisanih zakonskim propisima - za što su propisane kaznene i prekršajne sankcije,
- kršenje odredbi propisanih unutarnjim aktima pojedinih institucija - za što se provode interni stegovni postupci.

U slučaju povreda sigurnosti vezanih za poslovnu tajnu u nekoj pravnoj osobi, može se raditi o kombinaciji unutarnjeg stegovnog postupka i kaznenog postupka, jer se radi o povredi internog propisa koji koristi mehanizam kazneno-pravne zaštite iz područja intelektualnog vlasništva. Slična situacija može postojati i u slučaju državnih službenika, za koje se u nekim slučajevima mogu voditi paralelni stegovni i kazneni postupak.

Za razliku od ovih primjera za povrede sigurnosti, osnovno načelo etičkog kodeksa je postavljanje okvira za razmatranje etičnosti postupanja pojedinca koji je, primjerice, ulaskom u strukovnu udrugu, ili zaposlenjem, prihvatio obvezu poštivanja određenog etičkog kodeksa. Iako sličnog naziva, prethodno navedeni primjeri dva etička kodeksa bitno se razlikuju. Etički kodeks državnih službenika samo proširuje okvire u kojima je moguće prepoznati i utvrditi kršenje drugih postojećih propisa koje državni službenici moraju poštivati. Etički kodeks $ISC^2$ organizacije uobičajen je za strukovne organizacije (profesionalna etika) i sadrži u sebi potpunu proceduru procesuiranja etičkih sukoba kroz uspostavu etičkih sudova, mogućnost prijavljivanja etičkih sukoba, procesuiranje pojedinačnih slučajeva kršenja etičkih načela te stegovno kažnjavanje članova strukovne organizacije kojima je utvrđeno kršenje odredbi etičkog kodeksa, sukladno pravilima određene strukovne organizacije.

## 4.5. Kibernetički prostor i regulativni okvir informacijske sigurnosti

Na temelju zaključka iz poglavlja 4.2.2., o povezanosti segmenata informacijskog prostora, kao ključni elementi utjecaja informacijskog prostora na politike informacijske sigurnosti prepoznate su domene podataka koje predstavljaju sastavni dio informacijskog prostora i globalne komunikacijsko-informacijske infrastrukture (kibernetički prostor). Nadalje su u poglavlju 4.4. razmatrani regulativni okvir informacijske sigurnosti, odnosno hijerarhija različitih vrsta propisa koji imaju izravni utjecaj na sigurnosne zahtjeve politika informacijske sigurnosti koje se provode u pojedinim organizacijama.

U ovom poglavlju analizira se kibernetički prostor uz pomoć regulativnog pogleda i povezanosti tako dobivenog regulativnog okvira kibernetičkog prostora s regulativnim okvirom informacijske sigurnosti prikazanim u poglavlju 4.4. Razlog potrebi detaljnog regulativnog pogleda vidljiv je sa slike 4.5, odnosno proizlazi iz stanja u kojem sve veći broj zahtjeva u suvremenim politikama informacijske sigurnosti dolazi iz različite vrste regulative, pa tako primjerice prema [27] osnovni zahtjev za provedbu norme ISO27001 predstavlja

analiza poslovnih zahtjeva, zakonskih i regulativnih zahtjeva te ugovornih sigurnosnih zahtjeva. U prethodnom poglavlju utvrđena je visoka složenost regulativne hijerarhije i različitih vrsta propisa informacijske sigurnosti te se može reći da procjenjivanje potrebe primjene određene regulative najčešće nije jednostavan zadatak, jer se radi o regulativi koja ne spada u opću pravnu regulativu, a ne pripada niti isključivo tehničko-normativnom segmentu pa najčešće traži multidisciplinaran pristup. Upravo stoga, jedan od ciljeva modeliranja u ovom radu je osigurati odgovarajuću taksonomijsku razradu i za ovo područje regulativnih zahtjeva koji danas čine veliki dio suvremenih sigurnosnih zahtjeva, sa stalno prisutnim trendovima povećanja, osobito u dijelu regulative kibernetičkog prostora koji se analizira u ovom poglavlju.

U cilju stvaranja šire slike regulativnog okvira i rješavanja potreba za daljnjom raščlambom regulative, potrebno je razmotriti temeljne informacijske kriterije koji se mogu grupirati u tri skupine [2]:

1. sigurnosni informacijski kriteriji (povjerljivost, cjelovitost i raspoloživost);
2. informacijski kriteriji povjerenja (sukladnost i pouzdanost);
3. informacijski kriteriji kvalitete (učinkovitost i efikasnost).

Tradicionalna politika informacijske sigurnosti usmjerena je prvenstveno na sigurnosne informacijske kriterije. S druge strane, suvremeno informacijsko društvo sve više promatra informacije u okviru intelektualnog vlasništva koje ima sličnu ulogu u društvu, kakvu je tržišna ekonomija uspostavila za privatno vlasništvo. To znači da u suvremenom društvu koje je nedjeljivo od kibernetičkog prostora, nije moguće informacije izolirati, već se njima nužno mora svakodnevno komunicirati i razmjenjivati ih, te je stoga nemoguće razdvojiti koncepte sigurnosti podataka i sigurnosti kibernetičkog prostora preko kojeg se tim podatcima komunicira. Analogija pristupa sigurnosti kibernetičkog prostora, kao još jednoj dimenziji tradicionalnog života i društva, sve je vidljivija u novim strategijama kibernetičke sigurnosti, primjerice na razini EU u [70]. U poglavlju 4.2.2. već je prethodno izveden zaključak o bitnom utjecaju domena podataka i globalne komunikacijsko-informacijske infrastrukture na politike informacijske sigurnosti. Može se zaključiti da su i politike informacijske sigurnosti u smislu njihove definicije u ovom radu, kao koncept nedjeljive od sigurnosti podataka i sigurnosti kibernetičkog prostora, jednako kao što su ova dva koncepta međusobno nedjeljiva u okvirima suvremenog društva.

Proširenje zahtjeva suvremenog informacijskog društva na komuniciranje i razdiobu informacija (engl. *Responsibility-to-Share*), kao načelo postupanja, tijekom proteklog desetljeća utjecalo je i na politike informacijske sigurnosti državnog sektora [71]. Odgovornost za razdiobu klasificiranih podataka, za sve osobe koje imaju poslovnu potrebu pristupa klasificiranim podatcima, sa stanovišta ovog rada i konceptualizacije politika informacijske sigurnosti, uvodi znatno više kriterije za osoblje. Prema hijerarhiji pojmova: podatak - informacija - znanje - mudrost, kao i prema definiciji koja je uvedena u poglavlju 2.4, mudrost je viša razina razumijevanja o tome koje znanje se koristi i s kojom namjerom, odnosno podrazumijeva dvije razine znanja: razinu poznavanja i razinu razumijevanja. Ova definicija je dodatno razrađena u poglavlju 3.2, gdje je, na temelju stanja politike informacijske sigurnosti u okviru šireg domenskog prostora, uočeno da je stanje razvoja došlo do faze znanja u kojem je veliki broj informacija uobličen u odgovarajuće proceduralne naputke za postupanje (znanje), no viša razina mudrosti u smislu razumijevanja korištenja takvih procedura na višoj domenskoj razini, nalazi se u početnoj fazi istraživanja. Ovdje se može reći da spomenuti viši kriteriji za osoblje i pojedine poslovne procese, vezani uz odgovornost za razdiobu podataka, traže ne samo poznavanje procedura postupanja (znanje), već i razumijevanje svrhe takvih procedura u širem domenskom okruženju (mudrost).

Vezano uz prethodno tumačenje, može se postaviti više povezanih pitanja o tome jesu li se uvođenjem novog načela odgovornosti za razdiobu podataka u politikama informacijske sigurnosti osigurale pretpostavke za provedbu viših kriterija znanja i razumijevanja odgovornog osoblja. Mogu li neformalno specificirane politike informacijske sigurnosti, u obliku niza tekstualnih nestrukturiranih dokumenata, vrlo složenog i usko povezanog sadržaja, uopće odgovoriti zahtjevima kao što je ovaj, u kojem je ulogu osoba potrebno promatrati višedimenzionalno prema [6]? Upravo ovakva, slaba koordinacija uvođenja novih načela u sustav u kojem su temeljni čimbenici kao i područja politika informacijske sigurnosti međusobno usko povezani i utječu jedni na druge, kako je to naglašeno u poglavlju 1.2, predstavlja motivaciju ovog istraživanja, odnosno upućuje na potrebu sveobuhvatnijeg i formalnijeg pristupa području politika informacijske sigurnosti.

Zahtjevi poslovne suradnje i razdiobe podataka preko kibernetičkog prostora dovode do potrebe korištenja, ne samo sigurnosnih informacijskih kriterija, već i kriterija povjerenja i kvalitete. Sigurnosni kriteriji povjerljivosti, cjelovitosti i raspoloživosti bili su dovoljni za zatvorene klasificirane informacijske sustave, za razliku od otvorenog kibernetičkog prostora

u kojemu se kao nužni kriteriji pojavljuju kriteriji povjerenja (npr. koncept elektroničkog potpisa i ovlaštenog davatelja certifikata, engl. *Certificate Authority – CA*) i kriteriji kvalitete (npr. ugovori o razini usluge, engl. *Service Level Agreements – SLA*).

### 4.5.1. Regulativni okvir kibernetičkog prostora

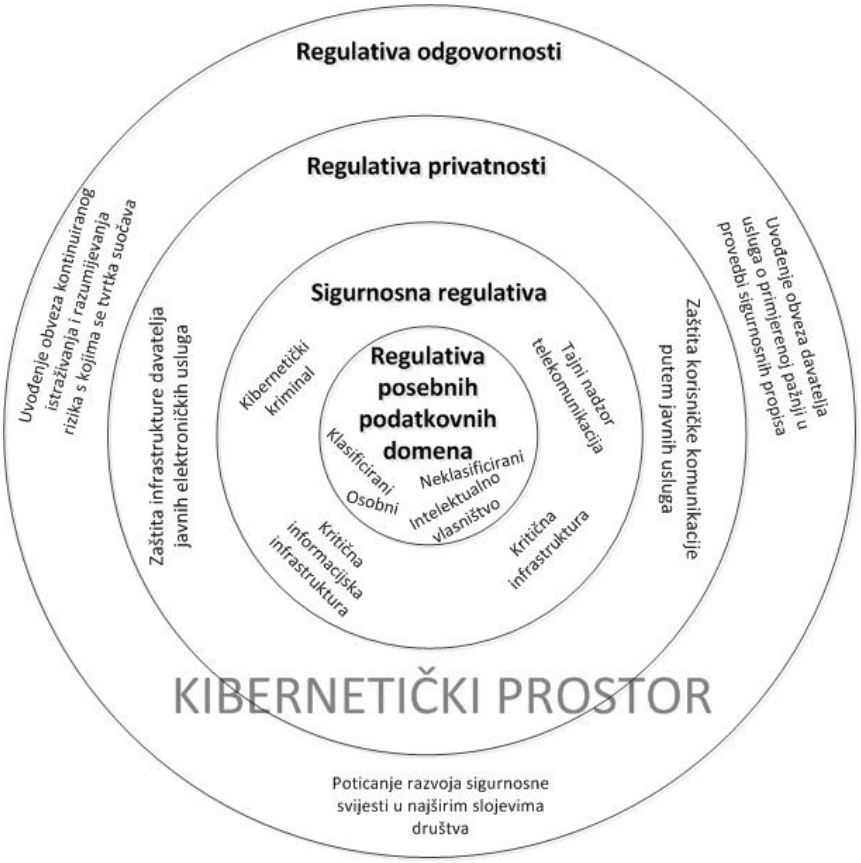
U širem kontekstu kibernetičkog prostora, svrha regulativnog okvira informacijske sigurnosti jest osigurati odgovarajuće preduvjete za komuniciranje, odnosno za primjenu sigurnosnih informacijskih kriterija na kibernetički prostor, ali i na regulativu koja ga uređuje [5]. U poglavlju 4.2., na slici 4.2, prikazane su vrste podataka za koje se može reći da su dominantne s obzirom na zahtjeve informacijske sigurnosti, jer imaju izravan utjecaj na sadržaje politika informacijske sigurnosti. Za potrebe opisa regulative kibernetičkog prostora, ovu kategoriju regulative koja regulira domene klasificiranih podataka, osjetljivih podataka, osobnih podataka i intelektualnog vlasništva, prema [5] naziva se regulativa posebnih podatkovnih domena. U osnovi se radi o regulativnom okviru informacijske sigurnosti državnog sektora prema slici 4.4, koji je proširen regulativom zaštite osobnih podataka i intelektualnog vlasništva u širem smislu. Svrha regulative posebnih podatkovnih domena je osigurati sigurnosne zahtjeve određenih vrsta podataka sa svim njihovim specifičnostima, dok je svrha sveukupne regulative kibernetičkog prostora osigurati minimalne sigurnosne zahtjeve za komunikaciju ovim podatcima u otvorenom kibernetičkom prostoru.

Regulativni okvir kibernetičkog prostora promatra se u kontekstu sve tri prethodno uvedene skupine informacijskih kriterija. Ovaj regulativni okvir predstavlja nadgradnju regulativnog okvira informacijske sigurnosti državnog sektora iz poglavlja 4.4.1., slika 4.4. Koristi se podjela regulativnog okvira kibernetičkog prostora na segmente prikazane na slici 4.6 [5]:

1. regulativa posebnih podatkovnih domena;
2. sigurnosna regulativa;
3. regulativa privatnosti;
4. regulativa odgovornosti.

Ovakva podjela ističe ranije spomenute i opisane prioritete informacijskih kriterija. U okviru sigurnosne regulative primarno se promatra regulativa koja se bavi sigurnosnim informacijskim kriterijima. U okviru regulative privatnosti obuhvaća se regulativa koja se primarno bavi kriterijima povjerenja i kvalitete, dok se u okviru regulative odgovornosti promatra regulativa koja se primarno usmjerava na problematiku odgovornosti u

informacijskom prostoru, sukladno tumačenju iz poglavlja 4.4., o načelu svijesti o rizicima poslovanja, odnosno načelu primjerene pažnje. Na slici 4.6, u središnjem dijelu je prikazana regulativa posebnih podatkovnih domena, koja se odnosi na podatke dominantne s obzirom na zahtjeve informacijske sigurnosti, grupirane u četiri kategorije uvedene u poglavlju 4.2. (klasificirani podatci, osjetljivi podatci, osobni podatci, intelektualno vlasništvo), a koji predstavljaju regulativni okvir informacijske sigurnosti državnog sektora (slika 4.4), proširen regulativom zaštite osobnih podataka i intelektualnog vlasništva u širem smislu (poglavlja 4.9.1. i 4.9.2.).




**Slika 4.6:** Podjela regulativnog okvira kibernetičke sigurnosti

Kibernetički prostor u suvremenom smislu obuhvaća sve ključne sektore društva: državni sektor, poslovni sektor i sektor građanstva. Stoga se najveći broj zahtjeva koji se postavlja pred organizaciju suvremenog društva, počevši od uvođenja osobnog identifikacijskog broja građana, preko transparentnosti redova čekanja u bolnicama, registra Trgovačkog suda s pravnim subjektima registriranim za poslovanje u državi, elektroničkih usluga državne uprave (engl. *e-Government*), registra obveznika kredita i slično, izravno ili neizravno naslanja na kibernetički prostor i zahvaća neko od ograničenja prethodno uvedenih preko regulative

posebnih podatkovnih domena. Time se u stvari postavljaju sigurnosni zahtjevi i prema samom kibernetičkom prostoru. Dakle, korištenjem podataka dominantnih s obzirom na zahtjeve informacijske sigurnosti, u okruženju kibernetičkog prostora, mijenja se kontekst u kojem se podatci primjenjuju, a time i skupina prijetnji i rizika, zbog međusobne interakcije novih i različitih prijetnji iz kibernetičkog prostora. Na taj način je nastala situacija u kojoj se zbog promjene okruženja u kojem komuniciramo istim domenama podataka, mora mijenjati sigurnosnu metodu pristupa, kako bi se postigli politikom informacijske sigurnosti zacrtani ciljevi, iako se sami ciljevi, primjerice u slučajevima tradicionalno prisutnih domena podataka kao što su klasificirani podatci, nisu bitno promijenili tijekom posljednjih desetljeća. Ovaj zaključak predstavlja važan zahtjev za modeliranje politika informacijske sigurnosti u ovom radu, jer sadržaj modela koji se razvija mora odraziti ne samo dominantne vrste podataka s obzirom na zahtjeve informacijske sigurnosti, već i kontekst njihove suvremene primjene (globalno okruženje kibernetičkog prostora).

Unatoč tome što se opisana promjena okruženja, odnosno stvaranje kibernetičkog prostora, događa u relativno kratkom razdoblju od posljednjih dvadesetak godina, promjene su iznimno velike. Primjerice, tijekom druge polovine 90-tih godina prošlog stoljeća procesi poput liberalizacije telekomunikacijskog sektora, uvelike su promijenili pristup državnih tijela najmu komunikacijskih kapaciteta ili području tajnog nadzora telekomunikacijskih usluga [58]. Nadalje, nastajanje projekata elektroničke državne uprave, kao okosnice otvaranja državne vlasti prema građanstvu i slijedna tendencija povezanosti državne uprave, gospodarstva i građanstva, na potpuno novi način otvara međuodnose ovih društvenih sektora. Dolazi i do razvoja internetskih usluga, osobito financijskih usluga i elektroničke trgovine, te pratećih pokušaja zaštite osobnih podataka koji, poprimajući nove oblike elektroničkih osobnih identiteta, postaju sve više izloženi novim prijetnjama kibernetičkog prostora. Regulativni okvir, da bi odgovorio na promjenu okruženja, ne može postavljati zahtjeve samo prema vlasnicima podataka koji su korisnici informacijskog prostora, i ne samo s obzirom na potrebne mjere koje ti vlasnici moraju primjenjivati u svrhu zaštite pojedinih vrsta podataka kojima komuniciraju. Regulativa mora postavljati zahtjeve i prema samom kibernetičkom prostoru, kao i prema subjektima koji ostvaruju kibernetički prostor, u smislu davanja usluga, odnosno infrastrukture, ali i prema samim korisnicima usluga i podataka.

S gledišta politika informacijske sigurnosti koje se provode u različitim organizacijama može se uočiti izravni utjecaj regulativnog okvira informacijske sigurnosti na njihove sadržaje

(hijerarhija propisa iz poglavlja 4.4.1., domene podataka iz poglavlja 4.2. i središnji dio regulative kibernetičkog prostora prema slici 4.6). Neizravni utjecaj regulativnog čimbenika na sadržaje informacijske sigurnosti, prisutan je uglavnom iz tri vanjska sloja regulativnog okvira kibernetičkog prostora prema slici 4.6 i očituje se u različitim utjecajima, od sigurnosnih zahtjeva, preko zahtjeva privatnosti, do regulative odgovornosti te u poglavlju 4.4. pojašnjenih načela primjerene pažnje i načela svijesti o rizicima poslovanja. Potrebno je napomenuti da ovisno o vrsti organizacije koja provodi politiku informacijske sigurnosti, neki od ovdje naznačenih neizravnih utjecaja, mogu biti i izravni regulativni zahtjev, primjerice za slučaj davatelja elektroničkih komunikacijskih usluga, koji može biti izravni obveznik primjene zahtjeva iz više slojeva regulativnog okvira sa slike 4.6.

## 4.6. Dominantne norme i politike informacijske sigurnosti

Za potrebe analize šire domenske razine područja informacijske sigurnosti, u ovom se istraživanju koristi skup dominantnih politika i normi informacijske sigurnosti u suvremenom poslovanju. Pri tome se odabir ovog skupa dominantnih politika i normi ne vrši unutar jednog od sektora društva, već se odabirom skupa želi obuhvatiti širu domensku razinu, kako bi se proces modeliranja što više poopćio i mogao biti primjenjiv na različite profile organizacija koje provode politiku informacijske sigurnosti, a osobito na slučajeve međusobne suradnje organizacija, koje pripadaju primjerice državnom i poslovnom sektoru. U prethodnom dijelu poglavlja 4. definirani su neki važniji pojmovi kao i pojam informacijske sigurnosti, prikazana je i analizirana povijest razvoja suvremenih politika i normi informacijske sigurnosti, ključne domene podataka koje su utjecale na razvoj i oblikovanje suvremenih politika i normi informacijske sigurnosti, obilježja regulativnih okvira informacijske sigurnosti, utjecaj globalne informacijske i komunikacijske tehnologije na oblikovanje i trendove razvoja politika i normi, zatim povezanost kibernetičkog prostora, domena podataka dominantnih s obzirom na zahtjeve informacijske sigurnosti kao i najvažnija obilježja suvremenih politika i normi informacijske sigurnosti.

Na temelju ove analize razvidno je da jedan od najzastupljenijih profila organizacija u području informacijske sigurnosti, predstavljaju različite organizacije koje pripadaju državnom sektoru neke zemlje, odnosno međunarodnim organizacijama kao što su NATO ili EU. Prema slici 4.3, prikazan je izravni međusobni utjecaj u razvoju politika informacijske sigurnosti državnih sektora razvijenih zemalja, kao i međunarodnih organizacija, NATO-a i

EU-a, te su i njihova suvremena obilježja, osobito u domeni klasificiranih podataka, vrlo slična i u najvećoj mjeri međusobno sukladna. Tako primjerice politika informacijske sigurnosti Vijeća EU [73], predstavlja osnovu za donošenje politika u svim institucionalnim stupovima EU-a (Vijeće EU, Europska Komisija, Europska služba vanjskih poslova - EEAS), pri čemu i Europska Komisija i Europska služba vanjskih poslova, kao i pojedine EU agencije u njihovoj odgovornosti (npr. *Europol*, *European GNSS Agency* i sl.), donose vlastitu provedbenu politiku na temelju [73]. Pored toga i zemlje članice EU-a usklađuju svoje nacionalne politike informacijske sigurnosti, sukladno obvezama preuzetim odgovarajućim međunarodnim ugovorima, kao što je npr. [74]. Slično se može reći i za NATO politiku informacijske sigurnosti [75], koja se također primjenjuje u odgovarajućem provedbenom obliku na pojedina civilna i vojna tijela NATO-a, a odgovarajućim međunarodnim ugovorima prenose se obveze usklađivanja minimalnih sigurnosnih mjera i na zemlje članice NATO-a [48], odnosno na druge zemlje partnere NATO-a. Daljnja obilježja ove velike i dominantne grupe politika informacijske sigurnosti državnog sektora analizirat će se preko važnijih načela koja se koriste u ovim politikama informacijske sigurnosti, kao i preko važnijih normi koje se koriste u području informacijske sigurnosti i u državnom i u poslovnom sektoru.

Prema slici 4.3, norma ISO 27001 [27], također je povijesno vrlo usko povezana s politikama informacijske sigurnosti državnog sektora. Primjena ove norme informacijske sigurnosti uobičajena je i u državnom sektoru i u poslovnom sektoru. Tako se prema [59] na ovu normu referira zakonodavac prilikom propisivanja sigurnosnih zahtjeva za državni sektor Republike Hrvatske u segmentu zaštite službenih podataka, odnosno neklasificiranih označenih podataka koji ne spadaju u kategoriju tajnih, već osjetljivih podataka. Slično tome i sigurnosne smjernice financijskog sektora u mnogim zemljama zasnovane su na ovoj normi [65], jednako kao i smjernice sektora javnih elektroničkih komunikacija i usluga [76], odnosno propisi zaštite osobnih podataka [77]. Stoga će se obilježja politika informacijske sigurnosti u poslovnom sektoru promatrati prvenstveno preko obilježja ove dominantne norme ISO 27001, za koju je u prethodnoj analizi u ovom poglavlju već pojašnjena mogućnost različitog načina primjene. Primjena ove norme je uobičajena u obliku certificiranja organizacija (vanjska neovisna revizija ovlaštenog tijela), u obliku interne revizije (unutarnja revizija koju provodi sama organizacija), odnosno u obliku smjernica s najboljom sigurnosnom praksom [41, 78, 79]. Moguće je i kombiniranje primjene norme ISO 27001 u okviru različitih sigurnosnih zahtjeva propisanih zakonskim [39, 59] ili sektorskim regulativnim zahtjevima [76].

## 4.7. Važnija načela u politikama informacijske sigurnosti

S obzirom na potrebe modeliranja politika informacijske sigurnosti u ovom radu, potrebno je analizirati važnija načela koja se koriste u suvremenim politikama informacijske sigurnosti. Analiza se stoga usmjerava na način korištenja, međusobnu povezanost i sličnost nekih načela, kao i njihovu povezanost s važnijim metodama poput metode upravljanja rizikom. Modeliranje ovih načela usko je povezano s razradom organizacije i strukture modela politika informacijske sigurnosti koji se ovim radom ostvaruje.

### 4.7.1. Odgovornost i koncept vlasnika imovine ili rizika

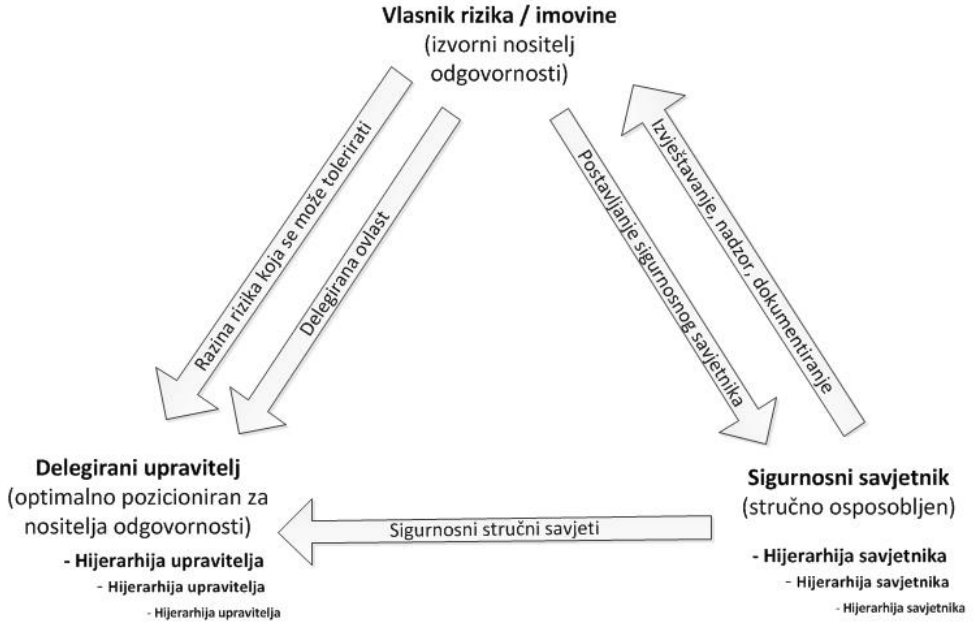
Temeljno načelo u metodama upravljanja rizikom jest načelo pridruživanja odgovornosti za rizik entitetu koji je najbolje pozicioniran za upravljanje rizikom. Važnost ovog načela već je opisana u poglavlju 4.4., u okviru analize šireg regulativnog okvira informacijske sigurnosti. Ovo načelo važno je i u tradicionalnoj politici informacijske sigurnosti državnog sektora i u suvremenim normama kao što je ISO 27001. Načelo odgovornosti uobičajeno se provodi na organizacijskoj razini. Cilj provedbe ovog načela može biti opća zaštita određene imovine kao što su podatci, ili informacijski sustavi, ali i mogućnost uvođenja decentralizacije u odlučivanju o pristupu klasificiranim podatcima, čime se postiže bolja operativnost i fleksibilnost potrebna u praktičnim primjenama politika informacijske sigurnosti. Primjena ovog načela i određivanje vlasnika imovine spada u provedbu prije spomenutog šireg regulativnog načela primjerene pažnje (poglavlje 4.4.) i usko je povezano s politikama informacijske sigurnosti. Cilj provedbe ovog načela može također biti odgovornost za sigurnosne rizike, a takvo određivanje vlasnika rizika spada u provedbu prije spomenutog šireg regulativnog načela svijesti o rizicima poslovanja (poglavlje 4.4.) te je usko povezano s metodama upravljanja rizikom.

U osnovi, ovakav model organizacije sastoji se od prepoznavanja vlasnika imovine ili rizika (izvorni nositelj), delegiranog upravitelja (zainteresirani nositelj) te sigurnosnog savjetnika (stručno osposobljeni savjetnik) [80]. Vlasnik imovine ili rizika utvrđuje model organizacije u okviru kojega mora:

- definirati rizik ili imovinu, odnosno procijeniti razinu rizika koju može prihvatiti (engl. *Risk Apetite*), što spada u metodu upravljanja rizikom, ili odrediti kriterije upravljanja imovinom, što spada u politiku informacijske sigurnosti,
- odrediti delegiranog upravitelja;

- uključiti se u provođenje postupka odabira sigurnosnog savjetnika.

Delegirani upravitelj provodi upravljanje u granicama koje zadaje vlasnik imovine ili rizika, pri čemu dobiva stručne savjete sigurnosnog savjetnika. Opisani međuodnos vlasnika imovine ili rizika, delegiranog upravitelja i sigurnosnog savjetnika prikazan je na slici 4.7 [53]. Vidljivo je da se ovaj odnos može proširivati po horizontali tako da vlasnik određuje više delegiranih upravitelja (npr. za različite vrste podataka ili informacijskih sustava), odnosno po vertikali, tako da se odredi daljnja decentralizirana organizacijska hijerarhija kojom upravlja delegirani upravitelj, a paralelno s njom i hijerarhija pridruženih sigurnosnih savjetnika.




**Slika 4.7:** Načelo pridruživanja odgovornosti za upravljanje rizikom i imovinom

Kao primjer ovog načela može se uzeti i koncept zakonske regulative informacijske sigurnosti u državnom sektoru Republike Hrvatske, koji prati opisana organizacijska načela odgovornosti. Tako primjerice Zakon o tajnosti podataka [54] i Zakon o informacijskoj sigurnosti [39], utvrđuju odgovornost središnjeg državnog tijela za informacijsku sigurnost (engl. *National Security Authority – NSA*), odnosno Ureda Vijeća za nacionalnu sigurnost (UVNS), za koordinaciju i usklađivanje donošenja i primjene mjera informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka sa drugim državama i međunarodnim organizacijama. Odgovornost za postupanje s klasificiranim podatcima u državnim tijelima dalje se prenosi na čelnike tih državnih tijela. U tu svrhu čelnik UVNS-a kontrolira taj proces „delegiranja odgovornosti“ donoseći pravila za postavljanje savjetnika za informacijsku sigurnost u državnim tijelima [81]. Uloga savjetnika za informacijsku sigurnost u državnim tijelima je dvojaka, jer su oni podređeni čelniku državnog

tijela i savjetuju ga u pitanjima informacijske sigurnosti, međutim istovremeno su strukovno odgovorni nadležnom središnjem državnom tijelu za informacijsku sigurnost – UVNS-u. Na temelju tako postavljene odgovornosti, savjetnici za informacijsku sigurnost provode unutarnji nadzor informacijske sigurnosti državnog tijela, o kojem izvještavaju i čelnika državnog tijela i čelnika UVNS-a.

Načelo pridruživanja odgovornosti za rizik organizacijskom entitetu najbolje pozicioniranom za upravljanje rizika, može se prepoznati i u drugim segmentima politika informacijske sigurnosti. Primjerice, jedan od čestih slučajeva je da se proces upravljanja rizikom provodi u središnjoj instituciji, a decentralizirani organizacijski segmenti provode ovaj proces prema potrebi i pod određenim uvjetima, dok obavezno moraju provesti definirani skup minimalnih sigurnosnih mjera. U ovom slučaju, prema terminologiji sa slike 4.7, radi se o procjeni vlasnika rizika za uspostavu sigurnosnih mjera u decentraliziranoj jedinici. Ova procjena može ići u smjeru procjenjivanja rizika u središnjoj instituciji i primjene rezultata na decentralizirane organizacijske segmente u obliku definiranog skupa minimalnih sigurnosnih mjera ili u smjeru delegiranja ovlasti za procjenjivanje rizika u lokalnom, decentraliziranom okruženju i lokalnom odlučivanju o primjeni sigurnosnih mjera za smanjivanje tako procijenjenih rizika.

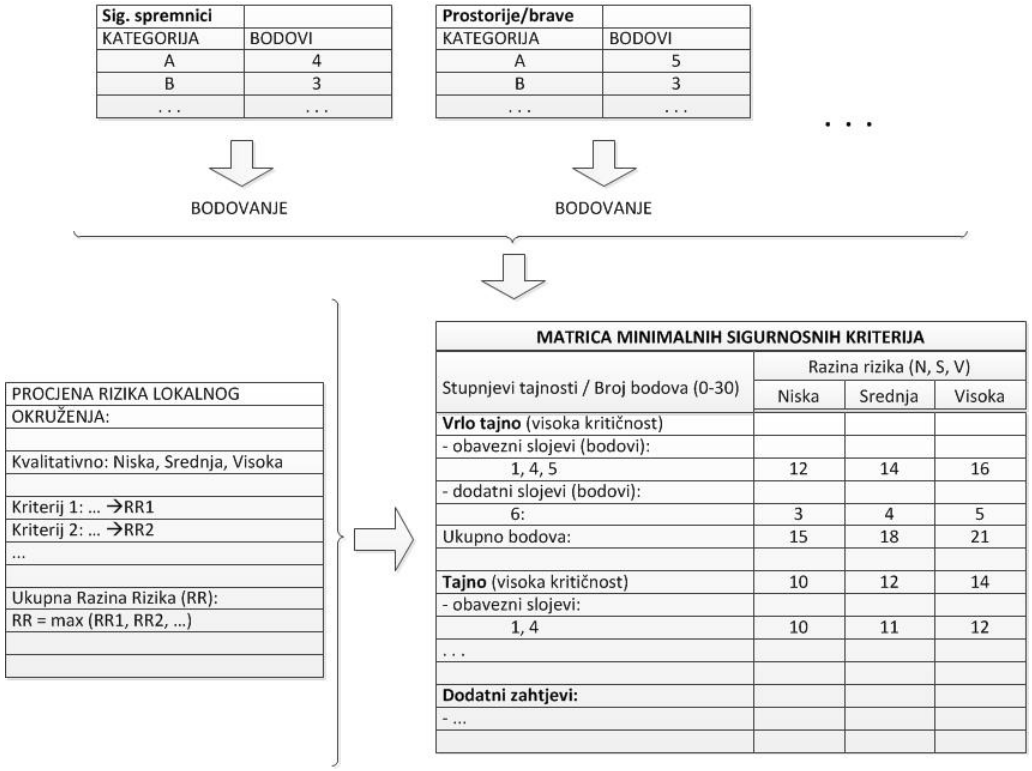
### 4.7.2. Višestruke zaštitne mjere

Načelo višestrukih zaštitnih mjera predstavlja dio područja fizičke sigurnosti u politikama informacijske sigurnosti državnog sektora [39, 73, 75]. U novije vrijeme ono se uključuje i u područje sigurnosti informacijskih sustava [59, 82], a kroz problematiku kritične nacionalne infrastrukture i puno šire, u politike informacijske sigurnosti u različitim poslovnim sektorima u kojima tvrtke koje se bave određenom djelatnošću predstavljaju obveznike primjene sigurnosnih zahtjeva iz propisa u području kritične nacionalne ili EU infrastrukture [4, 5]. Svi ovi primjeri predstavljaju razradu tradicionalnog sigurnosnog načela višestrukih zaštitnih mjera koje se implementiraju sukcesivno po dubini opsega zaštićenog prostora (engl. *Defence-in-Depth*).

Najčešća primjena ovog načela u politikama informacijske sigurnosti je u okviru fizičke sigurnosti, kada se predviđa niz slojeva zaštite kao što su primjerice:

- sigurnosni spremnici za zaštitu klasificiranih podataka;

- zaštita prostorija u kojoj se nalazi štićena imovina;
- kontrola pristupa u objekt;
- sustav otkrivanja napada/provale (engl. *Intrusion Detection System - IDS*);
- zaštita objekta;
- zaštita vanjskog perimetra.



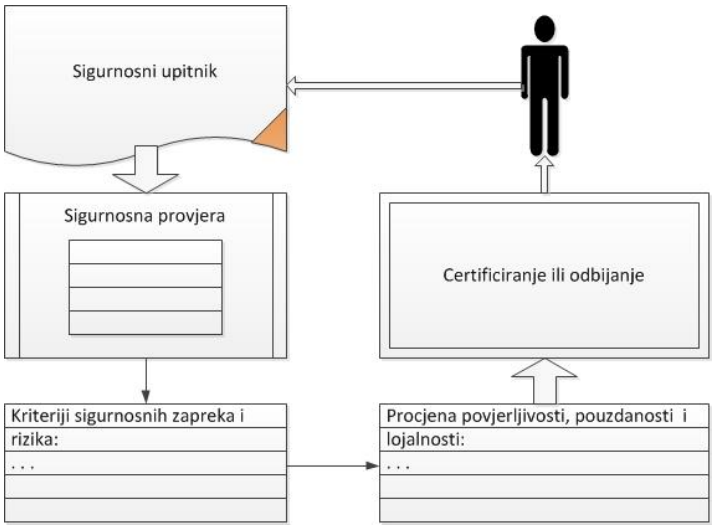

**Slika 4.8:** Matrična metoda upravljanja rizikom fizičke sigurnosti

Politike informacijske sigurnosti u državnom sektoru uobičajeno koriste tzv. matricu minimalnih sigurnosnih kriterija. Ovisno o pojedinoj metodi kojom se načelo razrađuje, koristi se određeni broj slojeva fizičke zaštite. Svaki sloj fizičke zaštite može se ostvariti na različite načine, kao što su: vrsta i visina ograde, vrsta IDS-a, način građenja objekta (montažni, čvrsti), vrsta vrata, zaštita prozora, prisutnost čuvara, nadzor i reakcija interventnih timova, vrste brava i sustava za kontrolu pristupa, tip i kategorizacija sigurnosnog spremnika i sl. Metoda se sastoji od definiranja određenog broja slojeva i kategorizacije načina izvedbe svakog pojedinog sloja, koja je opisna ili se povezuje s odgovarajućim normama, te od dodjeljivanja bodova (težinskih faktora) za svaki sloj zaštite, ovisno o korištenoj sigurnosnoj opremi. Ukupni zbroj bodova po svim ostvarenim slojevima u nekom konkretnom slučaju, uspoređuje se s matricom minimalnih sigurnosnih kriterija koju određuje primjenjiva matrična metoda rizika fizičke sigurnosti, odnosno vlasnik rizika. Matrična metoda rizika fizičke

sigurnosti može sadržavati i metodu kvalitativne procjene rizika lokalnog okruženja, na temelju koje se primjenjuju različiti minimalni sigurnosni kriteriji (ukupan broj bodova), odnosno obvezujući slojevi fizičke zaštite koji se moraju ostvariti, što je prikazano na slici 4.8 [53].

### 4.7.3. Sigurnosno certificiranje fizičkih i pravnih osoba

Načelo sigurnosnog certificiranja osoba tradicionalno se primjenjuje u politikama informacijske sigurnosti državnog sektora. U okviru sigurnosnog certificiranja, procesom sigurnosnih provjera fizičkih osoba utvrđuju se povjerljivost, pouzdanost i lojalnost osobe. Proces sigurnosnog certificiranja temelji se na obvezi vlastoručnog popunjavanja sigurnosnog upitnika i sigurnosnoj provjeri podataka koje osoba popuni u upitniku. Sigurnosnu provjeru provodi nadležno nacionalno tijelo (engl. *Security Vetting Authority*), a procjena rizika najčešće se provodi u nacionalnom NSA tijelu. Metoda je prikazana u glavnim crtama na slici 4.9 i uobičajena je za područje informacijske sigurnosti [53]. Sigurnosni upitnik kreira se kako bi sadržajno obuhvatio sve elemente prema kojima se utvrđuju početno određena tri kriterija za osobe: povjerljivost, pouzdanost i lojalnost. Ovakav koncept propisan je i u RH prema [39, 54, 83], a sigurnosni upitnici propisani su u [84].




**Slika 4.9:** Povezanost sigurnosnog upitnika, provjere, zapreka i rizika te sigurnosnog certifikata

Zakonski su propisana dva elementa koja se utvrđuju sigurnosnom provjerom, a to su sigurnosne zapreke i sigurnosni rizici. Sigurnosne zapreke su, primjerice, neistinito navođenje

podataka u upitniku za sigurnosnu provjeru te činjenice koje su posebnim zakonom propisane kao zapreke za prijam u državnu službu. U sigurnosne rizike ubrajaju se, primjerice, izrečene stegovne sankcije i druge činjenice o ponašanju osobe koje mogu predstavljati osnovu za sumnju u povjerljivost, pouzdanost ili lojalnost osobe za postupanje s klasificiranim podatcima. Uvidom u sadržaj sigurnosnog upitnika lako je uočiti koje su to činjenice koje mogu predstavljati sigurnosni rizik (npr. imovinsko stanje, dvojno državljanstvo, sudjelovanje u stranim vojnim postrojbama, rodbina, zdravstveno stanje i različite ovisnosti, kontakti s pripadnicima stranih obavještajnih službi i dr.). Sigurnosnom provjerom vrši se provjera podataka koje je osoba ispunila u upitniku. U konačnici, nakon utvrđivanja zapreka i sigurnosnih rizika opisanim postupkom, donosi se odluka o certificiranju osobe ili o odbijanju zahtjeva s određenom mogućnošću prava žalbe. Na odluku primarno utječu sigurnosne zapreke koje su postupkom sigurnosne provjere utvrđene, kao i kumulacija procijenjenih sigurnosnih rizika.

Postupak sigurnosne provjere za pravne osobe provodi se u slučaju potrebe izdavanja certifikata sigurnosti poslovne suradnje. Posjedovanje ovog certifikata obavezno je za sve pravne osobe prilikom sklapanja klasificiranog ugovora stupnja tajnosti „Povjerljivo“ ili više, s državnim tijelom (nacionalno, NATO, ili EU tijelo). Postupak sigurnosne provjere vrlo je sličan postupku opisanom za fizičke osobe, ali u sebi sadrži nekoliko segmenata provjere:

- sigurnosna provjera pravne osobe i sigurnosne provjere fizičkih osoba u pravnoj osobi koje će pristupati klasificiranim podatcima tijekom provođenja klasificiranog ugovora;
- sigurnosna akreditacija pravne osobe za korištenje klasificiranih podataka u prostoru pravne osobe (organizacija, edukacija, prostor i oprema), ukoliko je potrebna za provedbu klasificiranog ugovora;
- sigurnosna akreditacija informacijskog sustava, ukoliko je potrebna za provedbu klasificiranog ugovora.

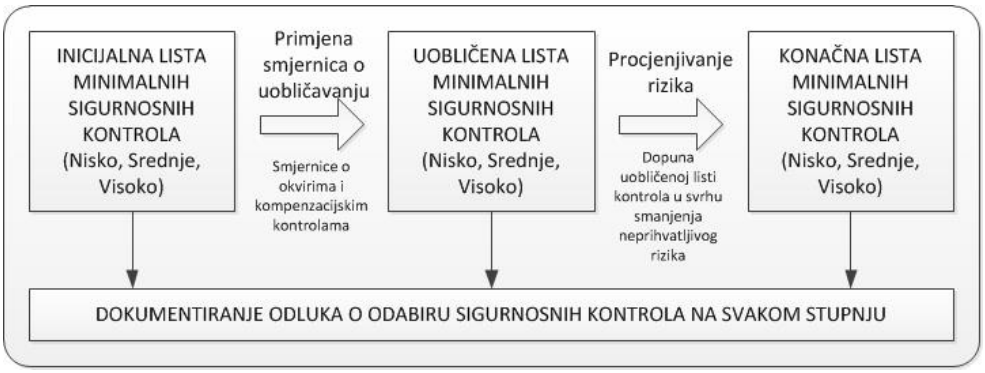
Sigurnosna provjera pravne osobe provodi se na sličan način kao i sigurnosna provjera fizičkih osoba pri čemu se koristi poseban upitnik za pravnu osobu, propisan prije spomenutim pravnim aktima, a fizičke osobe, zaposlenici pravne osobe, u smislu provedbe sigurnosne provjere prolaze isti postupak kao zaposlenici državnih tijela.

## 4.8. Različiti koncepti pristupa odabiru sigurnosnih kontrola u važnijim normama informacijske sigurnosti

S obzirom na veliki broj raspoloživih normi sa sigurnosnim kontrolama koje obuhvaćaju područje sigurnosti informacijskih sustava kao npr. [27, 85], uobičajena primjena u državnom sektoru ide za tim da utvrdi minimalne sigurnosne kriterije koji će neovisno o lokalnoj procjeni rizika, osigurati primjenu odgovarajućeg skupa sigurnosnih kontrola [86, 87, 88, 89]. Takav skup sigurnosnih kontrola može biti jedinstven kao u [82], ili se može sastojati od više skupova sigurnosnih kontrola, koji se primjenjuju sukladno kvalitativnoj procjeni sveukupnog utjecaja mogućih prijetnji na informacijski sustav (najčešće kvalitativno na tri razine).

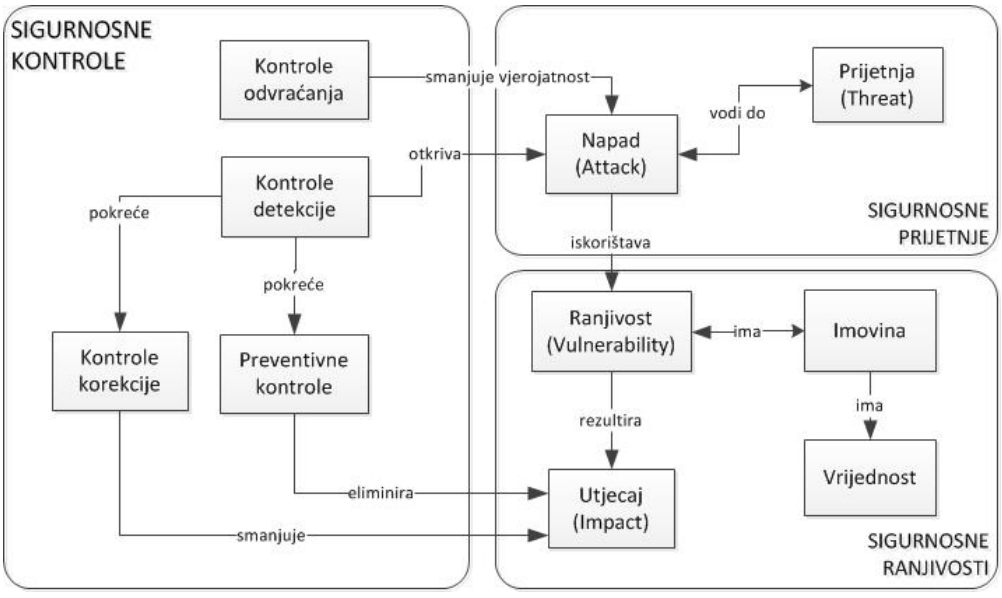
Tako primjerice NIST metoda prema [85, 86], provodi prvo analizu svih kategorija podataka na određenom informacijskom sustavu te procjenjuje mogući utjecaj povreda sigurnosti na sigurnosne kriterije povjerljivosti, cjelovitosti i raspoloživosti, za svaku korištenu kategoriju podataka zasebno, a zatim na temelju toga utvrđuje sveukupnu razinu utjecaja i tako određuje sigurnosnu kategorizaciju informacijskog sustava. Pri tome je sveukupna razina utjecaja jednaka najvećem pojedinačnom utjecaju na jedan od tri sigurnosna kriterija [86], ili na svaki od kriterija zasebno, u slučaju informacijskih sustava od važnosti za nacionalnu sigurnost [89]. Za svaku od tri razine utjecaja mogućih povreda sigurnosti informacijskog sustava, definiran je popis obvezujućih sigurnosnih kontrola iz kataloga u [85], odnosno minimalni sigurnosni kriteriji. Ovakvom kategorizacijom utvrđeni inicijalni popis sigurnosnih kontrola, dalje se oblikuje naputkom za primjenu kontrola opsega i kompenzacije, koje ovise o specifičnostima konkretnog informacijskog sustava (namjena, tehnologija, prostor, javni pristup i sl.). Tako oblikovanu listu sigurnosnih kontrola dalje je moguće prilagođavati operativnim specifičnostima provođenjem detaljne procjene rizika u konkretnom lokalnom okruženju.

Opisani primjer, prikazan na slici 4.10 [85], predstavlja pristup u kojem se tradicionalna politika informacijske sigurnosti u državnom sektoru kombinira s mogućnostima koje proizlaze iz suvremenog pristupa preko upravljanja rizikom. Ukratko prikazana metoda NIST-a prema [85], namijenjena je području sigurnosti informacijskih sustava, ali je u velikoj mjeri usklađena s nešto općenitijim pristupom informacijskoj sigurnosti u okviru međunarodne norme ISO 27001 [27], preko mapiranja sukladnih i sličnih kontrola.




**Slika 4.10:** Metoda NIST-a kojom se odabir sigurnosnih kontrola vrši kombiniranjem pristupa minimalnim sigurnosnim kontrolama i upravljanju rizikom

Metode upravljanja rizicima temelje se na identificiranju štićene imovine unutar opsega primjene politike informacijske sigurnosti, zatim na različitim katalozima ranjivosti određenih tipskih vrsta imovine, kao i na mogućim prijetnjama koje mogu iskoristiti pojedine ranjivosti [90]. Konačni cilj je određivanje sigurnosnih kontrola iz određene norme, kao npr. [27], s pomoću kojih se može na odgovarajući način djelovati na prijetnje, na ranjivosti, ili na utjecaj napada na imovinu, kao što je prikazano na slici 4.11.




**Slika 4.11:** Logički model sigurnosnih kontrola, prilagođeno prema [90]

Proces obrade pojedinačnih rizika (engl. *Risk Treatment*) dobivenih na temelju parova ranjivost - prijetnja, uobičajeno se, osim prikazanim smanjenjem rizika prema slici 4.11, provodi i izbjegavanjem rizika, prihvaćanjem rizika, ili prijenosom rizika, sukladno analizi i

procjeni potrebnog sigurnosnog ulaganja u odnosu na vjerojatnost nekog rizika, vrijednost imovine, odnosno mogući utjecaj takvog sigurnosnog rizika u širem smislu organizacije i procijenjenu razinu prihvatljivosti rizika. Sigurnosne kontrole u normama kao što su [27, 85], uobičajeno se ne propisuju detaljno, kako bi se provedba norme mogla prilagoditi različitim sigurnosnim okruženjima, u širokom rasponu pravnih osoba koje mogu koristiti različite norme, odnosno s ciljem što veće općenitosti i primjenjivosti norme. Stoga se uz norme često koriste i dodatne smjernice [91].

## 4.9. Suvremene promjene pristupa domenama podataka i potreba proširenja kategorizacije podataka

Uz pomoć prikaza razvoja informacijskog prostora, u poglavlju 4.2. ukazano je na ključne domene podataka koje su se razvile tijekom formativnog razdoblja politika informacijske sigurnosti: klasificirani podatci, osjetljivi podatci, osobni podatci i intelektualno vlasništvo (slika 4.2.). U nastavku su dana pojašnjenja i kratki opisi ovih domena podataka. Domena klasificiranih podataka prikazana je detaljnije u poglavlju 4.3.1. U nastavku je prikazana kratka analiza s obzirom na aktualne promjene do kojih dolazi u različitim domenama podataka u vezi sa suvremenim stanjem kibernetičkog prostora i povezanim društvenim promjenama.

### 4.9.1. Domena intelektualnog vlasništva

Intelektualno vlasništvo, predstavlja, najstariju zakonski uspostavljenu domenu podataka sa slike 4.2. Iako nije usko i izravno povezano s područjem informacijske sigurnosti, osobito gledano u okvirima državnog sektora u okviru kojeg se najviše promatrao razvoj područja, sa sve većim razvojem područja informacijske sigurnosti u poslovnom sektoru tijekom posljednja dva desetljeća, rasla je i važnost domene podataka koja se naziva poslovna tajna. S druge strane, razvoj kibernetičkog prostora značajno je potencirao problem zaštite intelektualnog vlasništva, ne samo kroz različite vidove autorskih djela, već i kroz problem korištenja programskih licenci.

Pojam intelektualnog vlasništva obuhvaća autorska prava (stvaratelji književnih, glazbenih, umjetničkih i znanstvenih djela) i autorskom pravu srodna prava (prava umjetnika izvođača, proizvođača fonograma, organizacija za radiodifuziju, filmskih producenata, nakladnika i

proizvođača baza podataka) [72]. Intelektualno vlasništvo u širem smislu obuhvaća i pojam industrijskog vlasništva koji uključuje patente, žigove, oznake geografskog porijekla, industrijski dizajn (zaštita vanjskog izgleda, odnosno pojavnosti nekog proizvoda), kao i poslovnu tajnu. Osnovne razlike u različitim pravnim institutima koji se koriste u okviru intelektualnog vlasništva nalaze se u različitim konceptima ostvarivanja prava, u dužini zakonske zaštite, kao i u obimu prava koji se pojedinim pravnim institutom štiti. Tako je, primjerice, osnovna razlika između autorskih prava i patenta u tome što se autorska prava stječu samim stvaranjem određenog djela ili rada, nisu prenosiva i traju 70 godina nakon smrti autora, dok se pravo patenta stječe u okviru propisanog postupka koji provodi nadležno tijelo te se može prenijeti na druge osobe ugovorom o licenci, a traje između 10 i 20 godina, ovisno o vrsti provedenog postupka patentiranja. Nacionalna prava intelektualnog vlasništva prilično su usklađena u svijetu, što uglavnom nije slučaj s drugim granama prava. Ovdje je ta usklađenost posljedica vrlo ranih multilateralnih ugovora (počevši od 19. stoljeća), poput Pariške konvencije o zaštiti industrijskog vlasništva iz 1883. godine. U tablici 4.1 prikazana je usporedba načina zaštite intelektualnog vlasništva usporedbom koncepata autorskog prava, patenta i poslovne tajne, s obzirom na čimbenike kao što su pravna zaštita koju pružaju, trajanje zaštite i sl. [3, 68, 72].

**Tablica 4.1:** Usporedba autorskog prava, patenta i poslovne tajne

| | **Autorsko pravo** | **Patent** | **Poslovna tajna** |
|---|---|---|---|
| **Objekt zaštite** | Izražavanje ideje, ne sama ideja | Izum: način kako nešto radi | Tajna, neka prednost u tržišnom natjecanju |
| **Javna objava zaštićenog objekta** | Da, intencija je promovirati objavljivanje | Projekt registriran u Državnom zavodu za intelektualno vlasništvo | Ne |
| **Zahtjev distribucije objekta** | Da | Ne | Ne |
| **Način registracije** | Vrlo jednostavno, autor samostalno ili automatizmom | Vrlo složeno, zastupnici na području industrijskog vlasništva | Nema registracije |
| **Trajanje** | 70 godina nakon smrti autora | 10 do 20 godina nakon registriranja | Neograničeno |
| **Pravna zaštita** | Tužba kada se neautorizirane kopije prodaju | Tužba ako se izum kopira | Tužba ako je poslovna tajna neovlašteno otkrivena |

Iako je domena intelektualnog vlasništva originalno zamišljena kao zaštita za objekte poput knjiga, skladbi ili fotografija, ovaj koncept danas se u velikoj mjeri primjenjuje i na digitalne objekte i programsku podršku. Autorsko pravo uobičajeno se primjenjuje na podatkovne medije s instalacijskim kopijama programske podrške koje se dostavljaju korisnicima. Na taj način može se uspješno zaštititi izvršni program koji se distribuira, ali ne i izvorni tekst programa, jer se zaštitom autorskih prava ne štiti ideja (u ovom slučaju algoritam programa), već samo način izražavanja ideje (u ovom slučaju instalacijska distribucija programa). Patenti kao sredstvo zaštite programske podrške nisu primjenjivi. U smislu patenta programi se promatraju kao apstraktne ideje, odnosno algoritam, pa ih nije moguće patentirati, osim u slučaju kada su dio šireg procesa koji je predmet patenta, međutim niti tada kao samostalno programsko rješenje nisu zaštićeni. Koncept poslovne tajne je najprimjenjiviji za zaštitu izvornog teksta programa, uz istovremenu distribuciju izvršnog programa zaštićenog autorskim pravom. Poslovna tajna ne pruža zaštitu od reverznog inženjeringa, što u određenim slučajevima treba uzeti u obzir. Sklopovska rješenja, kao što su čipovi, mogu biti patentirani, a za ugrađenu programsku podršku (engl. *Firmware*), bolje je rješenje zaštite poslovna tajna. Programska dokumentacija zaštićena je autorskim pravima, jednako kao i sadržaj web-mjesta koji predstavlja medij zapisa, poput knjige ili fotografije. Imena internetskih domena, tvrtki i proizvoda, kao i komercijalni simboli, štite se kao robni znakovi (žigovi) [68].

Zakon donesen 1998. godine u SAD-u, pod nazivom *Digital Millennium Copyright Act*, bio je jedan od prvih pokušaja prilagodbe koncepata intelektualnog vlasništva digitalnom dobu (npr. uvođenje prava pričuvne kopije kupljenog digitalnog medija sa zvučnim ili video sadržajem). Pokazalo se da ključni problem kopiranja u digitalnom svijetu nije moguće riješiti načelima nastalim u analognom svijetu zbog suštinske razlike između digitalnog i analognog svijeta koja proizlazi iz činjenice da je digitalna kopija, za razliku od analognih kopija objekata poput knjiga, fotografija i pjesama, istovjetna digitalnom originalu. Upravo stoga, suvremena zakonska rješenja idu za tim da kupnju digitalnih objekata definiraju sve više kao pravo najma, odnosno korištenja, a manje u smislu tradicionalnog poimanja kupnje (primjer je drugi zakon iz SAD-a: *No Electronic Theft Act*, 1997.), jer se na taj način učinkovitije sprječava daljnja distribucija digitalnih objekata, čak i kada nije predmet zarade već razmjene.

Poslovna tajna prema tablici 4.1 predstavlja jedan od načina zaštite intelektualnog vlasništva. U većini pravnih sustava poslovna tajna tumači se kao informacija nepoznata stručnoj

javnosti, koja na određeni način donosi ekonomsku korist svom vlasniku te čiju tajnost vlasnik poslovne tajne u razumnim okvirima nastoji sačuvati. Poslovna tajna može biti određena poslovna praksa, odnosno način postupanja, određeno znanje do kojeg se u poslovnom sustavu došlo ili bilo koja druga informacija koja poslovnom subjektu pomaže u natjecanju s konkurencijom. Pravni sustav svake države osigurava okvire korištenja poslovne tajne (tajni podatci pravnih osoba, tržišnih subjekata) na sličan način kako je to uređeno za područje klasificiranih podataka (tajni podatci državnog sektora, državnih tijela). To znači da podatak mora biti utvrđen kao poslovna tajna zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, ako predstavlja proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada, odnosno drugi podatak zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za gospodarske interese vlasnika podataka (trgovačko društvo, ustanovu ili drugu pravnu osobu). Ovdje dolazi do povezanosti sa politikom informacijske sigurnosti, koja na sličan način kao što je to u slučaju zaštite klasificiranih podataka, mora osigurati uvjete za održavanje kriterija povjerljivosti poslovne tajne. Drugim riječima, nije moguće utvrditi poslovnu tajnu bez istovremene provedbe potpuno funkcionalne politike informacijske sigurnosti u pravnoj osobi. Razlika u odnosu na klasificirane podatke je što ne postoji skup minimalnih sigurnosnih mjera, već se mjere mogu provesti prema regulativnom načelu primjerene pažnje (poglavlje 4.4.). Za razliku od poslovne tajne, autorska prava nemaju svojstvo tajnosti, no u okviru kategoriziranja različite imovine, potrebno je obuhvatiti njihove druge specifičnosti (zaštitu od kopiranja).

### 4.9.2. Domena osobnih podataka

Primjeri problema zbog različitog pristupa zaštiti domene osobnih podataka vidljivi su i vrlo česti između SAD-a i EU-a [92]. Europski model pristupa zasnovan je na zaštiti domene osobnih podataka kao posebne kategorije podataka, zakonski regulirane posebnim zakonom i prvi je ozbiljniji pristup zaštiti ove vrste podataka u svijetu [50]. S druge strane, pristup SAD-a zasniva se na prepoznavanju i zaštiti osobnih podataka u čitavom nizu sektorski specifičnih zakona, što s jedne strane otvara moguće prostore koji nisu obuhvaćeni sektorskim zakonima, a s druge strane, ne može jamčiti unificiran pristup zaštiti na razini domene podataka. Upravo zahtjev unificiranog pristupa zaštiti domenske kategorije podataka, temelj je politike informacijske sigurnosti, kao što je opisano za domenu klasificiranih podataka u poglavlju 4.3.1.

Aktualne promjene koje se u EU provode u segmentu regulative osobnih podataka i planirane su za razdoblje od 2013. do 2015., idu u smjeru stvaranja preduvjeta za primjenu sustavnih i unificiranih sigurnosnih mjera za zaštitu osobnih podataka za sve vrste organizacija i u svim oblicima i vrstama zapisa osobnih podataka na razini EU-a. Rezultat ovih promjena trebaju biti zahtjevi koji će se u zemljama članicama EU-a, sukladno pojašnjenom regulativnom načelu primjerene pažnje iz poglavlja 4.4., moći provesti jedino sveobuhvatnom primjenom politike informacijske sigurnosti. Ovi zahtjevi odnose se na usklađivanje i koordiniranje politike zaštite osobnih podataka u cilju osiguravanja ujednačenog pristupa i tumačenja načela zaštite osobnih podataka u svim zemljama članicama EU-a (svojstvo dosljednosti primjene).

U siječnju 2012. godine Europska komisija najavila je novu EU regulativu u području zaštite osobnih podataka kojom se uvodi ovo značajno proširenje zahtjeva u postupanju s osobnim podatcima, primjereno stanju razvoja kibernetičkog prostora danas, kako s aspekta raširenosti Interneta i razvoja komunikacijsko-informacijske tehnologije, tako i s aspekta suvremenih programskih rješenja, kao što su društvene mreže na Internetu i drugi internetski alati. Predloženi koncept EU-a ima još jednu bitnu novost kojom se planira dosadašnju EU direktivu [50] (engl. *Directive*) koja propisuje zaštitu osobnih podataka u EU, zamijeniti EU regulativom (engl. *Regulation*). Razlika je u tome da se EU direktive moraju prenijeti u nacionalno zakonodavstvo zemalja članica EU-a, kako bi postale nacionalno obvezujuće, dok se EU regulativa izravno primjenjuje na nacionalne prostore zemalja članica EU-a, tj. na državni sektor i sve pravne osobe registrirane u svakoj državi članici EU-a. Stupanje na snagu nove EU regulative o zaštiti osobnih podataka očekuje se u razdoblju do 2015. godine. Pored EU regulative planira se i donošenje nove EU direktive, kojom će se na višoj, pravno obvezujućoj razini, zamijeniti dosadašnja odluka o pravilima zaštite (Framework Decision 2008/977/JHA). Na ovaj način će načela za zaštitu osobnih podataka biti izravno primijenjena na sve zemlje članice EU-a, bez prethodnog preuzimanja u nacionalno zakonodavstvo. Na provedbenoj razini sigurnosnih mjera, sve zemlje članice EU-a bit će obvezane novom EU direktivom na preuzimanje propisanih sigurnosnih mjera u nacionalno zakonodavstvo. Tako će se formirati sustav, ne samo zajednički primjenjivih načela zaštite osobnih podataka (EU regulativa), već i jedinstveni sustav sigurnosnih mjera koje će se provoditi u svrhu ostvarenja zajedničkih koncepata zaštite osobnih podataka u svim državama članicama EU-a. Pristup je u velikoj mjeri sličan pristupu klasificiranim podatcima s obzirom na način propisivanja i međusobnog usklađivanja između EU-a kao međunarodne organizacije i zemalja članica sa svojim nacionalnim prostorima.

Novi EU pristup [93] predstavlja regulativnu razradu politike informacijske sigurnosti za zaštitu osobnih podataka, proizašlu iz iskustva s EUROJUST segmentom EU-a (engl. *The European Union's Judicial Cooperation Unit*), u kojem je zaštita osobnih podataka bila provedena u svrhu osiguravanja nesmetane i kvalitetne pravosudne suradnje država članica EU-a [94]. Navedeni se pristup zasnivao na uspostavi internih politika informacijske sigurnosti [95], kako bi se na sustavan način osigurala primjena odgovarajućih načela pristupa osobnim podatcima te provela zaštita osobnih podataka tijekom njihovog korištenja, pohrane i razmjene. Za ilustraciju pristupa iz novog prijedloga EU regulative, mogu se izdvojiti sljedeći elementi [96]:

- uvođenje obavezne prijave povreda sigurnosti;
- koordinacija preko jednog nacionalnog nadzornog tijela za nadzor provedbe mjera zaštite (engl. *Supervisory Authority*) za sve pravne osobe koje rade na području više zemalja članica EU-a (određivanje zemlje domaćina);
- korištenje osobnih podataka usko i u okviru svrhe za koju su prikupljeni, uz uvjet definiranja minimalnog skupa podataka potrebnog isključivo za poslovne svrhe, kao i određivanja minimalno potrebnog trajanja pohrane osobnih podataka;
- davanje eksplicitne suglasnosti osobe za korištenje njenih osobnih podataka;
- pravo korisnika čiji su osobni podatci pohranjeni na brisanje podataka iz svih sustava i evidencija određene pravne osobe, voditelja zbirke osobnih podataka;
- ozbiljne povrede sigurnosti osobnih podataka u svojoj odgovornosti, pravne osobe moraju prijaviti u roku od 24 sata i nadležnom nadzornom tijelu i fizičkim osobama o čijim se podatcima radi, uz prijetnju kazni koje mogu iznositi i do 2% ukupnog prihoda;
- povrede sigurnosti podataka dio su odgovornosti pravne osobe koja je podatke prikupila. Internim ugovorima s trećim stranama, ove odgovornosti ne mogu se prebaciti na njih (moguće je jedino pokrenuti naknadne sudske tužbe za odgovornost treće strane) već odgovornosti leže na pravnoj osobi, vlasniku odgovarajuće zbirke osobnih podataka.

Navedene mjere, kao i niz drugih predviđenih mjera, tipični su koncepti sigurnosnih mjera kakvi se provode u politikama informacijske sigurnosti, vezano za klasificirane podatke. Kako bi se ostvario ovakav pristup osobnim podatcima u nekoj pravnoj osobi, bit će nužno uvesti učinkovito upravljanje podatcima, odnosno uspostaviti shemu kategoriziranja podataka,

prepoznavanja vlasnika podataka, kao i identificiranje svih potencijalnih korisnika podataka, a to predstavlja zahtjeve za provedbu politike informacijske sigurnosti pravne osobe.

### 4.9.3. Kibernetički prostor i nove kategorije podataka

U dosadašnjoj analizi obuhvaćen je niz aspekata koji povezuju kibernetički prostor i suvremene politike informacijske sigurnosti te je zaključeno da se suvremene politike informacijske sigurnosti, zbog promjene okruženja u kojemu komuniciramo različitim domenama podataka, moraju mijenjati i prilagođavati metodu pristupa. Tako se politikom informacijske sigurnosti može postići zacrtane ciljeve, iako se sami ciljevi, primjerice u slučajevima tradicionalno prisutnih domena podataka kao što su klasificirani podatci, nisu bitno promijenili tijekom posljednjih desetljeća. Ovaj zaključak predstavlja važan zahtjev za modeliranje politika informacijske sigurnosti u ovom radu, jer sadržaj modela koji se razvija mora odraziti ne samo dominantne vrste podataka, s obzirom na zahtjeve informacijske sigurnosti, već i kontekst njihove suvremene primjene (globalno okruženje kibernetičkog prostora).

Razmatranje problematike podataka u kibernetičkom prostoru potrebno je proširiti i na prepoznavanje novonastalih kategorija podataka, specifičnih za korištenje kibernetičkog prostora, uočeno u [97]. Za potrebe ovog istraživanja vezanog za problematiku modeliranja politika informacijske sigurnosti, postavljaju se nešto drugačiji okviri od rada u [97]. U ovom radu od interesa su vrste podataka nastale u javnoj domeni u okviru aktivnosti samog organizacijskog entiteta koji provodi politiku informacijske sigurnosti ili aktivnosti drugih subjekata u kibernetičkom prostoru u odnosu na ovaj organizacijski entitet, odnosno kategorije koje u takvom slučaju mogu nastati uslijed specifičnosti kibernetičkog prostora, a važne su sa stanovišta politika informacijske sigurnosti.

U tom smislu, kategorija podataka interesantna za ovo istraživanje su povjereni podatci (engl. *Entrusted Data*) koji nastaju u slučaju kada vlasnik podataka nema odgovarajuću kontrolu nad podatcima koje je povjerio drugim subjektima. Ovaj slučaj je u politikama informacijske sigurnosti važan pri korištenju javnih komunikacijskih i informacijskih usluga na temelju različitih ugovora o razini usluge (engl. *Service Level Agreements - SLA*), što je danas redoviti slučaj. Kategorija podataka koja nastaje kroz takve ugovore, instalaciju i održavanje opreme, može obuhvatiti različite podatke vezane za poslovanje tvrtke ili državnog tijela, koji mogu

biti osjetljivi, ali i tajni. Nadalje, usko povezani s povjerenim podatcima su i podatci o ponašanju (engl. *Behavioral Data*), koji mogu nastajati na web-mjestu ili kod davatelja usluge/infrastrukture. Također, ovi podatci mogu obuhvatiti različite podatke vezane za poslovanje tvrtke ili državnog tijela, koji mogu biti osjetljivi, ali i tajni, te su povezani sa ugovorima o razini usluge za korištenje takvih komunikacijskih ili infrastrukturnih usluga. Podatci ove vrste trebaju biti prepoznati u politikama informacijske sigurnosti i odgovarajuće ugovorno regulirani.

## 4.10. Analiza politika i normi informacijske sigurnosti i rječnik domene

Analiza područja domene provodi se s ciljem šire domenske razine sistematizacije i integracije različitih pristupa i zahtjeva globalnog i lokalnog okruženja te dominantnih suvremenih politika i normi informacijske sigurnosti. Analizu je nužno provoditi na široj domenskoj razini kako bi se moglo prepoznati zajedničke koncepte te ih modelirati putem generalizacije ili apstrakcije. Tako dobiveni vršni domenski koncepti mogu se uz pomoć predložene metode modeliranja specijalizirati u odgovarajuće hijerarhije koncepata potrebne za modeliranje politika informacijske sigurnosti u stvarnim organizacijskim okruženjima.

Vršni domenski koncepti moraju obuhvatiti implicitno domensko znanje (poglavlja 2.4. i 3.2.), kao znanje koje u hijerarhiji: podatak – informacija – znanje – mudrost, predstavlja najvišu kategoriju, odnosno razumijevanje znanja o postupanju definiranog u pojedinim normama i politikama informacijske sigurnosti. U tom smislu potrebno je razlikovati koncepte koji pripadaju pojedinim normama ili politikama informacijske sigurnosti kao što su minimalne sigurnosne mjere ili upravljanje rizikom, ali je istovremeno nužno promatrati i ulogu ovih koncepata na višoj domenskoj razini gdje oni općenito predstavljaju zaštitu podataka i drugih poslovnih vrijednosti, odnosno štićenih vrijednosti. Cilj analize opisane u četvrtom poglavlju jest definiranje opće domenske taksonomije, odnosno osnovnog rječnika domene. Usporedbama i razmatranjem ključnih sadržaja politika i normi informacijske sigurnosti na vršnoj domenskoj razini, kao i zahtjeva koji se na njih postavljaju, ostvarena je opća domenska taksonomija čiji je primjer prikazan u tablici 4.2. Domenska taksonomija informacijske sigurnosti, odnosno rječnik domene, kao okvir općenitih domenskih koncepata koji proizlazi iz analize, predstavlja opseg modeliranja u ovom radu te je u cijelosti prikazan u prilogu A. Svakom pojmu u tablici 4.2, odnosno u prilogu A, pridružen je odgovarajući domenski koncept s opisom značenja, čime se osigurava domenski valjana interpretacija

uvedenih pojmova, odnosno interpretacija u skladu sa značenjem koje se koristi za ove pojmove u okviru modeliranja predloženog u ovom radu.

**Tablica 4.2:** Primjeri pojmova iz domenske taksonomije informacijske sigurnosti (rječnik domene)

| R.br. | **POJAM** | **OPIS PRIDRUŽENOG KONCEPTA (opći domenski koncepti)** |
|---|---|---|
| 1. | Informacijska sigurnost | *Željeno stanje povjerljivosti, cjelovitosti i raspoloživosti štićenih vrijednosti, koje se postiže organizacijskom podrškom i primjenom odgovarajućih mjera zaštite;* |
| 2. | Politika informacijske sigurnosti | *Skup procedura kojima se planira, ostvaruje, provodi i preispituje informacijska sigurnost u određenom opsegu primjene;* |
| 3. | Domena politike informacijske sigurnosti | *Obuhvaća politiku informacijske sigurnosti kroz životni ciklus (planiranje, ostvarenje, provođenje i preispitivanje) te globalno i lokalno sigurnosno okruženje organizacije koja provodi politiku informacijske sigurnosti;* |
| 4. | Opseg primjene politike informacijske sigurnosti | *Organizacijski entitet, ustrojstveni dio organizacije, informacijski sustav;* |
| 5. | Organizacijski entitet | *Organizacija koja provodi politiku informacijske sigurnosti ili organizacija koja surađuje;* |
| 6. | Regulativni zahtjev | *Sastoji se od taksonomije koja osigurava strukturirani pristup analizi i primjeni regulativnih zahtjeva kroz proces planiranja koji obuhvaća zakonske, sektorske i ugovorne zahtjeve;* |
| 7. | Povreda sigurnosti | *Svaka aktivnost ili neprovođenje mjera sigurnosti, protivno propisima, a koje je uzrokovalo ili može uzrokovati štetu za utvrđene štićene vrijednosti;* |
| 8. | Razdioba podataka | *Poslovna razdioba podataka koja se provodi u sklopu redovnih poslovnih aktivnosti organizacijskog entiteta ili javna razdioba podataka;* |
| 9. | Javna razdioba podataka | *Javna objava podataka, zahtjevi za javni pristup podatcima ili podatci nastali u kibernetičkom prostoru aktivnošću organizacijskog entiteta ili drugih subjekata;* |
| 10. | Proces nadzora | *Opća obilježja procesa nadzora kao vrsta, metode i opseg nadzora;* |
| 11. | Provedba nadzora | *Tipični procesi nadzora koji se koriste u različitim politikama i normama informacijske sigurnosti:akreditacija, certifikacija, nadzor/revizija;* |
| 12. | Akreditacija | *Odobrenje rada u segmentu poslovanja organizacije, čime organizacija preuzima odgovornost za poslovanje u skladu sa određenom normom ili politikom te odgovornost za rizike u ovom segmentu poslovanja;* |
| 13. | Certifikacija | *Sveobuhvatna procjena tehničkih, organizacijskih i administrativnih kontrola, kako bi se utvrdilo jesu li kontrole primijenjene sukladno normi kojom su propisane;* |
| 14. | Nadležno sigurnosno tijelo | *Sastoji se od taksonomije koja obuhvaća nacionalna i međunarodna tijela, razrade potrebnih hijerarhija nacionalnih sigurnosnih tijela, kao i tijela s koordinacijskim i operativnim zadaćama povezanim s područjem informacijske sigurnosti;* |
| 15. | Štićena vrijednost | *Obuhvaća podatke i druge poslovne vrijednosti za koje se osigurava zaštita sigurnosnih kriterija povjerljivosti, cjelovitosti i raspoloživosti;* |

Pored opće domenske taksonomije iz priloga A, analiza prikazana u četvrtom poglavlju osnova je i za detaljiziranje ovih općih domenskih koncepata koje se provodi postupnom razradom sukladno predloženoj metodi modeliranja.

# 5. METODA MODELIRANJA POLITIKA INFORMACIJSKE SIGURNOSTI TEMELJENA NA UPRAVLJANJU ZNANJEM

## 5.1. Modeliranje složenih sustava

Rekapitulacijom uvodnih razmatranja i definiranja provedenih u uvodnim poglavljima, postavljaju se temeljni zahtjevi na metodu modeliranja i obilježja koja se očekuju od predloženog modela. Ključni zahtjev povezan je s opsegom modeliranja koji se usmjerava na širu domensku razinu područja informacijske sigurnosti (rječnik domene, prilog A), prepoznajući pri tome problem složenosti i heterogenosti domene, odnosno slabe povezanosti raspoloživog domenskog znanja.

Šira domenska razina podrazumijeva ostvarenje metode koja na odgovarajući način mora uzeti u obzir problematiku složenosti i međusobne nepovezanosti sigurnosnih zahtjeva u okviru različitih sektora društva. Pri tome je cijelu domensku problematiku potrebno istovremeno promatrati u nacionalnom i međunarodnom okruženju, sukladno pojašnjenim zahtjevima suvremenog društva koji se uočavaju kroz poslovanje različitih vrsta organizacija i njihovu potrebu sigurnosne suradnje i međusobne razdiobe osjetljivih podataka, kao i kroz nužnost korištenja globalne infrastrukture kibernetičkog prostora. Ova obilježja utječu na potrebu više razine razumijevanja domenske problematike između različitih vrsta organizacija koje međusobno surađuju, ali i između različitih nacionalnih i međunarodnih okruženja. Jednako tako, određeni zakonski zahtjevi, poput zaštite osobnih podataka, uvode jednake norme pristupa ovoj domeni podataka u svim sektorima društva. Ipak, unatoč svim ovim sličnostima koja obilježavaju zahtjeve suvremenog globalnog okruženja, šira domenska razina informacijske sigurnosti i dalje ima obilježja visoke složenosti, heterogenosti i međusobne slabe povezanosti znanja raspoloživog u različitim politikama i normama informacijske sigurnosti, odnosno taksonomijama razrađenim u pojedinim segmentima domene (npr. sigurnosne prijetnje, ranjivosti, incidenti i sl.).

Prepoznavanje i odabir dominantnih politika i normi informacijske sigurnosti u suvremenoj praksi, predstavlja pogodan način pristupa preko kojeg se može izvršiti sistematizaciju utjecaja globalnog i lokalnog okruženja, odnosno povezati srodne koncepte iz dominantnih

politika i normi, kao što je pokazano u četvrtom poglavlju. Sistematizacija i integracija ključnih obilježja dominantnih politika i normi informacijske sigurnosti omogućava razvoj zajedničkog, konceptualiziranog rječnika domene (tablica 4.2, prilog A), te normizaciju šireg domenskog područja. Cilj konceptualizacije je jasno i razumljivo, odnosno eksplicitno opisivanje pojmova i stvaranje zajedničkog jezika za komuniciranje na široj domenskoj razini. Konceptualni domenski metamodel mora poslužiti istovremeno i kao formalna specifikacija, odnosno temelj programskog ostvarenja ontoloških modela politika informacijske sigurnosti. Cilj istraživanja je omogućiti bolje upravljanje i komuniciranje znanjem u heterogenoj i složenoj domeni informacijske sigurnosti. Uloga konceptualizacije je u dijelu modeliranja kojim se provode usporedbe i prepoznavanje pojedinih općenitih koncepata, atributa i relacija između koncepata, kao što je pokazano na primjeru koncepata nadzora informacijske sigurnosti na slici 2.2. Konceptualni domenski metamodel time predstavlja središnju točku procesa modeliranja (razvoj, specifikacija, održavanje, dorade i proširenja), ali i okvir koji poboljšava razumljivost domenskog znanja i olakšava komuniciranje stručnjaka o sadržajima konceptualizirane domene. Pri tome se koristi domenski rječnik s odgovarajućom specifikacijom i međusobnim relacijama, kao i vizualni način zapisa radi jasnoće i razumljivosti ljudima. Kao što je prikazano na slici 2.1, konceptualizacija prvenstveno osigurava sadržaje za proces modeliranja politika informacijske sigurnosti temeljen na upravljanju znanjem, odnosno odabir pojmova kojima se definira sadržaj i kontekst primjene u konceptualnom metamodelu. Pri tome je zahtjev općenitosti nužan za opis šire domenske razine, ali ga treba ujednačiti sa zahtjevom praktične primjenjivosti, koji je nužan za modeliranje konkretnih organizacijskih okruženja koja provode politiku informacijske sigurnosti u nekim određenim i specifičnim uvjetima okoline i poslovanja različitih vrsta organizacija.

Domenska taksonomija razvija se kao klasifikacijska shema koja strukturira znanje u domeni i stvara rječnik domene. Ovaj rječnik predstavlja prethodno konceptualizirane pojmove, koji imaju jedinstveno, zajedničko značenje za domenu i kontekst modela u kojem se primjenjuju. Izbor pojmova koji se rječnikom domene uvode, potrebno je do određene mjere ograničiti i ujednačiti uspostavljenim opsegom modeliranja, sukladno pojmovnoj zastupljenosti u dominantnim politikama i normama informacijske sigurnosti. Pristup konceptualizaciji, kao metodi za razvoj metamodela, omogućava nam korištenje općeg domenskog rječnika za razinu metamodela, istovremeno zadržavajući mogućnost korištenja specifičnog rječnika za razinu modela nekog ciljanog okruženja, u kojem se želi modelirati određena vrsta politika

informacijske sigurnosti, kao što je prikazano na slici 2.2. Konceptualizacijom dobiveni rječnik domene, predstavlja taksonomiju domene, strukturiranu u kategorije i hijerarhije unutar njih, definirajući način prikaza međusobno logički povezanih pojmova (sintaksa). Daljnjom specifikacijom značenja ovih, logički povezanih pojmova taksonomije dolazimo do ontološkog modela (semantika). Ontologija sadrži rječnik pojmova, definiciju pojmova koja pojašnjava pojmovima pridružene koncepte i daje domenski valjanu interpretaciju koncepata, odgovarajuću strukturu kategorija i hijerarhija pojmova, kao i relacije između koncepata, u svrhu korištenja pretpostavljene zajednice korisnika. Ontologija u velikoj mjeri predstavlja logičnu nadgradnju domenske konceptualizacije i taksonomije. Za ovo istraživanje ontološki model je nužan, jer odgovor na ključno istraživačko pitanje o jednostavnosti, dosljednosti, sveobuhvatnosti i učinkovitosti upravljanja životnim ciklusom politika informacijske sigurnosti, uporabom konceptualnog metamodela domene, traži odgovarajuće, programski podržano ostvarenje modela. Upravo to je i navedeno u drugom poglavlju kao ključna razlika između konceptualnog modela koji je prvenstveno namijenjen ljudima i ontološkog modela koji koristi zapis prilagođen čitljivosti i za programske aplikacije i za ljude. Uloga ontoloških metoda u okviru procesa modeliranja predloženog ovim radom, prema slici 2.1, prvenstveno je u detaljiziranju sadržaja modela, odnosno u razradi atributa i relacija konceptualiziranih pojmova u domeni.

U poglavlju 2.4. ukazano je na potrebu sustavskog pristupa modeliranju politika informacijske sigurnosti, jer se radi o modeliranju složenog sustava, kojeg čine heterogeni elementi i procesi, koji su međusobno povezani. Ovu povezanost potrebno je opisati na svim razinama organizacije sustava. Stoga modeliranje treba obuhvatiti povezanost elemenata unutar sustava na različitim organizacijskim razinama sustava te interakciju sustava i okoline. Modeliranje šire domenske razine, predstavljene dominantnim politikama i normama informacijske sigurnosti, promatra se kao složeni sustav. Model stoga mora obilježavati povezanost politike informacijske sigurnosti s vanjskim svijetom (npr. regulativni aspekti ili kibernetički prostor), međusobne utjecaje pojedinih elemenata i procesa (npr. fizička sigurnost, sigurnost informacijskih sustava ili sigurnost osoblja), multidisciplinarnost problematike koja usko povezuje heterogene čimbenike kao što su osobe, procesi, tehnologija, kao i složen organizacijski okvir u kojem ovi čimbenici djeluju.

U procesu stvaranja instanci modela za konkretna organizacijska okruženja u kojima se primjenjuje određena politika informacijske sigurnosti, koriste se podatci u obliku

dokumenata ili evidencija. Na taj način se u procesu modeliranja prati hijerarhija pojmova u kojoj znanje predstavlja organizirane informacije na domenskoj razini, informacije predstavljaju podatke u kontekstu pojedinih politika ili normi informacijske sigurnosti, a podatci su zapisi u obliku dokumenta (normativni, postupovni) ili nekom drugom obliku koji koriste konkretne politike koje se modeliraju (različiti oblici i zapisi evidencija). Hijerarhija pojmova: podatak – informacija - znanje, sadrži mudrost kao najviši pojam. Mudrost je viša razina razumijevanja koja podrazumijeva dvije razine znanja, razinu poznavanja i razinu razumijevanja. Promatrajući stanje politike informacijske sigurnosti u okviru šireg domenskog prostora, u poglavlju 2.4. ukazano je na stanje razvoja, koje je došlo do faze znanja u kojem je velik broj informacija uobličen u odgovarajuće proceduralne naputke za postupanje (organizirane informacije na domenskoj razini koje predstavljaju znanje). Pri tome je viša razina mudrosti, u smislu razumijevanja načina i razloga korištenja tih procedura na široj domenskoj razini, odnosno primjene znanja u širem i sveobuhvatnom domenskom smislu i prostoru djelovanja, na različite organizacijske sustave i u različitim uvjetima, još uvijek u početnoj fazi istraživanja. Upravo ova nepovezanost različitog proceduralnog znanja, uzrokovana slabom međusobnom koordinacijom različitih stupova sigurnosnih zahtjeva, kako je to naglašeno u poglavlju 1.2, predstavlja motivaciju ovog istraživanja. Prema slici 2.1, u okviru procesa modeliranja predloženog ovim radom, uloga sustavskog pristupa prvenstveno je u davanju željenih funkcionalnosti sadržaju modela, odnosno u prilagodbi pojmova, koncepata, atributa i međusobnih relacija konceptualiziranih pojmova u domeni, potrebnom načinu koordinacije i međusobnog utjecaja tako definiranih koncepata u modeliranom sustavu.

U trećem poglavlju, u pregledu srodnih istraživanja, navedeni su ciljevi modeliranja u ovom istraživanju, usmjereni na razvoj šire domenske taksonomije i ostvarenje detaljno razrađenog i formalno specificiranog, višerazinskog modela politika informacijske sigurnosti, koji bi bio primjenjiv za široki spektar organizacijskih okruženja iz različitih sektora društva. Upravo mogućnost korištenja istog metamodela u različitim profilima organizacija, daje ključne prednosti ovakvog pristupa modeliranju politika informacijske sigurnosti. Pri tome, modelske instance metamodela predloženog u ovom radu, relativno jednostavnim konfiguriranjem konkretnih podataka o određenoj organizaciji mogu predstavljati detaljan model politike informacijske sigurnosti ciljane organizacije. Takvim modeliranjem daje se odgovor na postavljeni istraživački problem u poglavlju 1.3, vezano za jednostavnost, dosljednost, sveobuhvatnost i učinkovitost upravljanja životnim ciklusom politika informacijske sigurnosti

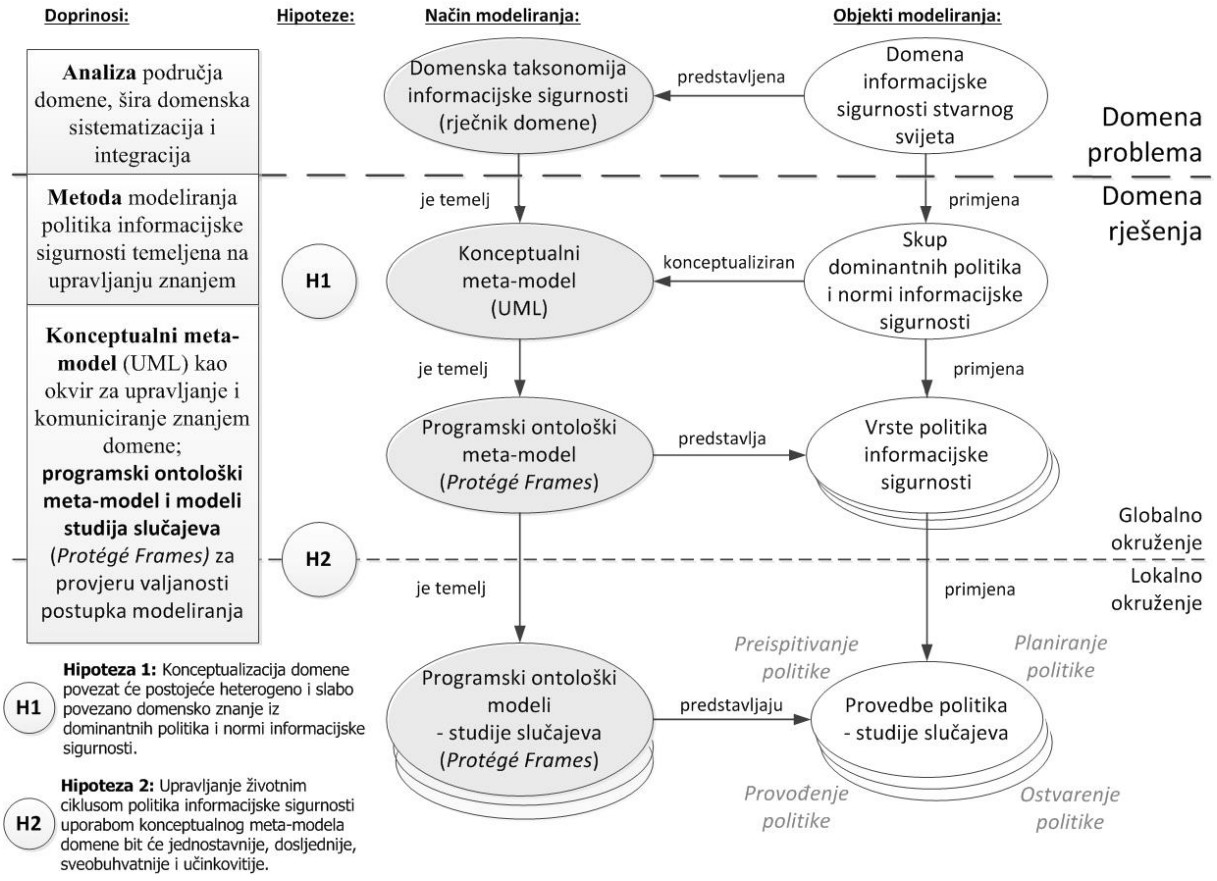
uporabom konceptualnog metamodela. U segmentu razrade funkcionalnosti modela, u ovom radu koristi se prikazani model slojeva sigurnosne arhitekture prema slici 3.2 [23], u svrhu provjere funkcionalnosti sigurnosnih zahtjeva za razvoj modela. Uvedena je i kategorizacija znanja na deklarativno (ontološki modelirani koncepti), proceduralno (opisi prirodnim jezikom pohranjeni uz pripadajuće ontološke koncepte) i relacijsko znanje (relacije između ontološki modeliranih koncepata), koja se u ovom radu primjenjuje na sličan način kao u [35]. U procesu modeliranja predloženom u ovom radu, šira domenska razina informacijske sigurnosti konceptualizira se pristupom preko implicitno sadržanog domenskog znanja, a ne samo preko eksplicitno izraženog znanja u odgovarajućim politikama i normama informacijske sigurnosti. Prema poglavlju 2.4, u kojem je pojašnjena hijerarhija pojmova: podatak – informacija – znanje – mudrost, implicitno izraženim znanjem domene informacijske sigurnosti smatra se viša razina koncepata kojima se definira „znanje o znanju“, odnosno najviši pojam ove hijerarhije – mudrost. To znači da, sukladno definiciji pojma mudrosti, model u ovom radu razrađuje i koncepte poznavanja eksplicitnog znanja (zahtjevi dominantnih normi i politika informacijske sigurnosti), ali i koncepte razumijevanja implicitnog znanja (međusobne sličnosti koncepata različitih normi i politika, njihovih zahtjeva te načina i potrebe njihove primjene na široj domenskoj razini). Na modelskoj razini to znači međusobnu povezanost konceptualiziranih pojmova iz dominantnih politika i normi, kao i njihovu povezanost s višim i općenitijim konceptima šireg domenskog područja, kojima mogu pripadati, što je ilustrirano i na slici 2.2 u poglavlju 2.2. o domenskoj taksonomiji.

Ontologija predstavlja formalnu specifikaciju koja se izražava jezikom čiji su rječnik, sintaksa i semantika formalno definirani. U području informacijske sigurnosti, norme i politike pisane su prirodnim jezikom u nestrukturiranom obliku dokumenata i predstavljaju neformalne specifikacije. Poluformalni pristup tipičan je samo za neke segmente politike informacijske sigurnosti, primjerice uskonamjenske politike prava pristupa korisnika informacijskom sustavu. Upravo stoga, uvođenje formalizacije pristupa u multidisciplinarno područje politika informacijske sigurnosti predstavlja motiv istraživanja i cilj ostvarenja predložene metode modeliranja.

## 5.2. Metoda modeliranja i okviri istraživanja

Na temelju uvodnih razmatranja, na slici 5.1 prikazana je metoda modeliranja i okviri ovog istraživanja, s naznačenim najvažnijim rezultatima istraživanja koji se opisuju u ovom radu. S

desne strane označene su razine domene problema i domene rješenja. Problemsku domenu predstavlja domena informacijske sigurnosti stvarnog svijeta u okviru koje se provodi analiza područja prema prikazu u četvrtom poglavlju i koja sadrži objekte modeliranja prikazane na slici 5.1.




**Slika 5.1:** Metoda modeliranja i okviri istraživanja s opisom rezultata

Procesom analize područja domene, provodi se šira domenska razina sistematizacije i integracije različitih pristupa i zahtjeva globalnog i lokalnog okruženja (četvrto poglavlje). Cilj analize je odabir dominantnih suvremenih politika i normi informacijske sigurnosti, kao i odabir temeljnog rječnika šireg domenskog područja informacijske sigurnosti. Stoga se provodi apstrakcija i generalizacija pojmova na razinu općih domenskih pojmova i procedura, kako je pojašnjeno u poglavljima 2.1. i 4.10. Takvi poopćeni domenski pojmovi, koji su dovoljno prepoznatljivi u različitim sigurnosnim zahtjevima, mogu se uz pomoć modela specijalizirati za posebne zahtjeve i primjene u različitim okruženjima u kojima se provodi politika informacijske sigurnosti. Rezultat analize prikazane u četvrtom poglavlju predstavljen

je općom domenskom taksonomijom informacijske sigurnosti, koja je temelj za ostvarenje konceptualnog metamodela sukladno primjeru na slici 2.2, tablici 4.1 i prilogu A.

Daljnja razrada domenske taksonomije provodi se u smislu specificiranja značenja domenskih pojmova, određivanja atributa, odnosno relacija između pojmova. Konceptualni metamodel razvija se u UML-u (engl. *Unified Modelling Language –UML*) [98], koji je odabran, s jedne strane zbog zahtjeva jasnoće i razumljivosti te vizualnog prikaza konceptualnog modela, a s druge strane, zbog potrebe za formalnom specifikacijom metamodela (rječnik, sintaksa i semantika koncepata) u svrhu programskog ostvarenja ontološkog metamodela. Standardni način zapisa modela u UML-u, svojim unificiranim grafičkim simbolima olakšava razumijevanje modela, što je u prethodnim razmatranjima označeno kao cilj konceptualnog metamodela. Konceptualni metamodel u ovom istraživanju predstavlja okvir za upravljanje i komuniciranje znanjem o domeni, primarno između osoba zaduženih u različitim organizacijama za poslove informacijske sigurnosti (rukovoditelji sigurnosti, savjetnici za informacijsku sigurnost i sl.), ali isto tako i između niza osoba s različitim stručnim i interesnim profilima povezanim na određeni način uz ovo multidisciplinarno područje informacijske sigurnosti (stručnjaci za različita područja sigurnosti kao što je sigurnost osoblja, fizička sigurnost, sigurnost informacijskih sustava, upravljanje rizikom, vlasnici podataka i informacijskih sustava, rukovoditelji i sl.).

Prema slici 5.1 vidljivo je da ostvareni konceptualni metamodel predstavlja konceptualizirani skup dominantnih politika i normi informacijske sigurnosti, odnosno sukladno definiciji metamodela, predstavlja model za ostvarenje drugih modela, pojedinačnih vrsta politika i normi u određenom okruženju. U svrhu provjere valjanosti postupka modeliranja, kao i za potrebu ostvarenja modela politika informacijske sigurnosti određene organizacije, na temelju konceptualnog metamodela u UML-u, programski se ostvaruje ontološki metamodel, koristeći programsko razvojno okruženje *Protégé Frames* [99]. Ovako ostvareni programski ontološki metamodel osigurava potporu za modeliranje konkretnih politika informacijske sigurnosti, koje prema slici 5.1, predstavljaju pojedine vrste politika informacijske sigurnosti iz skupa dominantnih politika i normi informacijske sigurnosti (sektorske politike informacijske sigurnosti). Na taj način ostvaruju se ontološki modeli politika informacijske sigurnosti, za studije slučajeva odabrane u ovom istraživanju, a koje prema slici 5.1 predstavljaju modele provedbe pojedine vrste politike informacijske sigurnosti u konkretnim slučajevima odabranih organizacija (državno tijelo i pravna osoba).

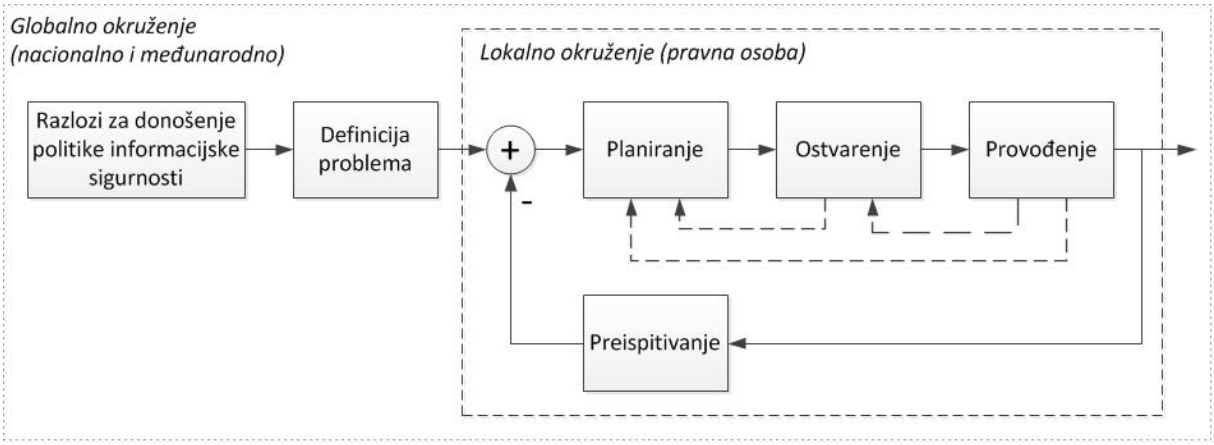
Na lijevoj strani slike 5.1 naznačene su hipoteze H1 i H2, koje predstavljaju istraživačke probleme opisane u poglavlju 1.3. Ostvarenjem konceptualnog metamodela u UML-u može se, prema H1, pokazati ostvarenje jedinstvenog šireg domenskog modela, kojeg obilježava povezanost heterogenog domenskog znanja iz dominantnih politika i normi informacijske sigurnosti, dok se programskim ontološkim modelima ostvarenim na temelju programskog ontološkog metamodela, prema H2, pokazuju tražena svojstva jednostavnijeg, dosljednijeg, sveobuhvatnijeg i učinkovitijeg upravljanja životnim ciklusom politika informacijske sigurnosti.

Metoda modeliranja politika informacijske sigurnosti temeljena na upravljanju znanjem (slika 5.1) koja se predlaže ovim radom, prema slici 2.1 mora osigurati sadržaj modela u obliku odabira domenskih pojmova (rječnik domene), odgovarajuće sistematiziranih i integriranih s obzirom na dominantne politike i norme informacijske sigurnosti u hijerarhijsku domensku taksonomiju (sintaksa domene) te detaljiziranih u svrhu razrade potrebnih atributa i relacija koncepata (semantika domene). Tako dobivena formalna specifikacija mora imati potrebnu funkcionalnost s obzirom na stvarne objekte modeliranja sa slike 5.1. Zadatak metode modeliranja jest osiguravanje okvira u kojima se provodi ostvarenje prethodno opisane formalne specifikacije, s ciljem postizanja odgovarajuće funkcionalnosti modela, koji se promatra kao složeni sustav s bitnim svojstvima i funkcionalnostima stvarnih objekata modeliranja prema slici 5.1.

## 5.3. Pretpostavke i ograničenja modeliranja

U poglavlju 4.1. definirana je politika informacijske sigurnosti kao skup procedura kojima se planira, ostvaruje, provodi i preispituje informacijska sigurnost u određenom opsegu primjene. Planiranje i ostvarenje politike informacijske sigurnosti u svojoj osnovi predstavlja preventivnu mjeru postupanja. S druge strane, provođenje politike informacijske sigurnosti predstavlja okvir za provedbu svih vrsta sigurnosnih mjera, odnosno kontrola, koje se koriste u nekom lokalnom okruženju. Preispitivanje provedene politike informacijske sigurnosti u nekom lokalnom okruženju pravne osobe podrazumijeva s jedne strane, preispitivanje ostvarenih sigurnosnih mjera gledano s aspekta unutarnjih, poslovnih i sigurnosnih zahtjeva, ali s druge strane i preispitivanje zahtjeva globalnog okruženja (zakonski sigurnosni zahtjevi, ugovorni sigurnosni zahtjevi, poslovna suradnja i razdioba osjetljivih podataka, kibernetički

prostor i sl.). Ovako definirani i opisani pojam politike informacijske sigurnosti prikazan je na slici 5.2. u obliku sustavske sheme životnog ciklusa politike informacijske sigurnosti [7].




**Slika 5.2:** Sustavska shema životnog ciklusa politike informacijske sigurnosti

S obzirom da šire domensko područje predstavlja vrlo složenu i heterogenu domenu, potrebno je na odgovarajući način prilagoditi opseg modeliranja. Jedno uvedeno ograničenje vezano je za predstavljanje šire domene informacijske sigurnosti stvarnog svijeta uz pomoć skupa dominantnih politika i normi informacijske sigurnosti (slika 5.1). S obzirom na definiciju politika informacijske sigurnosti koju koristimo u ovom radu, modeliranje će se temeljiti prvenstveno na osnovnim unutarnjim i vanjskim sigurnosnim zahtjevima te na njihovoj međusobnoj povezanosti i utjecaju na temeljne čimbenike informacijske sigurnosti: osobe, procese i tehnologiju. Koncept sigurnosnih rizika u modelu se obrađuje na nižim provedbenim razinama, odnosno povezano s lokalnim okruženjem primjene sigurnosnih kontrola. Procedure koje se provode u okvirima politika informacijske sigurnosti, kao što su različite akreditacije, certifikacije, procjene i sl., modeliraju se prema modelu crne kutije, za koje koristimo samo neka vanjska obilježja, koja su važna, gledano iz kuta politike informacijske sigurnosti kao okvira za upravljanje i komuniciranje znanjem domene. To znači da će se modelirati obilježja takvih koncepata kao što su njihova vrsta, srodnost, uloga, odgovornost, povezanost s drugim konceptima i ciljnim okruženjima i sl. (primjer za načine provedbe nadzora prikazan je na slici 2.2). Detaljni postupci od kojih se sastoje ovakve procedure definiraju se kao model crne kutije, jer je sa stanovišta politike informacijske sigurnosti važna uloga tih procedura, njihovi rezultati i povezanost s ostalim elementima modela. Ovakav pristup proizlazi i iz pojašnjenja u poglavlju 3.2., kojim je modeliranje politika informacijske sigurnosti u ovom istraživanju usmjereno na širu domensku razinu u smislu ostvarenja okvira

za upravljanje i komuniciranje znanjem o domeni, a ne na razradu pojedinih uskonamjenskih segmenata i procedura domene. S obzirom na modularni pristup razradi konceptualnog metamodela kao složenog sustava, modeliranje pojedinih procedura, u svrhu povezivanja s ovim modelom može predstavljati buduća proširenja metamodela, bilo korištenjem nekih postojećih rješenja kao u [35], ili uz pomoć modeliranja novih. U svrhu upravljanja i komuniciranja znanjem, u modelu je uvedena kategorizacija znanja u kojoj ontološki modelirani koncepti predstavljaju deklarativno znanje, relacije koje povezuju ontološki modelirane koncepte predstavljaju relacijsko znanje, dok se povezano proceduralno znanje koristi u obliku opisa prirodnim jezikom pohranjenih uz pripadajuće ontološke koncepte. Na taj način se u modelu koriste pojedini dokumenti koji predstavljaju obavezne regulativne zahtjeve (npr. određeni dokumenti koji su zahtjevi norme u okviru provedbe ISO 27001, ili pravilnici vezani za provedbu politika informacijske sigurnosti u državnom sektoru).

Upravo zbog složenosti domene istraživanja i zbog ciljeva istraživanja usmjerenih prema široj domenskoj razini upravljanja i komuniciranja znanjem, osnovni pristup modeliranju temelji se na modeliranju vanjskih pojavnosti velikog broja heterogenih domenskih pojmova. Takve domenske pojmove konceptualiziramo i modeliramo na temelju njihove međusobne povezanosti i koordinacije rada u složenom sustavu koji predstavlja metamodel politika informacijske sigurnosti.

## 5.4. Transformacija modela životnog ciklusa politika informacijske sigurnosti u hijerarhijski model domenske taksonomije

Složenost globalnog sigurnosnog okruženja razlog je zbog kojeg je problematiku politike informacijske sigurnosti potrebno promatrati u puno širem kontekstu od samog poslovno-organizacijskog okruženja [7]. Jedino na taj način stvaraju se potrebni uvjeti za pravilno postavljanje sigurnosnih odnosa u složenom globalnom (nacionalno i međunarodno) i lokalnom okruženju (pravna osoba) prikazanom na slici 5.2. Kako bi se ostvarili postavljeni ciljevi modeliranja i postigla opisana obilježja modela politika informacijske sigurnosti, potrebno je sustavsku shemu životnog ciklusa politika informacijske sigurnosti sa slike 5.2 transformirati na odgovarajući način. Slika 5.2 prikazuje životni ciklus politika informacijske sigurnosti u kojem su ključni elementi odlučivanja (definicija i razlozi donošenja) povezani s globalnim okruženjem. Iz analize provedene u poglavlju 4. proizlazi da je primjena

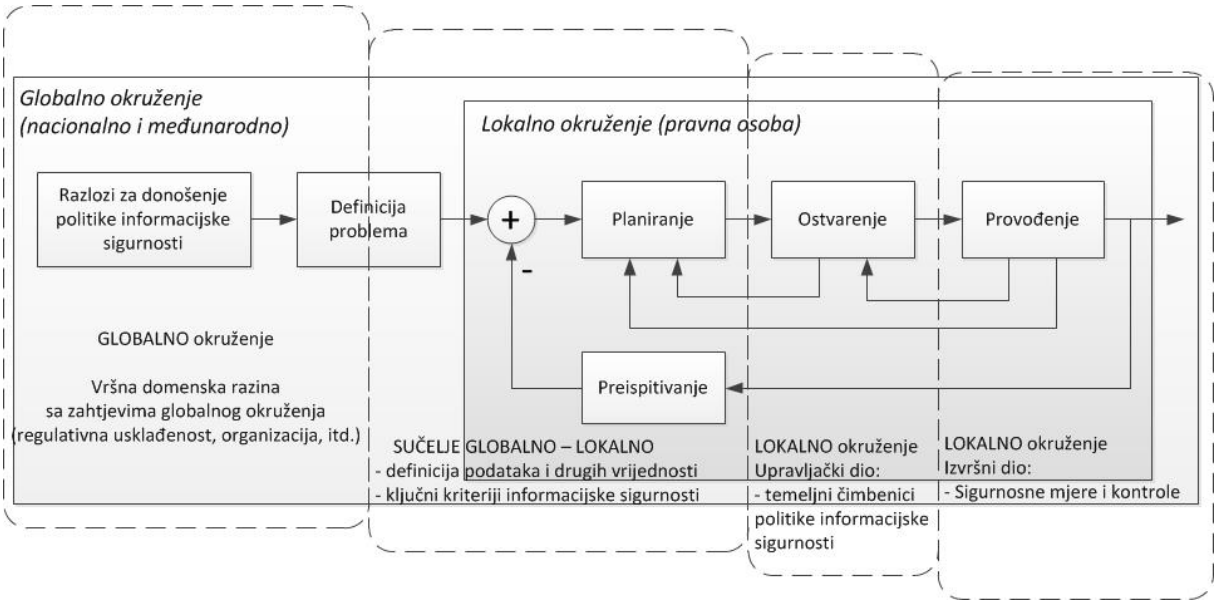
suvremenih politika informacijske sigurnosti u različitim sektorima društva i dalje usmjerena na lokalno okruženje, što se pokazalo kao uzrok niza uočenih nedostataka, od uskonamjenskog i nepovezanog korištenja segmenata politika informacijske sigurnosti, do sektorski specifičnih pristupa sigurnosnim zahtjevima. Takav pristup nije pogodan za širi domenski pogled koji je cilj ovog istraživanja. Globalno okruženje u suvremenom društvu diktira razloge za donošenje politika informacijske sigurnosti (npr. međunarodni i nacionalni zakonski zahtjevi, poslovna suradnja i razdioba osjetljivih podataka, kibernetički prostor) i time definira zahtjeve i ograničenja za sve vrste sektorskih politika informacijske sigurnosti u lokalnim okruženjima. Životni ciklus politike informacijske sigurnosti stoga je nužno promatrati u okvirima globalnog okruženja prema slici 5.2.

U svrhu daljnje razrade domenskog rječnika u hijerarhijsku taksonomiju domene (od općeg prema posebnom – specijalizacija) sustavsku shemu sa slike 5.2 potrebno je transformirati u pogodniji prikaz. Prema dosadašnjem opisu, novim prikazom potrebno je omogućiti razradu zahtjeva globalnog okruženja s obzirom na životni ciklus politika informacijske sigurnosti, pri čemu koristimo dominantne politike i norme informacijske sigurnosti kao specifičnosti lokalnog okruženja koje želimo modelirati unutar šireg globalnog okruženja, a cjelokupni prikaz prilagođavamo potrebama ostvarenja hijerarhijske domenske taksonomije, koja oblikuje sadržaj modela. Ovakva transformacija sustavske sheme životnog ciklusa politika informacijske sigurnosti u složeni sustav kojim će se modelirati politike informacijske sigurnosti, prikazana je na slici 5.3 [100]. Na slici 5.3 prikazane su glavne organizacijske razine složenog sustava na temelju kojeg se ostvaruje konceptualni metamodel:

- globalno okruženje, koje predstavlja vršnu domensku razinu i sadrži osnovne zahtjeve globalnog okruženja (npr. regulativna usklađenost, organizacija);
- sučelje između globalnog i lokalnog okruženja predstavljeno definicijama podataka i drugih vrijednosti, odnosno ključnim kriterijima informacijske sigurnosti;
- lokalno okruženje predstavljeno s dvije razine: upravljačkom razinom s odabranim ključnim čimbenicima politika informacijske sigurnosti, te izvršnom razinom sa sigurnosnim mjerama i kontrolama.

Sukladno ciljevima iz uvoda petog poglavlja, a na temelju poglavlja 2.4., sustavski pristup modeliranju politika informacijske sigurnosti, kao složenog sustava kojeg čine heterogeni elementi i procesi koji su međusobno povezani, opisuje se na svim relevantnim razinama organizacije, kako bi modeliranje obuhvatilo potrebnu povezanost između sustava i okoline,

ali i međusobnu povezanost elemenata sustava na unutarnjim organizacijskim razinama sustava.




**Slika 5.3:** Transformacija sustavske sheme životnog ciklusa politike informacijske sigurnosti za potrebe razvoja hijerarhijske domenske taksonomije

Vršna domenska razina sa slike 5.3 treba osigurati odgovarajuća funkcionalna i međusektorska obilježja konceptualnog metamodela, odnosno implicitno izraženo znanje, definirano u uvodu petog poglavlja, na temelju analize u poglavlju 3.2. Radi se o međusobno sličnim konceptima iz različitih dominantnih normi i politika informacijske sigurnosti te njihovim zahtjevima, načinima i potrebama primjene, apstrahiranim i generaliziranim na širu domensku razinu prema definicijama u poglavlju 2.1.

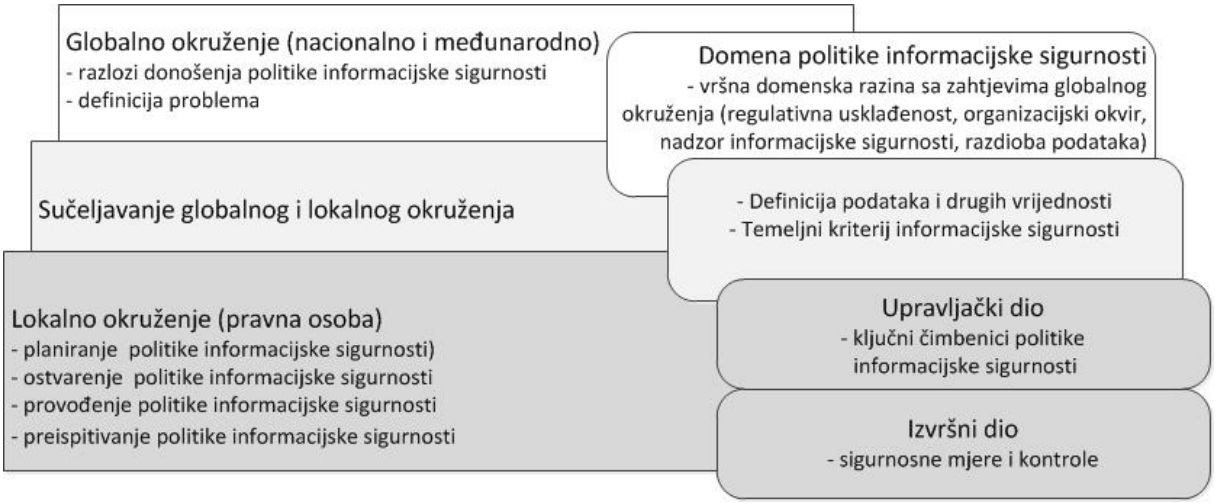
Transformacijom se prilagođava shema složenog sustava koji se modelira potrebama razvoja hijerarhijske domenske taksonomije i primjeni ontoloških metoda modeliranja koncepata, zadržavajući pri tome temeljna sustavska svojstva životnog ciklusa politika informacijske sigurnosti u globalnom okruženju, prema slici 5.2. Konceptualni metamodel zamišljen je kao skup međusobno povezanih podsustava koji opisuju pojedine segmente iz domene politike informacijske sigurnosti. Većina suvremenih zahtjeva informacijske sigurnosti proizlazi izravno ili neizravno iz globalnog okruženja (npr. regulativni zahtjevi, poslovna suradnja, kibernetički prostor i sl.), a lokalna okruženja pri tome predstavljaju različite pravne osobe, odnosno organizacije koje pripadaju određenim sektorima društva (npr. državni sektor, odnosno poslovni sektor). Politika informacijske sigurnosti različitih organizacija proizlazi s jedne strane, iz lokalno prepoznatih sigurnosnih rizika i potreba poslovnih procesa, a s druge

strane, iz sigurnosnih zahtjeva stupa sektorskog poslovanja kojemu organizacija pripada. S obzirom na zajedničko globalno okruženje, globalni procesi postupno dovode do sve veće sličnosti u sigurnosnim zahtjevima za ova lokalna okruženja, osobito u slučajevima kada je potrebna sigurnosna suradnja ili razdioba osjetljivih podataka između različitih organizacija koje pripadaju različitim sektorima društva ili različitim nacionalnim i međunarodnim okruženjima. Različitosti u politikama informacijske sigurnosti ipak postoje i najvidljivije su u nižim organizacijskim slojevima, napose u izvršnom dijelu lokalnog okruženja sa slike 5.3.

Na temelju transformacije sustavske sheme prikazane na slici 5.3, daljnjom razradom su odabrane funkcionalne grupe aktivnosti tipične za politike informacijske sigurnosti. Ove grupe aktivnosti formirane su od opće globalne razine prema posebnoj lokalnoj razini. Tako je razrađena hijerarhija organizacijskih slojeva ovog složenog sustava, potrebna za formiranje konceptualnog metamodela, što je prikazano na slici 5.4 [100]. S lijeve strane slike 5.4 prikazana je organizacijska hijerarhija sustavskom terminologijom sa slike 5.2, a s desne strane slike razrađeni su novi organizacijski slojevi sukladno transformaciji pokazanoj na slici 5.3, koji će se koristiti u daljnjem razvoju konceptualnog metamodela. Tako se na slici 5.4 s desne strane vide definirane organizacijske razine konceptualnog metamodela:

- domena politike informacijske sigurnosti - vršna domenska razina sa zahtjevima globalnog okruženja (regulativna usklađenost, organizacijski okvir, nadzor informacijske sigurnosti, razdioba podataka);
- sučelje globalnog i lokalnog okruženja - definicija podataka i drugih vrijednosti i temeljnih kriterija informacijske sigurnosti;
- upravljački dio lokalnog okruženja - temeljni čimbenici politike informacijske sigurnosti;
- izvršni dio lokalnog okruženja - sigurnosne mjere i kontrole.

Niz utjecaja globalnog okruženja opisan je i pojašnjen u prethodnim poglavljima rada, a ovdje je obuhvaćen uvođenjem četiri podsustava vršne domenske razine. Podsustav regulativne usklađenosti obuhvaća široki skup zahtjeva, od zakonskih, preko sektorskih, do ugovornih obaveza; podsustav organizacijskog okvira utvrđuje niz nadležnih sigurnosnih tijela, izravno ili neizravno povezanih s područjem informacijske sigurnosti (npr. NSA hijerarhija, CERT hijerarhija, nacionalno tijelo za zaštitu osobnih podataka, itd.); podsustav nadzora informacijske sigurnosti djelomice je ilustriran taksonomijom na slici 2.2; podsustav razdiobe podataka razrađuje koncepte poslovne i javne razdiobe podataka.




**Slika 5.4:** Formiranje podsustava konceptualnog metamodela politika informacijske sigurnosti

Kao što je već pojašnjeno, svrha organizacijskih razina složenog sustava je osiguravanje unutarnjih veza između različitih elemenata složenog sustava, kako veza između koncepata politike informacijske sigurnosti i čimbenika globalnog okruženja (vršni sloj), tako i veza između unutarnjih čimbenika politika informacijske sigurnosti: osoba, procesa i informacijskih sustava (donja dva sloja). Pri tome na svakoj organizacijskoj razini imamo više podsustava koji predstavljaju funkcionalnosti ovih razina. Poveznicu između globalnog i lokalnog okruženja čine podatci i druge vrijednosti koje se štite politikama informacijske sigurnosti, na temelju postavljenih kriterija informacijske sigurnosti (temeljni kriteriji povjerljivosti, cjelovitosti i raspoloživosti). Razlog tome je pojašnjen u poglavlju 4.5. na temelju povezanosti koncepata sigurnosti podataka i sigurnosti kibernetičkog prostora preko kojeg se tim podatcima komunicira, odnosno u poglavlju 4.2.2., u zaključku o bitnom utjecaju domena podataka i globalne komunikacijske i informacijske infrastrukture na politike informacijske sigurnosti. Tako je proizašlo da su i politike informacijske sigurnosti u smislu njihove definicije u ovom radu, kao koncept usko povezane i nedjeljive od sigurnosti podataka (domene podataka prikazane su na slici 4.2) i sigurnosti kibernetičkog prostora, jednako kao što su ova dva koncepta međusobno usko povezana i nedjeljiva u okvirima suvremenog društva.

U svrhu dodatne provjere kompletnosti sigurnosnih funkcionalnosti konceptualnog metamodela sa slike 5.4, koristi se usporedba preko slojeva sigurnosne arhitekture [23]. Slojevi sigurnosne arhitekture povezuju se s pripadnim segmentima politike informacijske

sigurnosti, odnosno prethodno razvijenim podsustavima konceptualnog metamodela prema slikama 3.2, 5.2 i 5.4. Za svaki općeniti sloj sigurnosne arhitekture utvrđuju se usporedivi slojevi sustavske sheme životnog ciklusa politika informacijske sigurnosti i slojevi konceptualnog metamodela, što je prikazano u tablici 5.1.

**Tablica 5.1:** Usporedni prikaz slojeva sigurnosne arhitekture, slojeva sustavske sheme životnog ciklusa politika informacijske sigurnosti i slojeva konceptualnog metamodela

| | **Slojevi sigurnosne arhitekture (slika 3.2)** | **Sustavska shema politika informacijske sigurnosti (slika 5.2)** | **Slojevi konceptualnog metamodela (slika 5.4)** |
|---|---|---|---|
| 1. | Kontekstualni pogled (Zašto?) | Globalno okruženje (Razlozi za donošenje) | Globalno okruženje (Vršna domenska razina) |
| 2. | Konceptualni pogled (Što?) | Globalno okruženje (Definicija problema) | Globalno okruženje (Sučeljavanje globalno – lokalno) |
| 3. | Logički pogled (Kako?) | Lokalno okruženje (Planiranje, preispitivanje) | Lokalno okruženje (Upravljački dio) |
| 4. | Fizički pogled (Tko?) | Lokalno okruženje (Ostvarenje, provođenje) | Lokalno okruženje (Izvršni dio) |
| 5. | Pogled na komponente (Gdje?) | Lokalno okruženje (Ostvarenje, provođenje) | Lokalno okruženje (Izvršni dio) |
| 6. | Operativni pogled (Kada?) | Lokalno okruženje (Ostvarenje, provođenje) | Lokalno okruženje (Izvršni dio) |

## 5.5. Usporedba dominantnih normi i politika informacijske sigurnosti

Cilj razrade konceptualnog metamodela metodom modeliranja sa slike 5.1 je predstavljanje šire domenske razine područja informacijske sigurnosti. Šira domenska razina ograničava se usmjeravanjem na skup dominantnih suvremenih politika informacijske sigurnosti, u kojima se, na temelju analize prikazane u poglavlju 4., apstrahira i generalizira vršne koncepte. Ovi koncepti se prema konkretnim potrebama modeliranja na odgovarajući način specijaliziraju u koncepte ciljanih organizacijskih okruženja koji će predstavljati modele dobivene na temelju zajedničkog metamodela. Da bi se ovaj proces konceptualizacije mogao provesti, nužno je utvrditi strukturu metamodela, koja mora biti usklađena s funkcionalnostima stvarnih objekata modeliranja. Stoga se u razradi metode modeliranja kreće od sustavske sheme životnog ciklusa politika informacijske sigurnosti, koja se proširuje povezanošću s globalnim okruženjem prema slici 5.2. Ova shema je u nastavku razrade metode, transformirana u prikaz prikladniji za razvoj hijerarhijske domenske taksonomije, prema slici 5.3. Pored prikladnosti za hijerarhijski domenski prikaz, ovdje se uvode četiri organizacijske razine složenog sustava,

koje će osigurati pravilnu razdiobu na podsustave modela, kao i potrebno povezivanje složenih unutarnjih veza heterogenih koncepata koji se modeliraju. Pored toga, ove organizacijske razine osiguravaju modeliranje lokalnog okruženja unutar šire domenske razine i ostvarenje, ne samo složenih unutarnjih veza, već i njihovo povezivanje s vršnim slojem modela, koji sadržava potrebne koncepte globalnog okruženja bitne za modeliranje politika informacijske sigurnosti (slika 5.4).

Prije nastavka postupka modeliranja pojašnjenjem razrade domenske taksonomije i ontološkog oblikovanja koncepata, analizirat će se uloga podsustava konceptualnog metamodela politika informacijske sigurnosti prikazanih na slici 5.4., u dominantnim normama i politikama informacijske sigurnosti. Provodi se usporedba odabranih dominantnih politika i normi informacijske sigurnosti iz suvremene prakse, prema elementima koji su odabrani za podsustave konceptualnog metamodela i koji su prikazani s desne strane slike 5.4. Ova usporedba prikazana je u tablici 5.2, za šest odabranih vrsta politika i normi informacijske sigurnosti koje zadovoljavaju načelo dominantnosti, s obzirom na utjecaj u suvremenoj praksi informacijske sigurnosti, a na temelju analize opisane u poglavlju 4. U tablici 5.2 prikazana je analiza sadržaja odabranih politika i normi informacijske sigurnosti na kvalitativan način, s četiri razine stanja podržanosti odabranih područja za podsustave konceptualnog metamodela. U tablici su bijelom pozadinom prikazani slučajevi u kojima politika ili norma, označena s lijeve strane tablice, sadržajno ne obuhvaća segment aktivnosti u nekom od podsustava konceptualnog metamodela, označenom na vrhu tablice. S tri razine sive pozadine, prikazani su slučajevi kada politika ili norma s lijeve strane tablice, podržava u uskom segmentu (svjetlo siva pozadina), većinom podržava (srednje siva pozadina) ili potpuno podržava (tamno siva pozadina), segment sadržaja u nekom od podsustava konceptualnog metamodela, označenim na vrhu tablice.

NATO politika informacijske sigurnosti [75] u najvećoj mjeri je usmjerena na klasificirane NATO podatke i sukladno prikazu na slici 4.3 te provedenoj analizi u ovom radu, predstavlja dominantnu i utjecajnu kategoriju. S jedne strane dominantnost se pokazuje kroz utjecaj na razvoj drugih politika i normi informacijske sigurnosti, a s druge strane preko 28 država članica NATO-a, s usklađenim nacionalnim politikama informacijske sigurnosti u državnom sektoru te uspostavljenom gospodarskom suradnjom, koja suradnju nacionalnog poslovnog sektora na nizu civilnih i vojnih NATO programa povezuje mogućnostima sklapanja klasificiranih ugovora, uz uvjet sukladnosti politika informacijske sigurnosti. Tome se može

dodati još dvostruko veći broj zemalja, koje s NATO-om surađuju u različitom obliku partnerske suradnje, koji također traži usklađivanja nacionalnih politika informacijske sigurnosti te omogućava određeni obim gospodarske suradnje. Slično se može reći i za EU politiku informacijske sigurnosti [73], koja ima kraću povijest prema poglavlju 4. i slici 4.3, ali na svoje zemlje članice i zemlje partnere, utječe puno šire, s obzirom da obim suradnje u okviru koje se koriste klasificirani podatci zahvaća sve resore državne uprave. Suprotno tome, politika informacijske sigurnosti NATO-a, nacionalno se profilira kroz osjetno manji dio državnih tijela.

**Tablica 5.2:** Usporedba dominantnih politika informacijske sigurnosti s obzirom na sadržaje koje definiraju u područjima odabranima za podsustave konceptualnog metamodela

| | **Globalno okruženje** | | | | **Sučeljavanje** | | **Lokalno okruženje** | |
|---|---|---|---|---|---|---|---|---|
| **Politike i norme inf. sigurnosti** | Organi-zacijski okvir | Razdioba podataka | Regulativ-na usklađe-nost | Nadzor inf. sigur-nosti | Definici-ja podataka | Krite-riji inf. sig. | Upra-vljački dio | Izvršni dio |
| NATO klasificirani podatci [75] | ✓ | ✓ | - | ✓ | - + | ✓ | ✓ | - + |
| EU klasificirani podatci [73] | ✓ | - + | - | ✓ | - + | ✓ | ✓ | + |
| NIST norma SP800-53 [85] | + | + | + | + | + | ✓ | ✓ | + |
| KATAKRI norma revi-zije [101] | + | - | + | + | + | ✓ | ✓ | + |
| ISO 27001 [27] | - + | - | + | - + | + | ✓ | ✓ | + |
| EU osobni podatci [93, 95] | ✓ | ✓ | - + | ✓ | - + | + | - + | - + |

**Oznake u tablici:**
- \- nije podržano (bijela pozadina)
- -+ podržano u uskom segmentu (svjetlo siva pozadina)
- \+ većinom podržano (srednje siva pozadina)
- ✓ podržano (tamno siva boja)

NIST norme informacijske sigurnosti SAD-a [85], odabrane su kao prijelaz iz državnog sektora u poslovni sektor, ali i kao odličan primjer naprednih nacionalnih normi informacijske sigurnosti. Razvijene države u odnosu na primjere NATO-a i EU-a, znatno lakše mijenjaju i prilagođavaju svoje nacionalne politike informacijske sigurnosti, jer su i NATO i EU opterećeni potrebom postizanja konsenzusa svih država članica u prihvaćanju promjena, što

može biti vrlo spor proces. Finska norma revizije za područje informacijske sigurnosti KATAKRI [101], također povezuje u određenoj mjeri politiku informacijske sigurnosti državnog sektora s poslovnim sektorom. Razlog donošenja ove norme bio je propisivanje norme revizije za potrebe suradnje poslovnog i državnog sektora (klasificirani ugovori), ali također i pokušaj da se u određenoj mjeri poveže raširenu primjenu norme ISO 27001 u poslovnom sektoru te prikažu ključne razlike u pristupu u odnosu na tradicionalnu politiku informacijske sigurnosti državnog sektora u Republici Finskoj kao članici EU. U tablici je kao ključna norma prikazana i međunarodna norma ISO 27001 [27], kao norma koja je prema opisima u prethodnim poglavljima, najčešći odabir u području informacijske sigurnosti u različitim sektorima gospodarstva, ali i u državnom sektoru, odnosno u području zaštite osobnih podataka. U posljednjem retku tablice nalazi se suvremeni pristup zaštiti osobnih podataka [93, 95], prema planovima koji se ubrzano pripremaju za provedbu na razini nacionalnih prostora svih država članica EU-a i razlozima širokog utjecaja na politike informacijske sigurnosti, koji su detaljnije opisani u poglavlju 4.9.2.

U daljem tekstu, ukazuje se na najvažnije zaključke, koji se mogu donijeti na temelju ovog kvalitativnog prikaza u tablici 5.2, za potrebe konceptualizacije domenskog područja i ostvarenja konceptualnog metamodela. Iz tablice 5.2 može se vidjeti kako postoji vrlo malo bijelih polja u tablici, tj. segmenata za koje vrijedi da nisu podržani u odabranim politikama i normama informacijske sigurnosti (manje od 10%). Ovo potvrđuje praktičnu primjenjivost (podržanost sadržaja podsustava) strukture konceptualnog metamodela s predloženim izborom podsustava prema slici 5.4, u širem domenskom području predstavljenom dominantnim normama i politikama informacijske sigurnosti prema tablici 5.2. U tablici je vidljiva i grupiranost najvećeg broja tamno sivih polja (segmenti koji su potpuno podržani) u nižim slojevima modela (sučeljavanje i lokalno okruženje), što je očekivani rezultat (oko 60% tamno sivih polja) i potvrđuje ispravnost ovakvog načina pregleda stanja, jer su svi, povijesno vrlo različiti pristupi informacijske sigurnosti, nastali upravo oko ovdje pozicioniranih sadržaja kao što su kriteriji informacijske sigurnosti (povjerljivost, cjelovitost, raspoloživost) i temeljni čimbenici informacijske sigurnosti (osobe, procesi, tehnologija). Ostatak tamno sivih polja grupiran je u redcima NATO-a i EU-a u gornjem dijelu tablice 5.2 te u posljednjem retku sa zaštitom osobnih podataka EU-a. U slučaju NATO-a i EU-a, to je rezultat tradicionalno čvrstog propisivanja organizacijskog i nadzornog okvira u politikama informacijske sigurnosti međunarodnih organizacija. Nadalje, NATO je napravio veliki iskorak tijekom razdoblja operacije ISAF u Afganistanu, u reguliranju koncepata razdiobe

klasificiranih i osjetljivih podataka, u vjerojatno najsloženijem prostoru mirovne operacije ikada, s obzirom na brojnost različitih vrsta organizacijskih entiteta koji tamo surađuju u zajedničkim vojnim i civilnim operacijama. Novi pristup EU-a u zaštiti osobnih podataka, uvodi upravo u ovim segmentima (razdioba podataka te organizacijski okvir i nadzor) vrlo jasna i unificirana pravila. Najbolje izbalansirani rezultat u tablici 5.2 daje NIST norma, iako je namijenjena prvenstveno sigurnosti informacijskih sustava, dok ostale norme obuhvaćaju širu problematiku informacijske sigurnosti. Razlog je taj što se radi o nacionalnoj normi SAD-a kao vodeće države, ne samo u području informacijske sigurnosti, već i u čitavom nizu povezanih sigurnosnih i tehnoloških područja s jedne strane, a s druge strane, u tome da NIST norma razrađuje opise sigurnosnih kontrola detaljnije od ostalih normi i politika, uspijevajući pri tome zadržati dobru ravnotežu između općenitosti i specijalizacije kontrola, te između pristupa minimalnim sigurnosnim mjerama i upravljanja rizikom, prema opisu u poglavlju 4.6.2. Norma ISO 27001, u odnosu na NIST normu je općenitija, osobito u dijelu razdiobe podataka, ali i u dijelu organizacijskog okvira i nadzora. Upravo zbog takve općenitosti, izuzetno je pogodna za primjenu i najraširenija u različitim poslovnim sektorima, državnom sektoru, te nacionalnim i međunarodnim okruženjima.

Analizom ilustriranom u tablici 5.2 može se vidjeti i da su politike i norme u primjeni većim dijelom usko usmjerene na organizacijsku i sigurnosnu problematiku unutar opsega primjene u kojemu su nastale i u kojem se najčešće primjenjuju. S druge strane, suvremeni zahtjevi kibernetičkog prostora i globalizacije društva, nužno stavljaju organizacijske entitete koji provode politiku informacijske sigurnosti u znatno šire, i velikim dijelom međusobno povezane okvire primjene. Takvi širi okviri uključuju korištenje globalne infrastrukture kibernetičkog prostora, kao i povremenu ili stalnu suradnju i razdiobu osjetljivih podataka, te stoga imaju različit doseg utjecaja u slučaju mogućih povreda sigurnosti (poslovni značaj, nacionalna sigurnost, zaštita osobnih podataka klijenata i zaposlenika i sl.) i samim time različite i specifične sigurnosne zahtjeve. Usporedni prikaz u tablici 5.2 bitan je zbog provjere valjanosti strukture konceptualnog metamodela, s obzirom na mogućnost obuhvaćanja sadržaja odabranih dominantnih normi i politika informacijske sigurnosti, ali i s obzirom na razradu općenitijih domenskih koncepata, upravo u segmentu nužne povezanosti ovih različitih pristupa, prikazanih u tablici 5.2.

## 5.6. Ontološko oblikovanje sadržaja metamodela

Pristup razradi taksonomije mora pratiti vanjsku pojavnost različitih elemenata od interesa na razinama unutar podsustava metamodela (najviše relacija koncepti imaju sa srodnim konceptima unutar podsustava) i to s obzirom na utjecaje globalnog (relacije s gornjim slojevima modela) i lokalnog sigurnosnog okruženja (relacije s donjim slojevima modela) na sadržaje politike informacijske sigurnosti. U razvoju unutarnjih sadržaja podsustava konceptualnog metamodela sa slike 5.4, koristimo ontološki pristup modeliranja uz pomoć dekompozicije neformalnih pitanja sposobnosti [16] te na ovaj način postižemo potrebnu razinu detalja u pojedinim segmentima domene. Neformalna pitanja sposobnosti predstavljaju zahtjeve za razradu sposobnosti koje konceptualni metamodel treba zadovoljavati (tablice 5.3 i 5.4). Na ovaj način formira se skup zahtjeva za razradu taksonomije pojmova unutar pojedinih podsustava konceptualnog metamodela politika informacijske sigurnosti, sukladno prethodno ostvarenoj strukturi modela prema slici 5.4.

Hijerarhije taksonomije unutar pojedinih podsustava, nastavljaju se razrađivati dekompozicijom neformalnih pitanja sposobnosti prema tablici 5.4., sve do željene razine detalja pojedinih podsustava. Potpuna razrada konceptualizacije za tako dobivenu hijerarhijsku domensku taksonomiju, obuhvaća i definiranje atributa i relacija koncepata što se prikazuje u šestom poglavlju zapisom u UML-u, kojim se specificira konceptualni metamodel u UML-u, sukladno predloženoj metodi prikazanoj na slici 5.1.

**Tablica 5.3:** Podsustavi metamodela i neformalna pitanja sposobnosti

| | **Podsustavi metamodela** | **Neformalna pitanja sposobnosti** |
|---|---|---|
| 1. | Domena politike inf. sigurnosti | Vrsta organizacije i uloga u politici inf. sigurnosti? |
| 2. | Regulativna usklađenost | Regulativni zahtjevi i povrede sigurnosti? |
| 3. | Razdioba podataka | Vrste i obilježja razdiobe podataka? |
| 4. | Nadzor informacijske sigurnosti | Obilježja procesa nadzora i načini provedbe? |
| 5. | Organizacijski okvir | Vrste nadležnih tijela? |
| 6. | Definicija podataka i drugih vrijednosti | Štićene vrijednosti i doseg utjecaja povrede sigurnosti? |
| 7. | Kriteriji informacijske sigurnosti | Vrste kriterija informacijske sigurnosti? |
| 8. | Upravljački dio | Vrste temeljnih čimbenika informacijske sigurnosti? |
| 9. | Izvršni dio | Vrste provedbenih sigurnosnih mjera? |

**Tablica 5.4:** Dekompozicija neformalnih pitanja sposobnosti

| | **Neformalna pitanja sposobnosti** | **Dekompozicija pitanja** |
|---|---|---|
| 1. | Vrsta organizacije i uloga u politici informacijske sigurnosti? | Elementi ustroja organizacije?<br>Temeljne uloge osoba na razini organizacije? |
| 2. | Regulativni zahtjevi i povrede sigurnosti? | Vrste regulativnih zahtjeva koji sadrže sigurnosne zahtjeve?<br>Vrste povreda sigurnosti s obzirom na posljedice? |
| 3. | Vrste i obilježja razdiobe podataka? | Organizacija poslovne razdiobe podataka?<br>Vrste i obilježja javne razdiobe podataka? |
| 4. | Obilježja procesa nadzora i načini provedbe? | Obilježja metoda, opsega i vrsta procesa nadzora?<br>Razrada načina provedbe nadzora? |
| 5. | Vrste nadležnih tijela? | Vrste organizacijskih hijerarhija sigurnosnih tijela u državnom sektoru?<br>Ostala koordinacijska i operativna tijela? |
| 6. | Štićene vrijednosti i doseg utjecaja povrede sigurnosti? | Materijalna i nematerijalna imovina?<br>Kategorizacija podataka?<br>Vrste dosega utjecaja povreda sigurnosti? |
| 7. | Vrste kriterija informacijske sigurnosti? | Raščlamba temeljnih, dodatnih i ostalih kriterija informacijske sigurnosti? |
| 8. | Vrste temeljnih čimbenika informacijske sigurnosti? | Definicija osoba?<br>Definicija informacijskih sustava?<br>Definicija fizičke sigurnosti? |
| 9. | Vrste provedbenih mjera? | Raščlamba zaštite klasificiranih podataka i pristupa uz pomoć minimalnih sigurnosnih mjera?<br>Proces odabira sigurnosnih kontrola na temelju procjene rizika i povezanosti imovine, ranjivosti i prijetnji?<br>Koncepti zaštite osobnih podataka? |

## 5.7. Razrada hijerarhijske domenske taksonomije pojmova

Ostvarenje konceptualnog metamodela sa slike 5.1, temelji se na razradi hijerarhijske domenske taksonomije, pojašnjenoj u poglavlju 2.2. U domenskoj taksonomiji želi se obuhvatiti širu domensku razinu, predstavljenu dominantnim normama i politikama informacijske sigurnosti, odnosno poopćenim konceptima koji iz njih proizlaze. Ovi poopćeni vršni koncepti, već su opisani kao implicitno znanje domene, ili znanje o načinu i ulozi određenog eksplicitnog koncepta iz pojedinačne norme ili politike. Tako poopćeni koncepti mogu se prema potrebi ciljanog organizacijskog okruženja koje provodi politiku informacijske sigurnosti, specijalizirati u koncept koji će zadovoljiti pojedine vrste politika informacijske sigurnosti ciljanog okruženja. Pri tome, takvi specijalizirani koncepti trebaju nasljeđivati opća obilježja iz hijerarhijski viših koncepata, dok im se unosom podataka okruženja oblikuju svojstva potrebna za ciljano okruženje. Primjer ovakvog pristupa

domenskoj taksonomiji već je prikazan na slici 2.2, na temelju podsustava nadzora informacijske sigurnosti iz sloja globalnog okruženja sa slike 5.4.

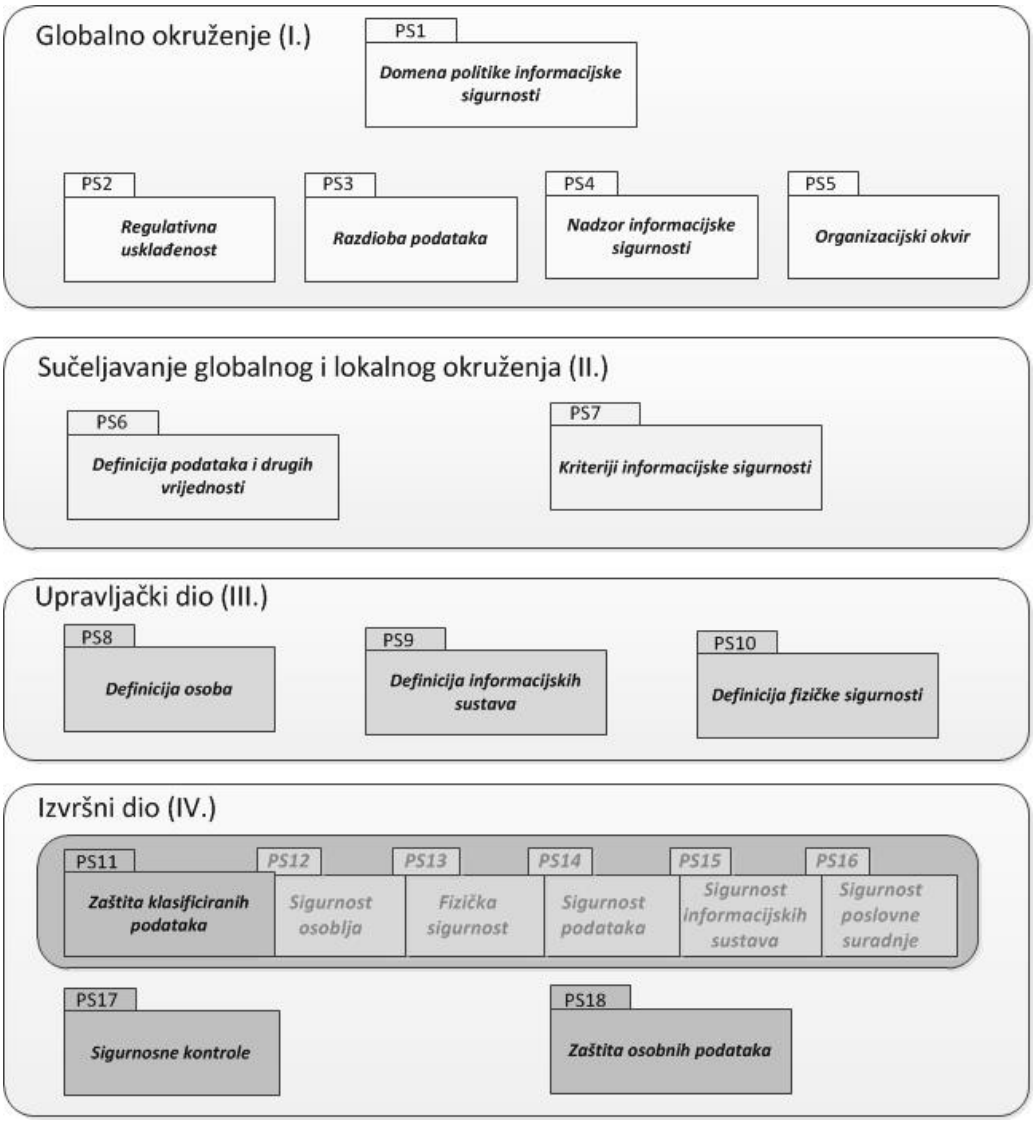
Koristeći metodu ontološkog oblikovanja za daljnju razradu sadržaja hijerarhijske domenske taksonomije, na temelju opće domenske taksonomije prikazane u tablici 4.2 i prilogu A, te na temelju ostvarene strukture konceptualnog metamodela u poglavlju 5.4., ostvarena je hijerarhijska domenska taksonomija za skup dominantnih politika i normi informacijske sigurnosti definiranih u poglavlju 5.5. U tablici 5.5 prikazan je primjer dijela ostvarene hijerarhijske domenske taksonomije koja se sastoji od hijerarhije pojmova, kategorizirane prema odabranim podsustavima metamodela (daljnja razrada prethodno uvedene četiri razine složenog sustava). Ostvarena hijerarhijska domenska taksonomija skupa dominantnih politika i normi informacijske sigurnosti u cijelosti je prikazana u prilogu B. Svakom pojmu u hijerarhiji (tablica 5.5 i prilog B), pridružen je odgovarajući domenski koncept s opisom značenja, čime se osigurava domenski valjana interpretacija svakog pojma, u skladu sa značenjem koje se koristi za taj pojam u okviru metode modeliranja predložene u radu.

**Tablica 5.5:** Primjer dijela hijerarhijske domenske taksonomije skupa dominantnih politika i normi informacijske sigurnosti

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| **PODSUSTAV PS1: DOMENA POLITIKE INFORMACIJSKE SIGURNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Domena politike informacijske sigurnosti | *Obuhvaća politiku informacijske sigurnosti kroz životni ciklus (planiranje, ostvarenje, provođenje i preispitivanje) te globalno i lokalno okruženje organizacije koja provodi politiku informacijske sigurnosti;* |
| 2. | • Organizacijski entitet | *Organizacija koja provodi politiku informacijske sigurnosti ili organizacija koja surađuje;* |
| 3. | • Organizacija provoditelj politike | *Organizacija koja provodi politiku inf. sigurnosti;* |
| 4. | • Organizacija koja surađuje | *Organizacija koja surađuje u provedbi politike informacijske sigurnosti;* |
| 5. | • Vlasnik | *Vlasnik organizacijskog entiteta;* |
| 6. | • Rukovoditelj | *Rukovoditelj organizacijskog entiteta;* |
| 7. | • Ustrojstvena cjelina | *Ustrojstvena jedinica organizacijskog entiteta;* |
| **PODSUSTAV PS2: REGULATIVNA USKLAĐENOST** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Regulativni zahtjev | *Sastoji se od taksonomije koja osigurava strukturirani pristup analizi i primjeni regulativnih zahtjeva kroz proces planiranja koji obuhvaća zakonske, sektorske i ugovorne zahtjeve;* |
| 2. | • Zakonski zahtjev | *Planiranje i provedba informacijske sigurnosti obuhvaća niz zakonskih zahtjeva propisanih u različitim vrstama zakonskih i podzakonskih akata, odnosno međunarodnih ugovora;* |

# 6. OSTVARENJE KONCEPTUALNOG METAMODELA POLITIKA INFORMACIJSKE SIGURNOSTI

Na slici 6.1 prikazana je struktura konceptualnog metamodela razrađena u prethodnim koracima modeliranja u petom poglavlju. Daljnja razrada konceptualizacije dominantnih normi i politika informacijske sigurnosti, kao i domenske taksonomije pojmova, temelji se na okvirima i strukturi ovako koncipiranog metamodela koji se ontološkim metodama oblikovanja popunjava konceptualiziranim sadržajima i razrađuje u UML-u (rječnik, sintaksa i semantika koncepata).

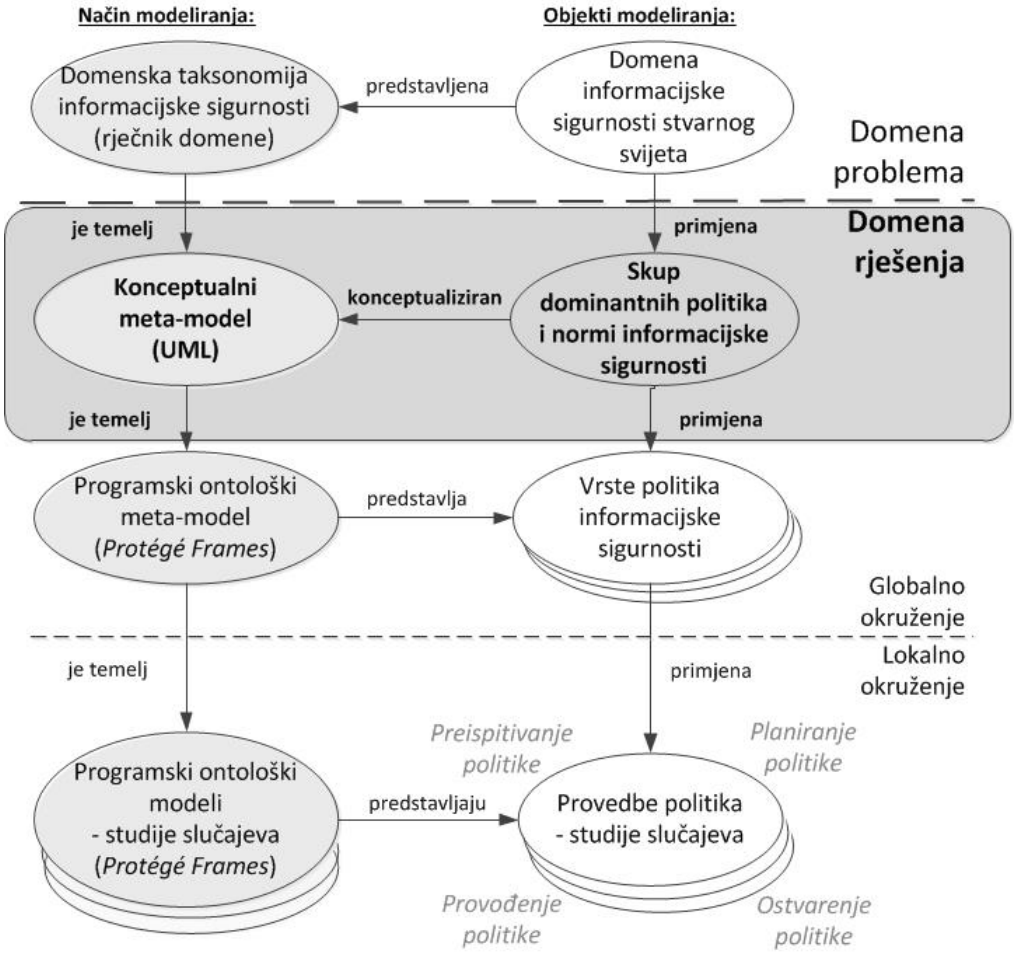



**Slika 6.1:** Struktura podsustava konceptualnog metamodela politika informacijske sigurnosti ostvarenog u UML-u

Vršni slojevi modela sa slike 6.1 prethodno su pojašnjeni u petom poglavlju, pa će se daljnje pojašnjenje usmjeriti na donje slojeve modela. U upravljačkom dijelu vidljiv je odabir tri podsustava koji obuhvaćaju definicije: osoba, informacijskih sustava i fizičke sigurnosti. Na slici 5.4 ovaj dio metamodela rezerviran je za temeljne čimbenike politike informacijske sigurnosti (osobe, procesi i tehnologija). S obzirom da je model podijeljen na više organizacijskih razina, tako su i tipični sigurnosni procesi, koji se odvijaju u politikama informacijske sigurnosti, raspoređeni prema pripadnim grupama aktivnosti i razinama modela. Primjerice, procesi akreditacije kao opći pojam pripadaju podsustavu nadzora u vršnom sloju modela, ali se specijaliziraju za potrebe modeliranja politika informacijske sigurnosti. Primjer je slučaj tijela iz državnog sektora koji u podsustavu zaštite klasificiranih podataka (podsustav označen s PS11 u izvršnom dijelu metamodela sa slike 6.1) koristi specijalizaciju općeg pojma akreditacije, koja se prema potrebi modeliranja konfigurira parametrima zadanog okruženja, kako će se pokazati u studijama slučajeva (ontološki modeli u donjem dijelu slike 6.2). U upravljačkom dijelu zadržani su temeljni čimbenici u obliku definicije osoba i informacijskih sustava, a umjesto procesa dodan je podsustav fizičke sigurnosti koji je vrlo važan za politike informacijske sigurnosti i usko je povezan s osobama i tehnologijom. Vidljivo je također da se upravljačka razina metamodela pretežito bavi definiranjem sigurnosnih zahtjeva, dok su provedbene sigurnosne mjere i kontrole raspoređene u najnižem sloju metamodela na izvršnoj razini. Izvršna razina sastoji se također od tri podsustava i odražava dva temeljna pristupa u politikama i normama informacijske sigurnosti, pristup utemeljen na minimalnim sigurnosnim mjerama i pristup utemeljen na upravljanju rizikom (poglavlje 4.3.3.), a u trećem podsustavu modeliraju se koncepti zaštite osobnih podataka (poglavlje 4.9.2.). Podsustav zaštite klasificiranih podataka predstavlja ključni izvršni dio politika informacijske sigurnosti državnog sektora te se sastoji od pet dodatnih podsustava, koji opisuju područja informacijske sigurnosti u politikama informacijske sigurnosti državnog sektora (poglavlje 4.3.2.). Podsustav sigurnosnih kontrola temelji se na upravljanju rizikom i primjerice služi kao osnova za različite zahtjeve provedbe norme ISO 27001, dok podsustav zaštite osobnih podataka definira koncepte koji predstavljaju specifične zahtjeve u okviru suvremene provedbe zaštite osobnih podataka.

Na slici 6.2 istaknut je dio slike 5.1 s prikazom ostvarenja UML konceptualnog metamodela. Temelj konceptualnog metamodela je domenska taksonomija koja predstavlja domenu informacijske sigurnosti stvarnog svijeta. Analizom u četvrtom poglavlju obrađena je šira domenska razina, na način prikladan za potrebe modeliranja u ovom istraživanju,

prepoznavanjem i usporedbama ključnih obilježja politika informacijske sigurnosti kroz njihovo povijesno nastajanje, međupovezanost, primjenjivost u suvremenoj praksi i općenito kroz aktualno stanje šire domene informacijske sigurnosti. Takva analiza i domenska taksonomija u obliku rječnika temeljnih pojmova šire domenske razine [1, 2, 3, 4, 5, 21, 53, 102], prema slici 6.2, predstavlja temelj za ostvarenje konceptualnog metamodela. Opći rječnik, utvrđen preko analize prikazane u četvrtom poglavlju i razrađen metodama oblikovanja u petom poglavlju, prati strukturu metamodela ostvarenog prema transformaciji na slici 5.3, a ostvaren je u formi hijerarhijske domenske taksonomije i prikazan je na slici 2.2, u tablici 4.2 i u prilogu B u cijelosti.




**Slika 6.2:** Metoda modeliranja s istaknutim dijelom ostvarenja UML konceptualnog metamodela

U nastavku procesa modeliranja tako dobivenoj hijerarhijskoj domenskoj taksonomiji (rječnik i sintaksa), potrebno je dodati značenje u kontekstu domene modeliranja (semantika) [103]. Upravo u tu svrhu modeliranje se nastavlja korištenjem UML-a, daljnjom razradom detalja, prateći strukturu metamodela (podsustavi) i hijerarhijsku domensku taksonomiju. Daljnja razrada detalja daje značenje hijerarhijski razrađenom rječniku (prilog B) postavljenom u

strukturne okvire metamodela sa slike 6.1. Ovo značenje se definira uz pomoć međusobnih relacija koncepata te dodavanjem atributa. Pri tome je cilj zadržavanje dovoljne razine općenitosti UML metamodela, za potrebe šire domenske razine koja ima obilježja visoke složenosti i heterogenosti, zatim zadržavanje razine jasnoće i razumljivosti UML metamodela s ciljem dobre vizualizacije, a istovremeno s navedenim ciljevima, omogućiti i dovoljnu razinu formalne specifikacije koncepata (relacije i atributi) koja je potrebna u daljnjim koracima ostvarenja programskog ontološkog metamodela.

U svrhu rješavanja ovako definiranog problema modeliranja, prema slici 6.2 koristimo apstrakciju domene informacijske sigurnosti stvarnog svijeta i prikazujemo ju odabranim skupom dominantnih politika i normi informacijske sigurnosti, uvedenim i opisanim u poglavlju 5.5. Za ovaj skup dominantnih politika i normi informacijske sigurnosti, smatramo da ima sva potrebna obilježja općenitosti šire domenske razine informacijske sigurnosti stvarnog svijeta, za potrebe modeliranja u okviru ovog istraživanja.

## 6.1. Osnovni elementi UML-a koji se koriste u modeliranju

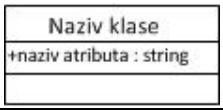
Kako je već rečeno u poglavlju 5.2, konceptualni metamodel razvija se u UML-u (engl. *Unified Modelling Language – UML*) [98], koji konceptualnom modelu osigurava tražena svojstva jasnoće i razumljivosti, kao i mogućnost formalne specifikacije metamodela (rječnik, sintaksa i semantika koncepata), u svrhu programskog ostvarenja ontološkog metamodela. Standardni način zapisa modela u UML-u svojim unificiranim grafičkim simbolima olakšava razumijevanje modela, što predstavlja jedan od ciljeva modeliranja u ovom istraživanju. Razlog za postavljanje ovog cilja je to, što konceptualni metamodel u okviru ovog istraživanja predstavlja okvir za upravljanje i komuniciranje znanjem o domeni, primarno između osoba zaduženih u različitim organizacijama za poslove informacijske sigurnosti (rukovoditelji sigurnosti, savjetnici za informacijsku sigurnost i sl.), ali isto tako i između niza osoba s različitim stručnim i interesnim profilima, povezanim na određeni način uz ovo, multidisciplinarno područje informacijske sigurnosti (stručnjaci za različita područja sigurnosti kao što je sigurnost osoblja, fizička sigurnost, sigurnost informacijskih sustava, upravljanje rizikom, vlasnici podataka i informacijskih sustava, rukovoditelji i sl.). Pored toga, konceptualni metamodel je i središnja točka procesa modeliranja (specifikacija, ostvarenje, održavanje, dorade i proširenja modela), ali istovremeno i okvir za ostvarenje programskog ontološkog metamodela sa slike 6.2, koji uz pomoć vizualnog načina prikaza,

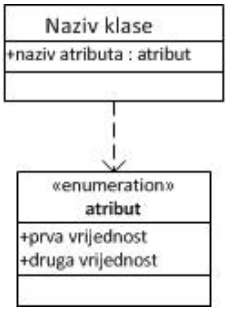
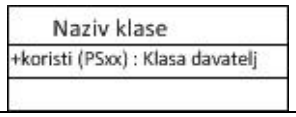
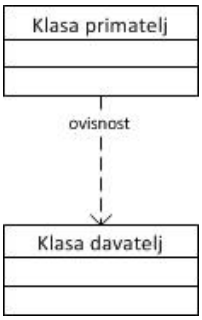
jasnoće i razumljivosti ljudima, olakšava proces ostvarenja, modeliranja i konfiguriranja ontoloških modela provedbe politika informacijske sigurnosti u nekoj organizaciji (sedmo poglavlje).

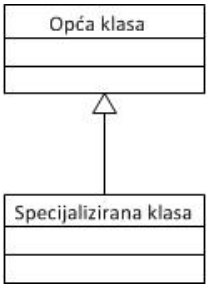
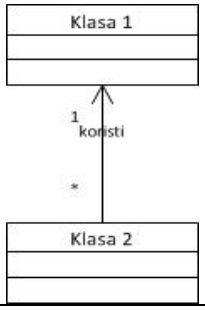
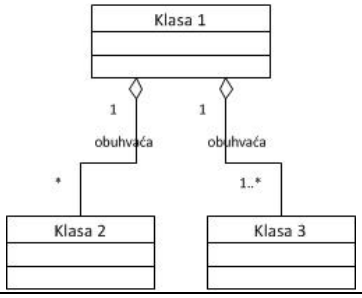
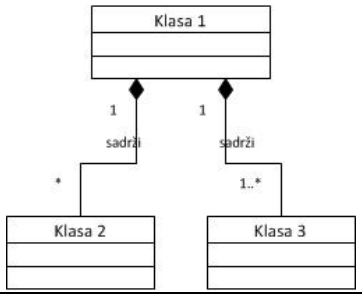
U procesu ostvarenja konceptualnog metamodela u UML-u, koristi se prethodno ostvarena i opisana struktura metamodela sa slike 6.1, kao i prethodno razrađen rječnik pojmova (tablica 4.2. i prilog A), odnosno hijerarhijska domenska taksonomija koncepata pridijeljenih tim pojmovima u kontekstu modeliranja (tablica 5.5 i prilog B), koja je razrađena prema strukturi razina i podsustava metamodela prikazanih na slici 6.1. U ovom poglavlju prikazujemo rezultate sljedeće faze modeliranja, kojom se nastavljaju razrađivati potrebni atributi i međusobne relacije prethodno opisanih koncepata pridruženih domenskom rječniku pojmova. Ovi koncepti prema dosadašnjoj razradi imaju osnovne hijerarhijske relacije i kategorizirani su prema razvijenoj strukturi konceptualnog metamodela sa slike 6.1 (tablica 5.5 i prilog B).

Daljnja razrada koncepata i relacija konceptualnog metamodela i njihova specifikacija, provode se na sličan način kao u [104], ali uz korištenje standardnih elemenata UML-a. Time se osigurava tehnološki neutralan pristup, dobra vizualna svojstva, jasnoća i razumljivost, kao i potrebna specifikacija koncepata (rječnik, sintaksa, semantika) za programsko ostvarenje ontološkog metamodela, koje slijedi na idućoj razini modeliranja prema slici 6.2. Pri modeliranju, koristi se ograničeni skup UML elemenata prikazanih u tablici 6.1, a konceptualni metamodel prikazuje se uz pomoć UML dijagrama klasa (statička struktura sustava).

**Tablica 6.1:** Elementi UML-a koji se koriste u konceptualnom metamodelu

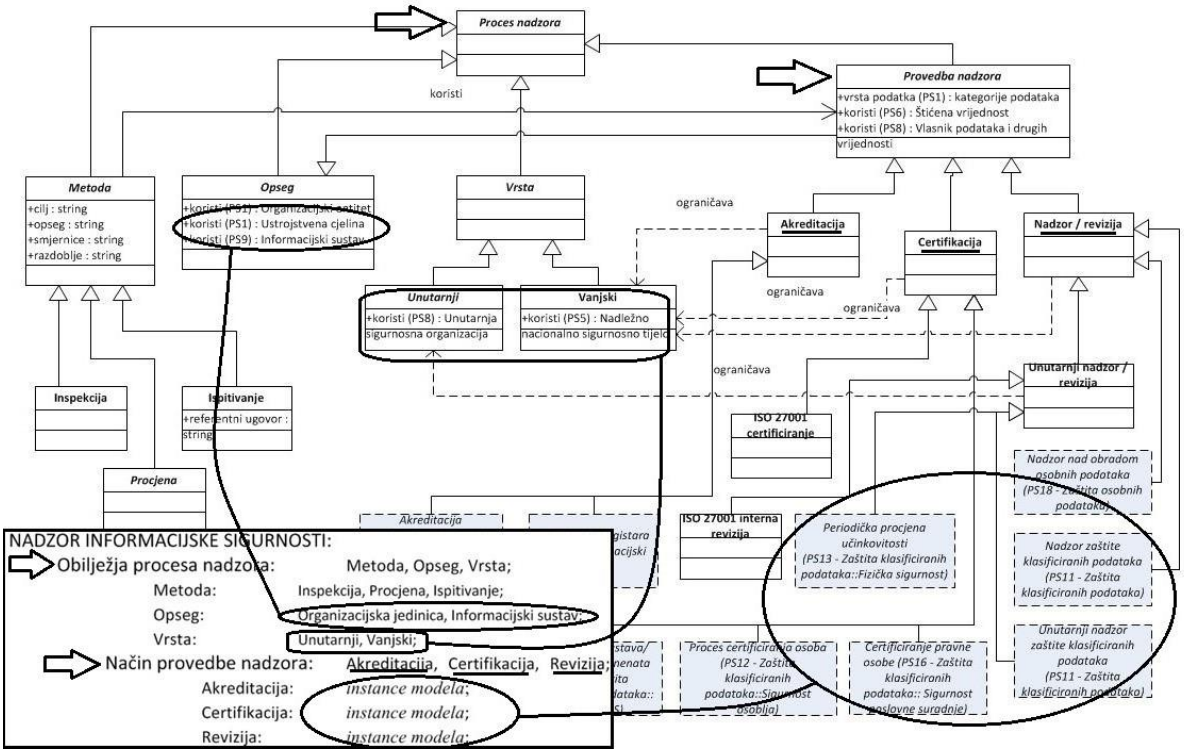
| **R.br.** | **Vrsta UML elementa i grafički simbol** | ***Značenje elementa u modelu*** | ***Opis*** |
|---|---|---|---|
| 1. | Paket (engl. *Package*)<br>  | *Podsustav konceptualnog metamodela* | *Jednostavan skup domenskih koncepata srodne vrste (klase); koristi se dodatna oznaka s brojem podsustava u gornjem lijevom kutu simbola.* |
| 2. | Klasa (engl. *Class*)<br>  | *Koncept metamodela* | *Klasama se predstavljaju koncepti koji su pridruženi rječniku domenske taksonomije; naziv klase je u gornjem dijelu simbola, atributi su u srednjem dijelu simbola.* |

| R.br. | Vrsta UML elementa i grafički simbol | *Značenje elementa u modelu* | *Opis* |
|---|---|---|---|
| 2.1 | Atribut klase<br>(engl. *Attribute*) | *Obilježje koncepta* | *Koriste se opisni atributi koji mogu biti tipa string (polje za unos alfanumeričkih znakova), int (polje za unos cjelobrojnih veličina) i enumeration (nabrojani tip predefiniranih alfanumeričkih konstanti).* |
| 2.2 | Tip atributa *enumeration*<br>  | *Obilježje koncepta* | *Atribut tipa enumeration povezuje klasu s podatkovnim tipom definiranim posebnim simbolom u kojem su nabrojane uvedene alfanumeričke konstante. Veza se predstavlja simbolom ovisnosti (isprekidana linija sa strelicom) prema 4. točki ove tablice. Grafički se prikazuje u zapisu UML metamodela za veze unutar jednog podsustava (atribut definiran u istom podsustavu u kojem je i klasa koja ga koristi), dok se za slučaj korištenja atributa definiranog u drugom podsustavu koristi samo atribut unutar simbola klase, s vezom na ovaj tip atributa označen malim početnim slovom.* |
| 2.3 | Tip atributa<br>*Class/Instance*<br>  | *Veza između klasa u različitim podsustavima* | *Atribut tipa class/instance povezuje klasu s instancom neke druge klase (odabir prije definirane klase modela). Naziv atributa sadrži riječ „koristi …“ te u zagradi alfanumeričku oznaku podsustava (npr. PS14) u kojem je definirana klasa (veliko početno slovo).* |
| 3. | Vanjska klasa<br>(engl. *External Class*)<br>  | *Koncepti koji se koriste u jednom podsustavu, a definirani su u drugom* | *Grupiranje klasa u podsustave (PSxx, gdje je xx broj podsustava od 1 do 18) provodi se sukladno prethodno određenoj strukturi konceptualnog metamodela; simbol vanjske klase koristi se primjerice kod nasljeđivanja nadklase, ili jedne od nadklasa pri višestrukom nasljeđivanju, koja je iz drugog podsustava.* |
| 4. | Ovisnost<br>(engl. *Dependency*)<br>  | *Ovisnost kao relacija između koncepata pri čemu je klasa davatelj uvijek klasa uz strelicu* | *Ovisnosti su tipizirane i označavaju se oznakom na isprekidanoj liniji sa strelicom.* |
| 4.1 | Koristi se oznaka na isprekidanoj strelici: „ograničava“ | | *Klasa davatelj ograničava Klasu primatelj (npr. klasa Akreditacija registara u PS5 ograničava klasu organizacije Sustav registara koja se akreditira, tj. koncept primatelja sadrži koncept davatelja kao obavezni atribut).* |
| 4.2 | Koristi se oznaka na isprekidanoj strelici: „ostvaruje“ | | *Klasa primatelj ostvaruje se na temelju Klase davatelja (npr. klasa Akreditacija registara u PS5 ostvaruje se uz pomoć klase nadležnog tijela NSA hijerarhija/tijelo).* |

| R.br. | Vrsta UML elementa i grafički simbol | *Značenje elementa u modelu* | *Opis* |
|---|---|---|---|
| 5. | Specijalizacija<br>(engl. *Specialization*)<br>  | *Predstavlja specijalizaciju koncepata (nasljeđivanje) koja može biti višestruka* | *Specijalizirana klasa ima opće atribute koje nasljeđuje od opće klase, a može imati i posebne atribute koji su dodani ovoj klasi (npr. klasa Međunarodni ugovor u PS2 je specijalizirana klasa iz opće klase Zakonski zahtjev).* |
| 6. | Povezivanje<br>(engl. *Association*) | *Relacije između klasa* | *Koristi se više vrsta povezivanja: jednostavno povezivanje, združivanje i sastavljanje.* |
| 6.1 | Jednostavno povezivanje<br>(engl. *Association*)<br>  | *Jednostavno povezivanje: „koristi“* | *Jedna klasa koristi drugu klasu, a strelica određuje smjer (npr. Klasa 1 je organizacijski entitet koji koristi Klasu 2 koja predstavlja više rukovoditelja u organizaciji).*<br>*Veza može imati strelicu smjera, oznaku „koristi“ i oznaku brojnosti s obje strane veze. Grafički se prikazuje u zapisu UML metamodela za veze unutar istog podsustava, dok se za veze između klasa iz različitih podsustava koristi prikaz iz točke 2.3 (tip atributa class/instance).* |
| 6.2 | Združivanje<br>(engl. *Aggregation*)<br>  | *Združivanje (cjelina – dijelovi) „obuhvaća“* | *Cjelina (Klasa 1) obuhvaća više dijelova (Klase 2 i 3), pri čemu su dijelovi klase domene koje postoje i bez združivanja u cjelinu s Klasom 1 (npr. klasa Sigurnosna uloga IS-a u PS9 obuhvaća klase Sigurnosni kriteriji pristupa korisnika, Organizacijski elementi IS-a, Razvoj sigurnosne svijesti, edukacije i obuka i dr.).* |
| 6.3 | Sastavljanje<br>(engl. *Composition*)<br>  | *Sastavljanje (kontejner – sadržaj) „sadrži“* | *Jedna klasa (spremnik) sastoji se od više klasa koje su sa stanovišta domene važne u sastavljenom obliku, a ne pojedinačno (npr. klasa Odgovornosti pravne osobe u PS18 sadrži više klasa odgovornosti pravne osobe za osobne podatke, koje su važne samo u kontekstu zaštite osobnih podataka).* |
| 6.4 | Brojnost elemenata<br>(engl. *Association numbering)*<br>0; 1; 0..*; 1..*; * | *Brojnost elemenata u različitim povezivanjima* | *Oznaka se stavlja na kraju poveznice na koju se odnosi.* |

## 6.2. Struktura konceptualnog metamodela

Prema slici 6.1, konceptualni metamodel sastoji se od 18 podsustava (PS1 do PS18) koji se prikazuju uz pomoć UML dijagrama klasa. UML klase u dijagramima klasa predstavljaju pojmove ostvarene u hijerarhijskoj domenskoj taksonomiji i prikazane u tablici 5.5 i prilogu B. Na slici 6.3 prikazan je UML dijagram klasa za podsustav nadzora informacijske sigurnosti (PS4), zajedno s razrađenom hijerarhijskom domenskom taksonomijom ovog podsustava, prethodno prikazanom na slici 2.2.




**Slika 6.3:** Ostvarenje konceptualnog UML metamodela na temelju hijerarhijske domenske taksonomije

Na slici 6.3 može se vidjeti način ostvarenja UML dijagrama klasa zasnovan na pojmovima koji su prethodno ostvareni i prikazani u hijerarhijskoj domenskoj taksonomiji. Nakon ostvarenja ovih osnovnih klasa i njihovih hijerarhijskih relacija u UML konceptualnom metamodelu (sintaksa), potrebno je dodatno razraditi značenje pojmova i pridruženih koncepata (semantika), što se provodi ostvarenjem relacija između klasa u različitim podsustavima metamodela, kao i između klasa unutar pojedinih podsustava. Ove relacije obuhvaćaju, pored osnovnog hijerarhijskog odnosa među klasama i višestruke specijalizacije

(nasljeđivanja), povezivanje klasa i instanci klasa unutar i između podsustava, kao i uvođenje ograničenja relacijama između klasa. Proces definiranja značenja koncepata pridruženih klasama UML-a, nakon ostvarenja osnovne hijerarhije klasa te razrade ove hijerarhije opisanim relacijama između klasa i podsustava, nastavlja se definiranjem i uvođenjem atributa u klase, što je također vidljivo na simbolima klasa na slici 6.3. Atributi omogućavaju uvođenje različitih tipova podataka, prikazanih u tablici 6.1, koji se koriste prilikom opisivanja stvarnih organizacijskih okruženja u kojima se provodi politika informacijske sigurnosti.

U nastavku šestog poglavlja prikazuje se i opisuje ostvareni konceptualni metamodel u UML-u, koji se sastoji od četiri organizacijske razine prema slici 6.1 (razine I. do IV.) u okviru kojih su ostvareni srodni podsustavi (18 podsustava, od PS1 do PS18). Složenost i specifičnost sigurnosnih zahtjeva pojedinih politika i normi informacijske sigurnosti modelirana je u okviru podsustava koji se nalaze na izvršnoj razini metamodela. Tako je složenost politike informacijske sigurnosti državnog sektora modelirana daljnjom razradom podsustava zaštite klasificiranih podataka (PS11), na pet dodatnih podsustava (PS12 do PS16). Prethodno ostvarena hijerarhijska domenska taksonomija, prikazana u tablici 5.5, odnosno u prilogu B, prikazuje hijerarhijski složen skup pojmova domene, kategoriziran u odabrane podsustave, s opisima koncepata pridruženih ovako složenim pojmovima. Pomoću ovako definiranih pojmova ostvaruju se klase UML metamodela grupirane u podsustave. Tako dobivenim klasama dalje se razrađuju svojstva kroz dodavanje atributa i relacija između klasa te se u daljem opisu ostvarenja konceptualnog UML metamodela, prikazuju ostvareni podsustavi konceptualnog metamodela prikazani UML dijagramima klasa s kratkim opisima.

## 6.3. Razina globalnog okruženja konceptualnog metamodela

Razina globalnog okruženja (označena s I. na slici 6.1) modelira segment globalnog okruženja, koji prema slici 5.2 obuhvaća različite zahtjeve šireg globalnog okruženja (nacionalno i međunarodno). Ovi zahtjevi predstavljaju razloge i zahtjeve za provedbu normi i politika informacijske sigurnosti, odnosno definiraju okvire provedbe prema slici 5.4. Ova razina konceptualnog metamodela modelira se podsustavima domene politike informacijske sigurnosti (PS1), regulativne usklađenosti (PS2), razdiobe podataka (PS3), nadzora informacijske sigurnosti (PS4) i organizacijskog okvira (PS5).

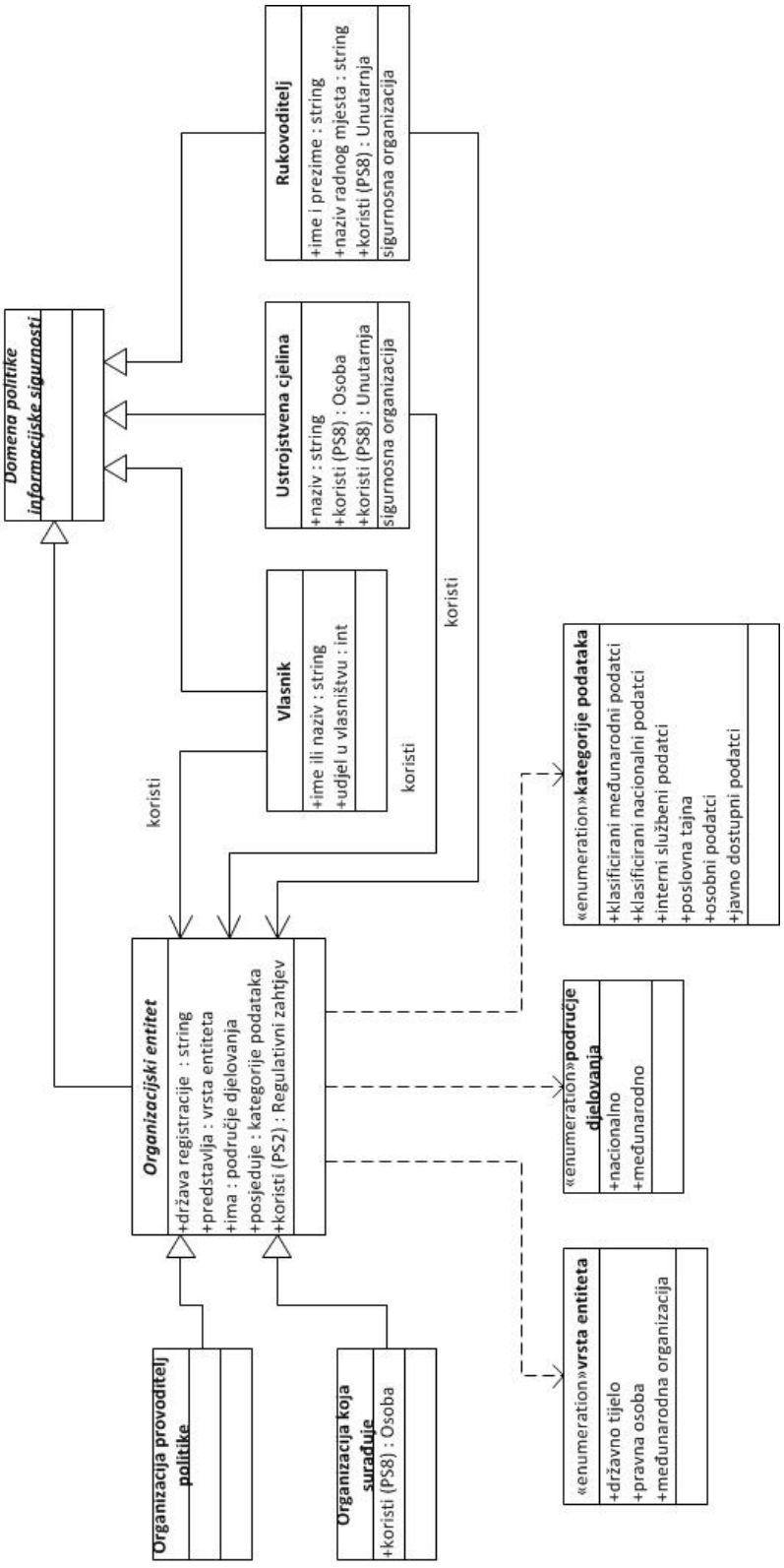
### 6.3.1. Podsustav domene politike informacijske sigurnosti

Podsustav domene politike informacijske, prikazan je na slici 6.4, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja vršni podsustav u I. organizacijskom sloju globalnog okruženja. Uloga ovog podsustava je raščlaniti uloge organizacijskih entiteta koji s gledišta politika i normi informacijske sigurnosti mogu biti organizacije provoditelji politike ili organizacije koje s provoditeljem politike surađuju u određenom, sigurnosno relevantnom području.

Svi organizacijski entiteti koji se koriste u okviru politike informacijske sigurnosti definiraju se u okviru hijerarhije klase *Organizacijski entitet*, kao instanca klase *Organizacija provoditelj politike*, ili kao instance klase *Organizacija koja surađuje*. Pri tome se koriste taksonomije *vrsta entiteta*, *područje djelovanja* i *kategorija podataka*, ostvarene kao tip atributa *enumeration* prema tablici 6.1 (za razliku od naziva klasa, nazivi atributa koriste malo početno slovo).

Također, ovdje su klasama UML-a posebno modelirani koncepti, koji predstavljaju bitna obilježja organizacijskih entiteta povezanih s provedbom normi i politika i koji se koriste u drugim razinama i podsustavima metamodela (klase: *Vlasnik*, *Rukovoditelj*, *Ustrojstvena cjelina*).

Klasa *Organizacijski entitet* definira i relacije prema važnijim obilježjima organizacije koja su definirana posebnim klasama, a ne kao atributi klase *Organizacijski entitet*. Stoga su klase *Vlasnik*, *Ustrojstvena cjelina* i *Rukovoditelj* povezane relacijom *koristi* unutar podsustava PS1. Relacije između klasa u konceptualnom metamodela prikazane su u završnom poglavlju 6.7, odnosno u tablici 6.2 i prilogu C. Razlika između način prikaza relacija unutar istog podsustava i između različitih podsustava opisana je u tablici 6.1.




**Slika 6.4:** Podsustav domene politike informacijske sigurnosti (PS1), UML dijagram klasa

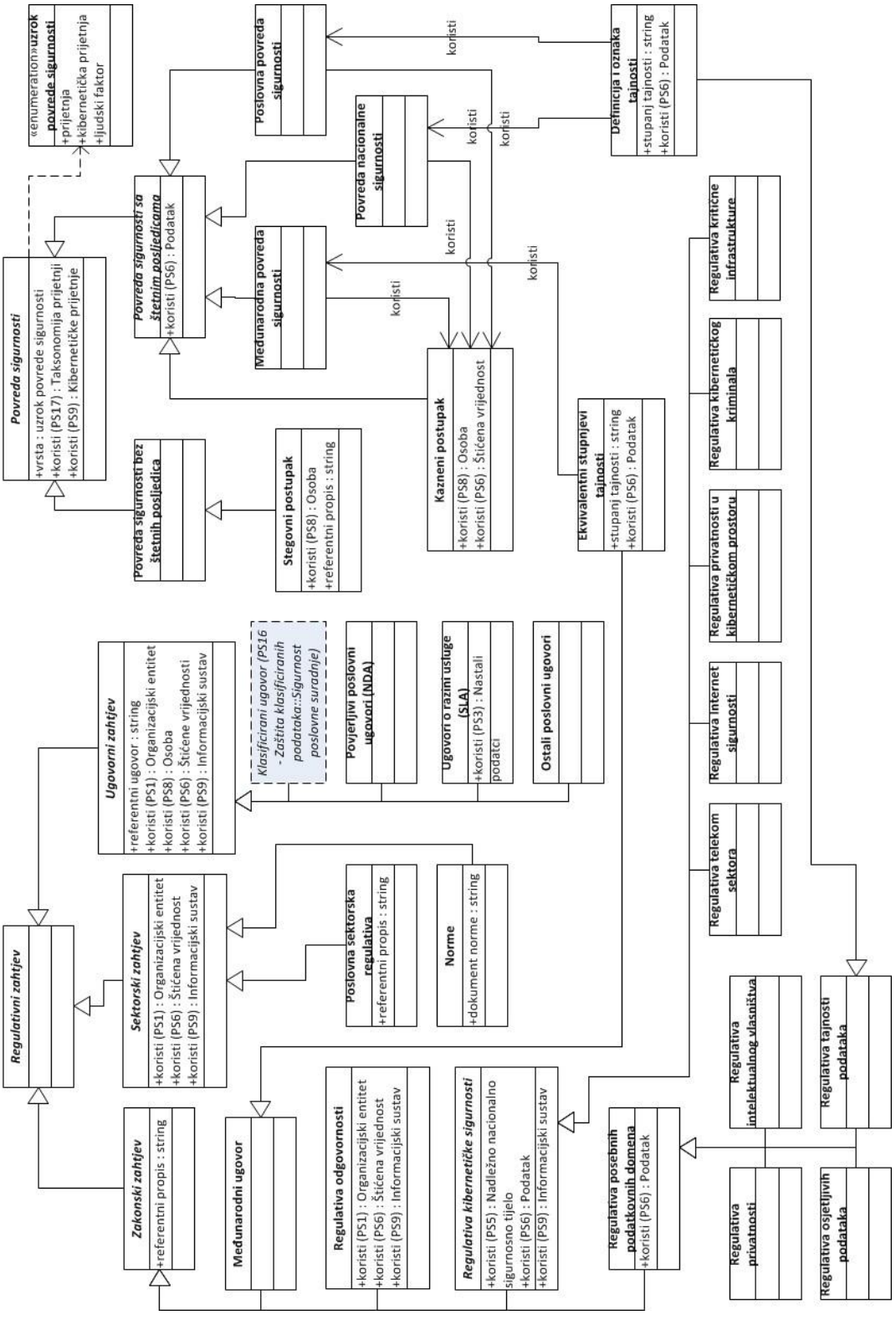
### 6.3.2. Podsustav regulativne usklađenosti

Podsustav regulativne usklađenosti, prikazan je na slici 6.5, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od podsustava u I. organizacijskom sloju. Uloga ovog podsustava je modeliranje različitih vrsta regulativnih zahtjeva, kao i povezanog koncepta povreda sigurnosti (engl. *Breach of Security*), za što se koriste dvije vršne klase. Klasa *Regulativni zahtjev* razvijena je u detaljnu hijerarhiju, zbog svoje iznimne važnosti za suvremene politike informacijske sigurnosti. U poglavljima 4.4. i 4.5. naznačena je visoka složenost regulativne hijerarhije informacijske sigurnosti, koja se sastoji od čitavog niza različitih propisa iz pravne i tehničko-normativne regulative te zahtijeva multidisciplinaran pristup. Upravo stoga modeliranjem su obuhvaćene prije predložene regulativne taksonomije u radovima [3, 5], a razrada je provedena u skladu s osnovnim smjernicama, koje u ovom području daju dominantne politike i norme informacijske sigurnosti. Područje regulativne usklađenosti predstavlja temeljno vršno područje modeliranja, jer postavlja okvire suvremenih sigurnosnih zahtjeva čija nedovoljna razrađenost predstavlja jednu od slabosti koja dovodi do nepovezanosti domenskog znanja.

Za razradu klase *Regulativni zahtjev*, odabrane su ključne kategorije modeliranja preko klasa *Zakonski zahtjev*, *Sektorski zahtjev* i *Ugovorni zahtjev*. Klasa *Zakonski zahtjev* razrađuje se na dvije razine hijerarhije te se dalje povezuje s klasama koje su poveznice s hijerarhijom razrade klase *Povreda sigurnosti* (npr. klasa *Definicija i oznaka tajnosti*). Obje vršne klase, s pripadnom hijerarhijom klasa, povezane su s nizom drugih klasa u ostalim podsustavima (PS3, PS5, PS6, PS9, PS17), preko atributa ili simbolom vanjske klase prema tablici 6.1. Također, obje hijerarhije koriste i nacionalnu i međunarodnu problematiku, sukladno odabranom načinu pristupa globalnom okruženju u ovom istraživanju. Klasa *Klasificirani ugovor*, pripada dvjema različitim hijerarhijama klasa, jer je izvorno definirana u specijaliziranom podsustavu sigurnosti poslovne suradnje (PS16), na izvršnoj razini, a istovremeno pripada klasi *Ugovorni zahtjev* u općenitijoj hijerarhiji ovog podsustava. Relacije u klasama prenose se procesom specijalizacije, odnosno nasljeđivanja (tablica 6.1), na niže klase u hijerarhiji.

Hijerarhija klase *Povreda sigurnosti*, grana se na dvije različite hijerarhije, s obzirom na postojanje (engl. *Compromise*) ili nepostojanje štetnih posljedica (engl. *Infraction*). Klasa *Povreda sigurnosti sa štetnim posljedicama* razrađuje i međunarodno-nacionalni i sektorski

pristup (državni i poslovni sektor), s obzirom na razlike i specifičnosti u postupanju koje postoje. Taksonomija povreda sigurnosti *uzrok povreda sigurnosti*, definirana je preko tipa atributa *enumeration*, te definira ljudski faktor, opće prijetnje (razrađuju se dalje u PS17) i kibernetičke prijetnje (razrađuju se u PS9).




**Slika 6.5:** Podsustav regulativne usklađenosti (PS2), UML dijagram klasa

### 6.3.3. Podsustav razdiobe podataka

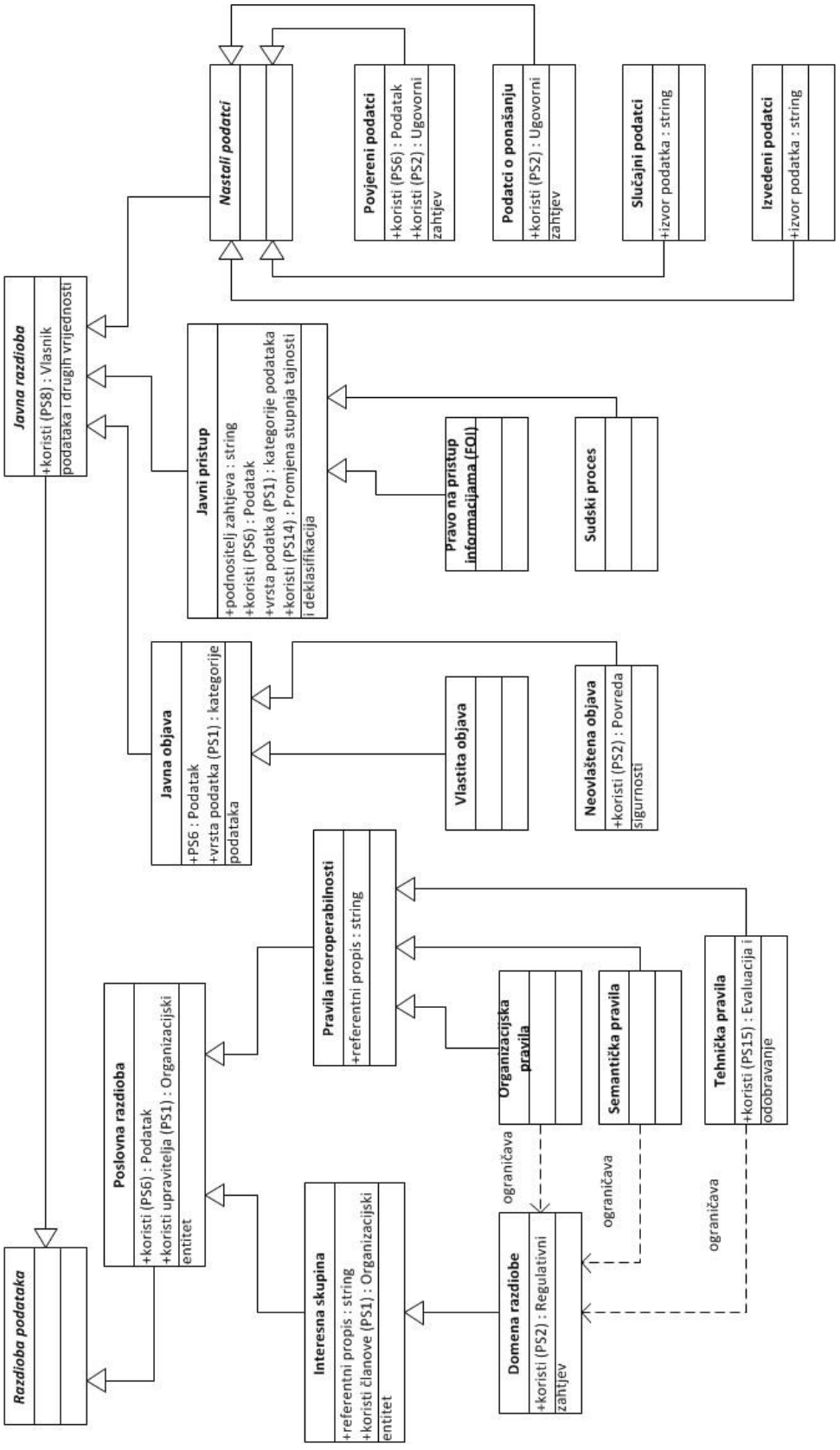
Podsustav razdiobe podataka, prikazan je na slici 6.6, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od podsustava u I. organizacijskom sloju. Uloga ovog podsustava je modeliranje suvremenih zahtjeva razdiobe podataka, koji su, prema provedenoj analizi domenskog područja, modelirani preko dvije osnovne klase: klase *Poslovna razdioba* i klase *Javna razdioba*.

Klasa *Poslovna razdioba* predstavlja modeliranje suvremenih zahtjeva za razdiobom podataka po različitim potrebama i pravilima poslovne suradnje (engl. *Information Sharing*). Klasa sadrži pravila, oblikovana posebnom hijerarhijom klasa, kojima se postavljaju zahtjevi na sadržaj i logičku povezanost elemenata politike informacijske sigurnosti kojom se planira razdioba podataka. Zahtjevi koji su postavljeni sastoje se od klase *Interesna skupina* (engl. *Community of Interest – COI*) s atributima organizacija članova i organizacije upravitelja skupine te podklasom *Domena razdiobe*, koja ograničava klase *Organizacijska pravila*, *Semantička pravila* i *Tehnička pravila*, kao podklase u hijerarhiji klase *Pravila interoperabilnosti*. U atributima je naznačena i potreba postojanja referentnog propisa za svaku klasu kojom su ovi ključni elementi procesa razdiobe propisani.

Klasa *Javna razdioba* podataka sastoji se od tri hijerarhije podklasa modeliranih klasama *Javna objava*, *Javni pristup* i *Nastali podatci*. Klasa *Javna objava* modelira proces vlastite objave podataka samog vlasnika podataka, što također treba strukturirati za potrebe politike informacijske sigurnosti. Podklasa *Neovlaštena objava* ostvaruje vezu s klasom *Povreda sigurnosti* iz podsustava regulativne usklađenosti sa slike 6.5. Ove dvije hijerarhije klasa usko su povezane s vlasnikom podataka naznačenim u atributu vršne klase hijerarhije, klase *Javna razdioba*. Klasa *Javni pristup* predstavlja slučajeve vanjskih zahtjeva za pristup podatku i ograničena je mogućom tajnošću podatka (klasificirani podatak), odnosno potrebom njegove prethodne deklasifikacije preko podsustava PS14. Vanjski zahtjevi ovog tipa mogu se svrstati u klasu *Pravo na pristup informacijama (Freedom of Information - FoI)* i klasu *Sudski proces*.

Klasa *Nastali podatci* modelira vrste podataka koje nastaju u okviru kibernetičkog prostora [97] (poglavlje 4.9.3.), a odabrana taksonomija podklasa usko je povezana s vlasnikom

podataka te se promatra s gledišta potreba politika i normi informacijske sigurnosti, kroz prevenciju i ograničenja uvedena ugovornim zahtjevima.



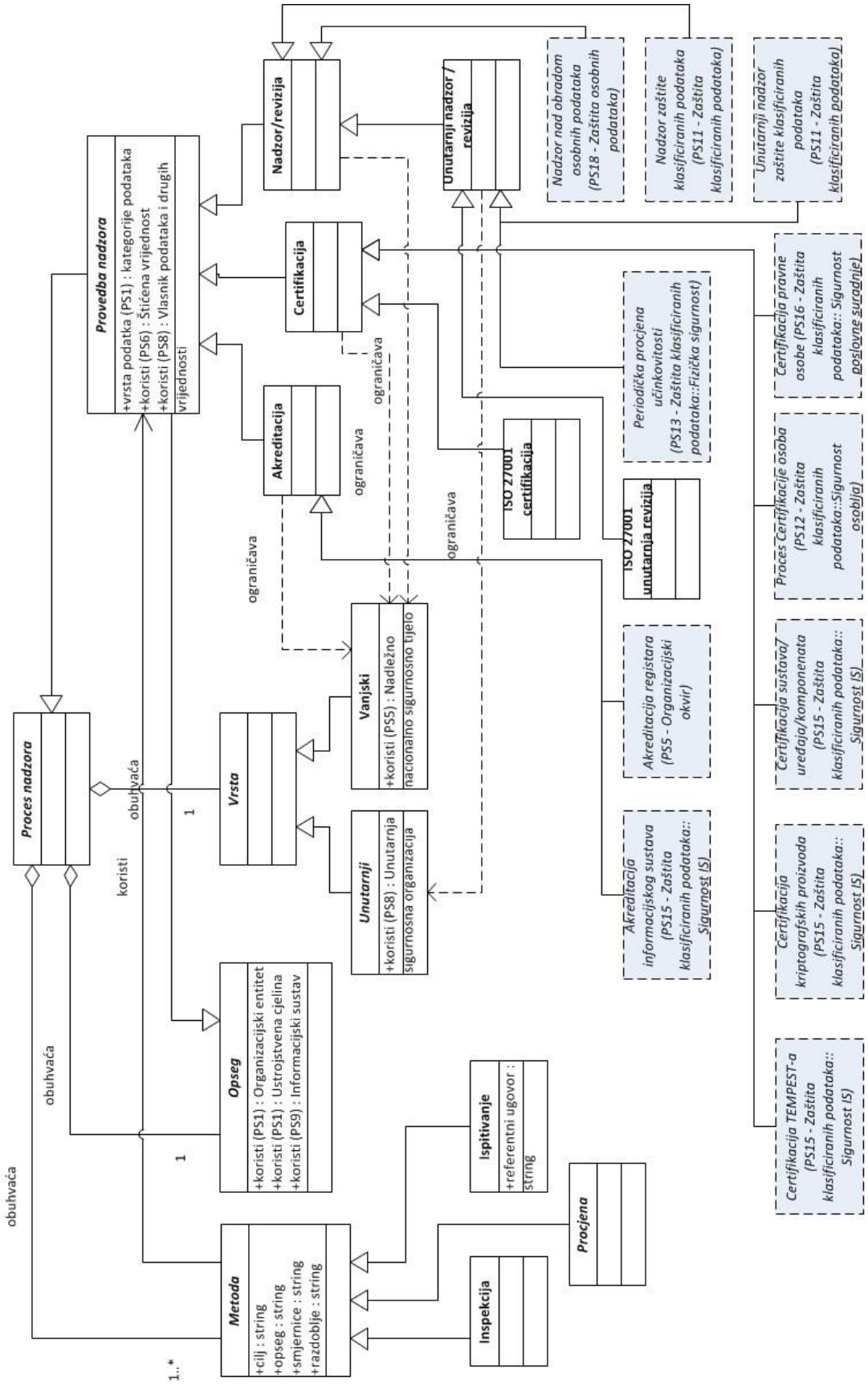

**Slika 6.6:** Podsustav razdiobe podataka (PS3), UML dijagram klasa

### 6.3.4. Podsustav nadzora informacijske sigurnosti

Podsustav nadzora informacijske sigurnosti prikazan je na slici 6.7, a prema prikazu konceptualnog metamodela na slici 6.1 predstavlja jedan od podsustava u I. organizacijskom sloju. Uloga ovog podsustava je modeliranje suvremenih zahtjeva nadzora informacijske sigurnosti koji su prema provedenoj analizi domenskog područja u četvrtom poglavlju i prema slici 2.2, modelirani preko vršne klase *Proces nadzora*. Ova klasa sadržava temeljna obilježja različitih vrsta nadzora koji se koriste u politikama i normama informacijske sigurnosti, koja se ostvaruju klasama *Metoda*, *Opseg* i *Vrsta*. Klase *Metoda* i *Vrsta* dalje se hijerarhijski modeliraju, a klasa *Opseg* obuhvaća potrebne atribute organizacija/ustrojstvena cjelina i informacijski sustav.

Klasa *Provedba nadzora* specijalizira se iz vršne klase *Proces nadzora* s ciljem ostvarenja podklasa procesa nadzora koji se stvarno koriste u organizacijskim okruženjima. Stoga se ova klasa dalje raščlanjuje na tri glavne vrste nadzornih procesa iz kojih se izvode sve potrebne instance nadzornih procesa u ciljanim okruženjima. Pri tome se koriste prethodno pojašnjena opća svojstva procesa nadzora. Glavne vrste provedbe nadzora predstavljaju podklase *Akreditacija*, *Certifikacija* i *Nadzor/revizija*. Definirana su i tipična ograničenja sukladno široko prihvaćenim definicijama unutarnjeg i vanjskog nadzora te definicijama akreditacijskih i certifikacijskih procesa (prilog A i B).

Pored modeliranja nadzornih procesa za potrebe ciljanog okruženja, naznačeno je i 11 vanjskih klasa koje su u drugim podsustavima ovog metamodela formirane daljnjom specijalizacijom ove tri podklase provedbe nadzora: *Akreditacija*, *Certifikacija* i *Nadzor/revizija*, koristeći njihova opća obilježja za posebne potrebe metamodela u različitim podsustavima kao što su: PS5, PS11, PS12, PS13, PS15, PS16 i PS18. Ovdje su također kreirane i dvije podklase: *ISO 27001 certificiranje* i *ISO 27001 unutarnja revizija*, za potrebe modeliranja instanci certifikacijskih i revizijskih procesa sukladno zahtjevima norme ISO 27001 [27], pri čemu se, kao i za ostale vrste provedbe nadzora, koristi specijalizacija općih klasa metamodela: *Certifikacija* i *Nadzor/revizija*, kao i povezanost sa svim ostalim dijelovima metamodela.



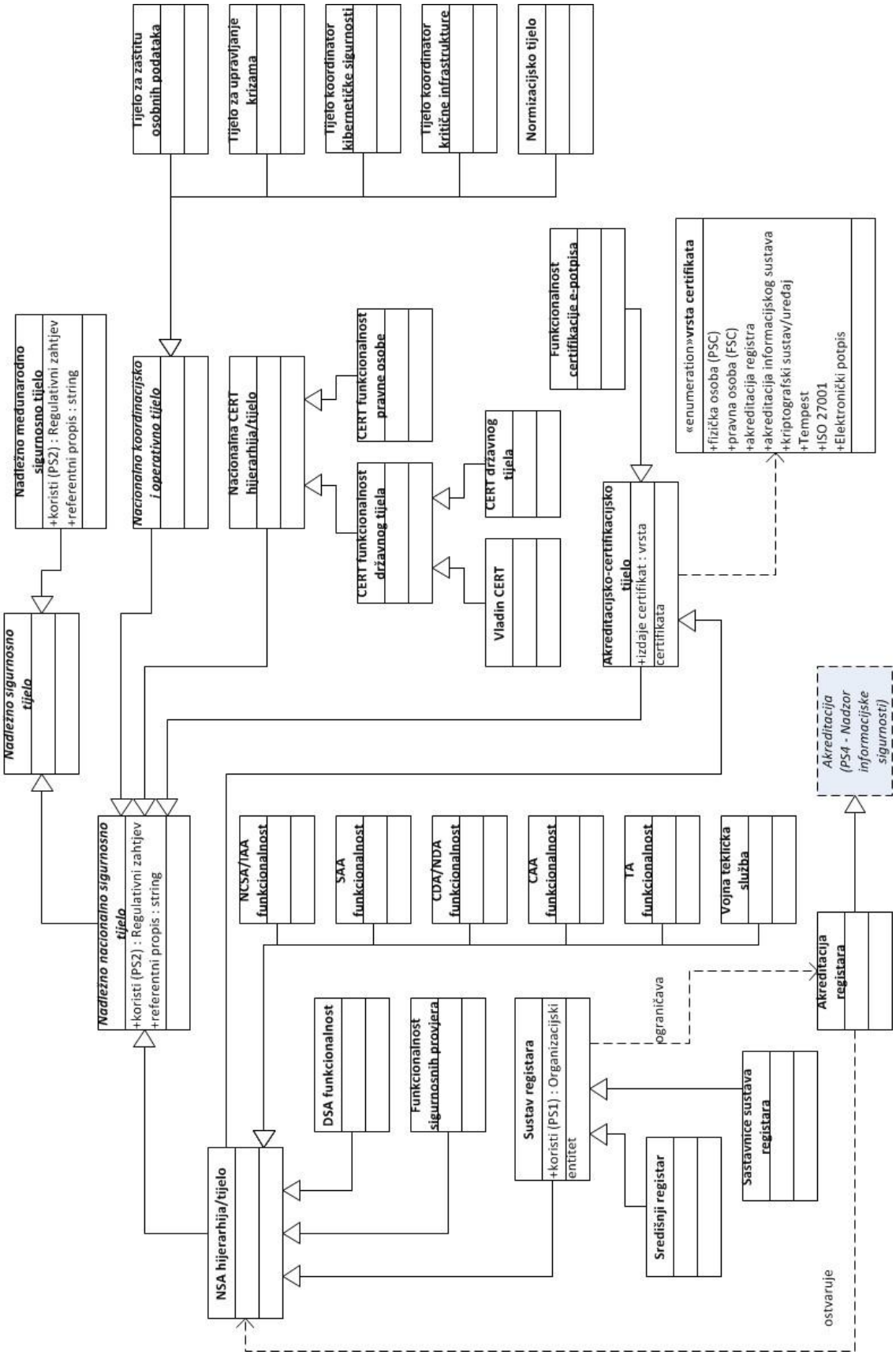

**Slika 6.7:** Podsustav nadzora informacijske sigurnosti (PS4), UML dijagram klasa

### 6.3.5. Podsustav organizacijskog okvira

Podsustav organizacijskog okvira, prikazan je na slici 6.8, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od podsustava u I. organizacijskom sloju. Uloga ovog podsustava je modeliranje nadležnih sigurnosnih tijela primjenjivih za potrebe šireg domenskog modeliranja (vršna klasa *Nadležno sigurnosno tijelo*). Prema analizi područja vidljivo je da se sve potrebe organizacijskog okvira rješavaju kroz nacionalni organizacijski okvir (podklasa *Nadležno nacionalno sigurnosno tijelo*) uz moguću koordinaciju nadležnog međunarodnog sigurnosnog tijela (podklasa *Nadležno međunarodno sigurnosno tijelo*). Klasa *Nadležno nacionalno sigurnosno tijelo* stoga obuhvaća nekoliko različitih hijerarhija i grupa tijela.

Najsloženija hijerarhija zasnovana je na klasi *NSA hijerarhija/tijelo*, koja obuhvaća niz klasa koje predstavljaju funkcionalnosti politike informacijske sigurnosti u državnom sektoru (npr. *DSA funkcionalnost*, *SAA funkcionalnost* i sl.), odnosno NATO/EU okruženju prema [73, 75], koje se moraju definirati i provoditi u odabranim nacionalnim državnim tijelima. S obzirom da su funkcionalnosti međusobno povezane i koordinirane iz središnjeg tijela (nacionalno NSA tijelo), ostvarene su kao specijalizacija klase *NSA hijerarhija/tijelo*. Unutar ove klase još je jedna manja hijerarhija klasa za potrebe modeliranja nacionalnog sustava registara za distribuciju međunarodnih klasificiranih podataka, koja je također ostvarena uz pomoć vršne klase *Sustav registara*. Ovdje je modelirana i klasa *Akreditacija registara*, kao specijalizirana podklasa opće klase *Akreditacija* iz podsustava nadzora informacijske sigurnosti (PS4), dodatno povezana relacijama *ograničava* i *ostvaruje* s organizacijskim entitetima za koje je obvezujuća i organizacijskim entitetima koji akreditaciju provede. Po istom načelu za CERT tijela je modelirana hijerarhija, ostvarena preko klase *Nacionalna CERT hijerarhija/tijelo*.

Za ostale potrebe, izravno ili neizravno povezane s politikama informacijske sigurnosti, modelirana je klasa *Nacionalno koordinacijsko i operativno tijelo*, koja se dalje raščlanjuje na važnije vrste tijela koja proizlaze iz analize šireg domenskog područja, kao što je primjena klase *Tijelo za zaštitu osobnih podataka* u podsustavu zaštita osobnih podataka (PS18). Klasa *Akreditacijsko-certifikacijsko tijelo* koristi podatkovni tip atributa *vrsta certifikata* s nabrojanim vrstama certifikata koje se koriste u modelu kao alfanumeričkim konstantama (*«enumeration»*).




**Slika 6.8:** Podsustav organizacijskog okvira (PS5), UML dijagram klasa

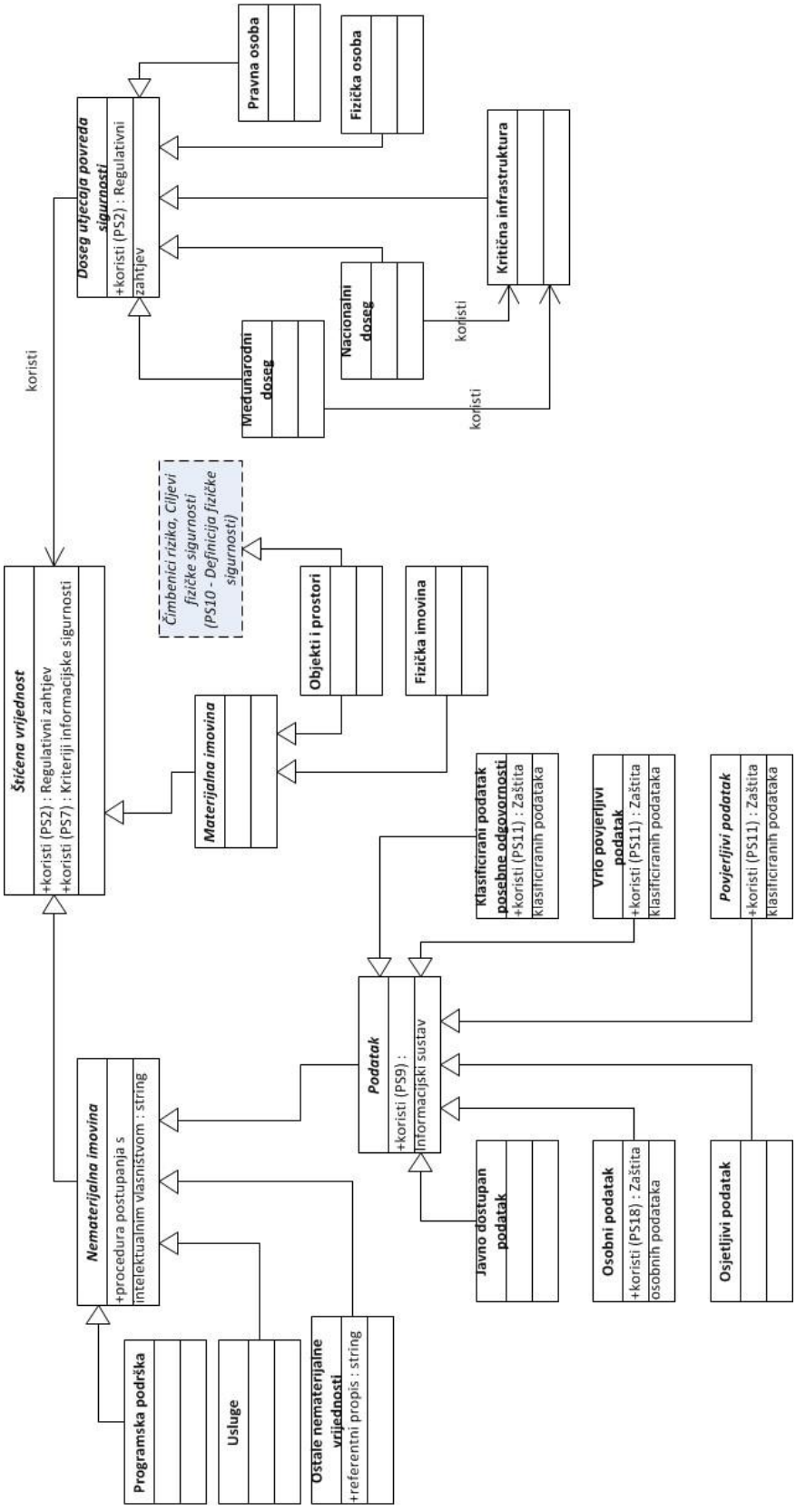
## 6.4. Razina sučeljavanja globalnog i lokalnog okruženja konceptualnog metamodela

Razina sučeljavanja globalnog i lokalnog okruženja (označena s II.), prema slici 6.1, modelira segment unutar kojeg se sučeljavaju regulativni i poslovni sigurnosni zahtjevi, odnosno zahtjevi globalnog i lokalnog okruženja koji razrađuju kriterije i definicije za provedbu sigurnosnih zahtjeva, te se definiraju okviri provedbe politike informacijske sigurnosti prema slici 5.4. Ova razina modelira se podsustavom definicije podataka i drugih vrijednosti (PS6) i podsustavom kriteriji informacijske sigurnosti (PS7).

### 6.4.1. Podsustav definicije podataka i drugih vrijednosti

Podsustav definicije podataka i drugih vrijednosti prikazan je na slici 6.9, kao podsustav na II. organizacijskom sloju sučeljavanja globalnog i lokalnog okruženja. Uloga ovog podsustava je središnji pregled štićenih vrijednosti metamodela politika informacijske sigurnosti (vršna klasa *Štićena vrijednost*), koje su ograničene dosegom utjecaja povreda sigurnosti (vršna klasa *Doseg utjecaja povreda sigurnosti*). Klasa *Štićena vrijednost* koristi klase *Regulativni zahtjevi* iz PS2 i *Kriteriji informacijske sigurnosti* iz PS7. Klasa *Štićena vrijednost* dijeli se na podhijerarhije preko klasa *Nematerijalna imovina* i *Materijalna imovina*. Klasa *Nematerijalna imovina* raščlanjuje se u klase *Programska podrška*, *Usluge* i *Ostale nematerijalne vrijednosti* te u podhijerarhiju s vršnom klasom *Podatak*. Klasa *Podatak* raščlanjuje se u taksonomiju šest različitih klasa koje omogućavaju osnovno kategoriziranje podataka prema najvažnijem kriteriju povjerljivosti (klase: *Klasificirani podatak posebne odgovornosti*, *Vrlo povjerljivi podatak, Povjerljivi podatak*), odnosno kriteriju privatnosti (klase: *Osobni podatak, Osjetljivi podatak*), kao i kriterijima cjelovitosti i raspoloživosti (klasa: *Javno dostupan podatak*) [103]. Ovakvo kategoriziranje omogućava primjenu tipičnih pristupa državnog i poslovnog sektora (klasificirani podatci, poslovna tajna), kao i suvremeni pristup privatnosti fizičkih osoba (osobni podatak), ali i pravnih osoba (osjetljivi podatak). Klasa *Materijalna imovina* koristi se u podsustavu definicije fizičke sigurnosti (PS10), a klasa *Fizička imovina*, potrebna je primjerice za definiranje prijenosnih računalnih i komunikacijskih uređaja, na koje se primjenjuju posebne sigurnosne kontrole u nižim podsustavima. Klasa *Doseg utjecaja povreda sigurnosti* omogućava definiranje utjecaja za prethodno uvedenu taksonomiju podataka i prema potrebi za povezivanje tih utjecaja s posebnom vrstom utjecaja definiranog

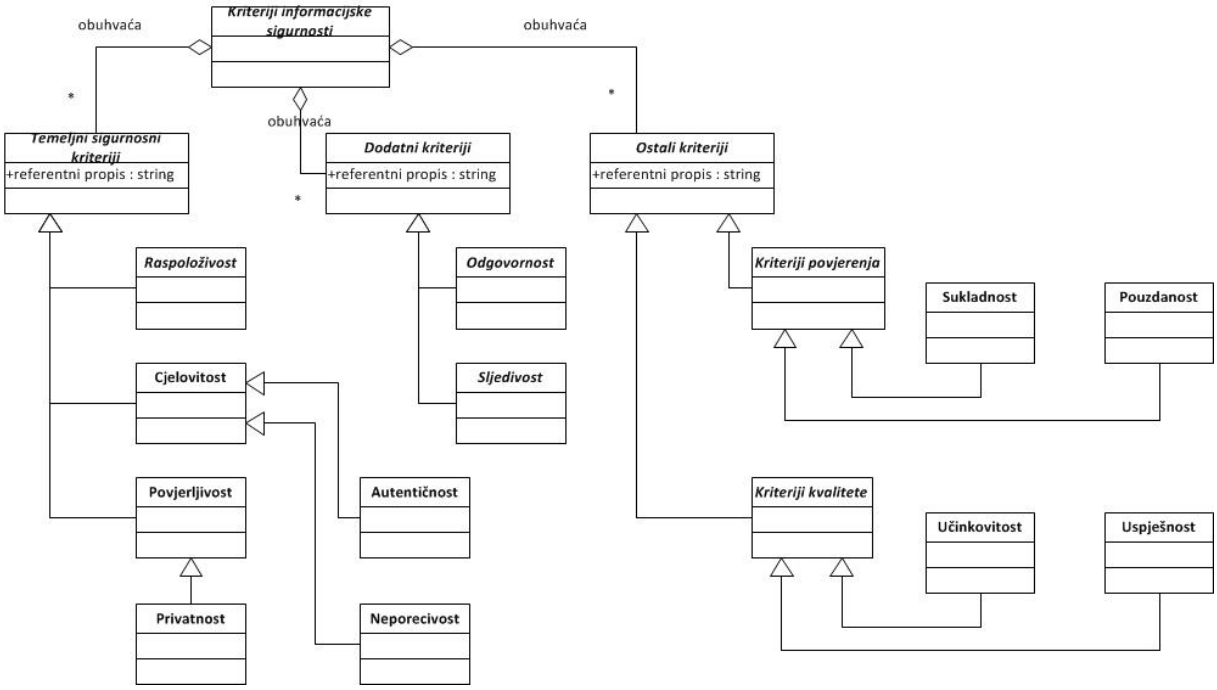
klasom *Kritična infrastruktura* (nacionalne i međunarodne primjene, te potrebe državnog i poslovnog sektora).




**Slika 6.9:** Podsustav definicije podataka i drugih vrijednosti (PS6), UML dijagram klasa

### 6.4.2. Podsustav kriterija informacijske sigurnosti

Podsustav kriterija informacijske sigurnosti prikazan je na slici 6.10, a prema prikazu konceptualnog metamodela na slici 6.1, ovaj podsustav predstavlja jedan od dva podsustava u II. organizacijskom sloju. Uloga podsustava je stvaranje središnjeg mjesta za modeliranje kriterija informacijske sigurnosti koji se povezuju sa štićenim vrijednostima metamodela politika informacijske sigurnosti. Vršna klasa *Kriteriji informacijske sigurnosti*, obuhvaća tri hijerarhije klasa razrađene klasama: *Temeljni sigurnosni kriteriji*, *Dodatni kriteriji* i *Ostali kriteriji*. Klasa *Temeljni sigurnosni kriteriji* specijalizira se u najčešće korištene kriterije u području informacijske sigurnosti klasama: *Povjerljivost*, *Cjelovitost* i *Raspoloživost*. Klasa *Privatnost* koristi se kao specijalizacija klase *Povjerljivost*, dok se klase *Autentičnost* i *Neporecivost* koriste kao specijalizacije klase *Cjelovitosti* prema [85]. Klasa *Dodatni kriteriji* specijalizira se u klase *Odgovornost* i *Sljedivost*, koje se koriste u politikama informacijske sigurnosti u slučaju visokih zahtjeva povjerljivosti, kao što je primjerice kategorija klasificiranih podataka posebne odgovornosti [73, 75]. U klasi *Ostali kriteriji* predviđena je specijalizacija na klase *Kriteriji povjerenja*, koji se koriste u nekim regulativnim zahtjevima, odnosno *Kriteriji kvalitete* koji se više primjenjuju u okviru ugovornih zahtjeva [2].




**Slika 6.10:** Podsustav kriterija informacijske sigurnosti (PS7), UML dijagram klasa

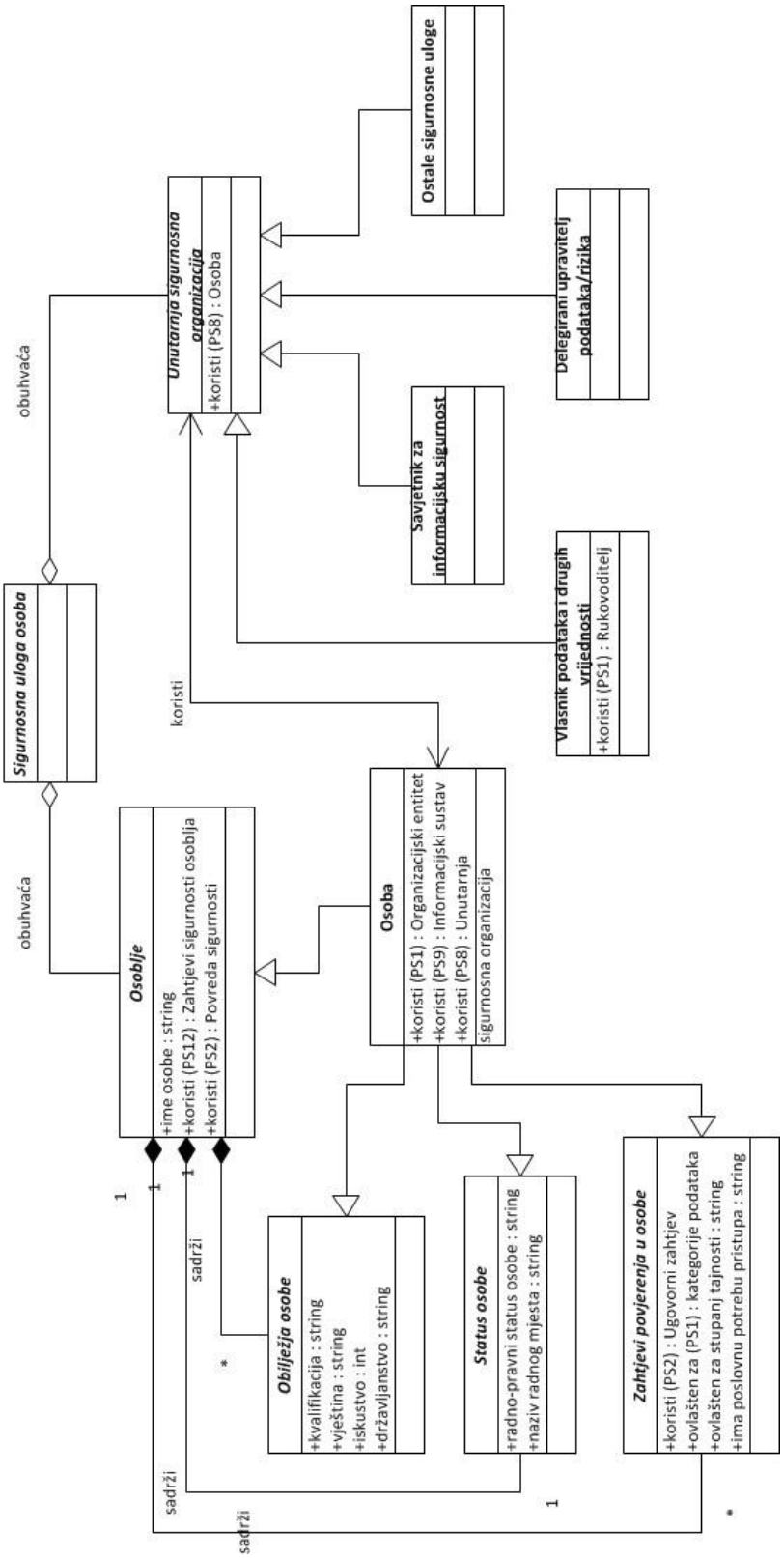
## 6.5. Razina upravljačkog dijela konceptualnog metamodela

Razina upravljačkog dijela konceptualnog metamodela (označena s III.), prema slici 6.1, modelira segment unutar kojeg se ostvaruje politika informacijske sigurnosti i definira temeljne čimbenike informacijske sigurnosti u metamodelu uz pomoć podsustava: definicija osoba (PS8), definicija informacijskih sustava (PS9) i definicija fizičke sigurnosti (PS10).

### 6.5.1. Podsustav definicija osoba

Podsustav definicija osoba, prikazan je na slici 6.11, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od tri podsustava na III. upravljačkoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje fizičkih osoba s obzirom na obilježja osoba i s obzirom na sigurnosne uloge osoba koje su potrebne u okviru politike informacijske sigurnosti.

Vršna klasa *Sigurnosna uloga osoba*, obuhvaća klasu *Osoblje* i klasu *Unutarnja sigurnosna organizacija*. Klasa *Osoblje* definira provedbeno najvažnije atribute osobe grupirane u tri sadržane klase s dodatnim obilježjima, statusom i zahtjevima povjerenja u osobe. Klasa *Osoba* specijalizira se višestrukim nasljeđivanjem i uz to koristi klasu *Unutarnja sigurnosna organizacija*. Klasa *Unutarnja sigurnosna organizacija* specijalizira se u niz klasa koje definiraju sigurnosne uloge u organizaciji koja provodi politiku informacijske sigurnosti i koje se koriste u različitim klasama koje definiraju odgovornosti određene vrste. Primjerice, definirana je klasa *Vlasnik podataka i drugih vrijednosti*, koja predstavlja odgovornog rukovoditelja. Klasa *Savjetnik za informacijsku sigurnost* specijalizira osnovnu sigurnosnu ulogu u politici informacijske sigurnosti, kao i klasa *Delegirani upravitelj podataka/rizika*. U klasi *Ostale sigurnosne uloge* predviđeno je definiranje svih drugih sigurnosnih uloga (sigurnosni koordinatori, vlasnici informacijskog sustava, administratori i sl.).



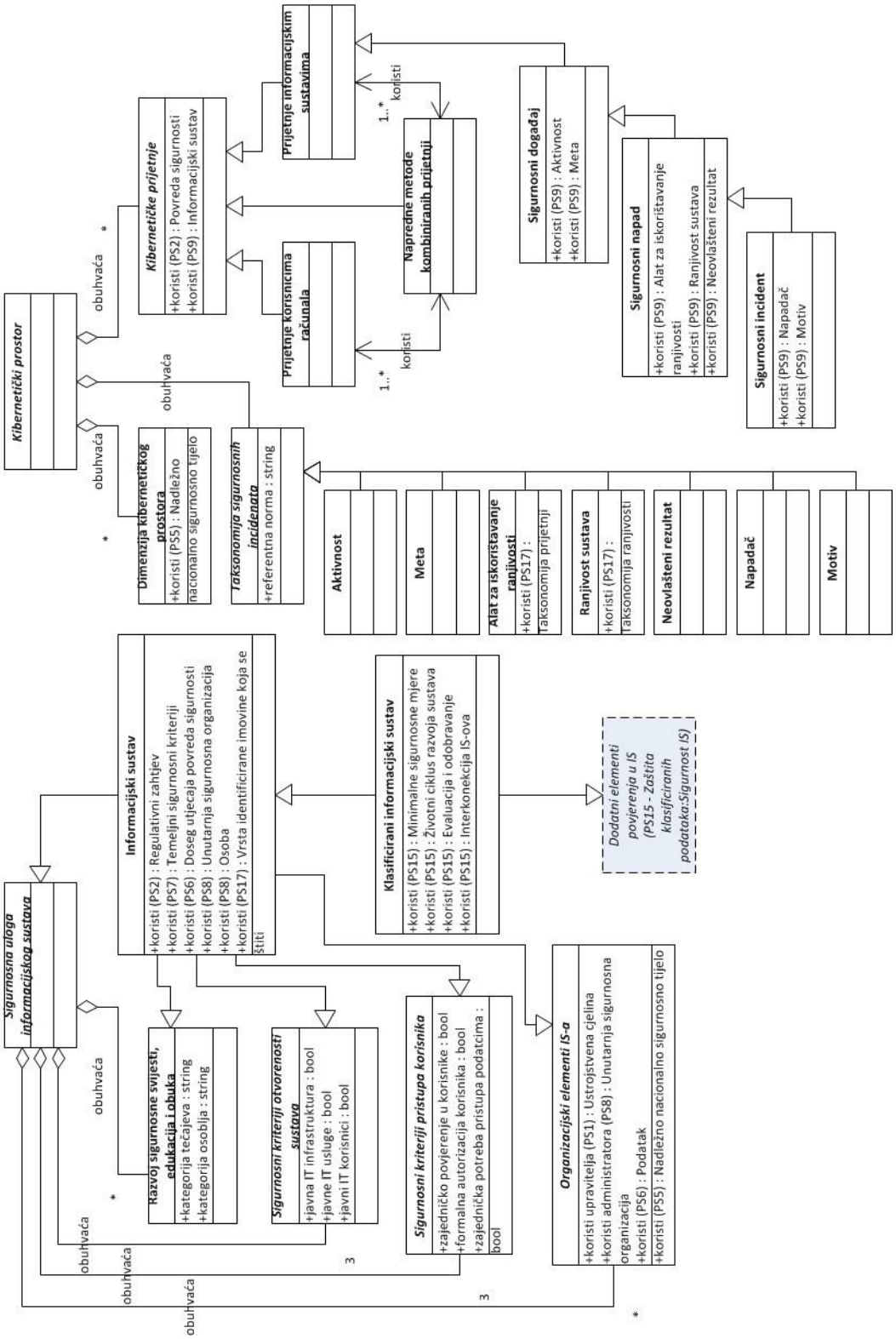

**Slika 6.11:** Podsustav definicija osoba (PS8), UML dijagram klasa

### 6.5.2. Podsustav definicije informacijskih sustava

Podsustav definicije informacijskih sustava, prikazan je na slici 6.12, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od tri podsustava na III. upravljačkoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje definicija informacijskih sustava s obzirom na njihova sigurnosna obilježja i sigurnosnu ulogu u okviru politike informacijske sigurnosti. Modeliranje podsustava provedeno je preko dvije vršne klase, klase *Sigurnosna uloga informacijskog sustava* i klase *Kibernetički prostor*. Klasa *Sigurnosna uloga informacijskog sustava* obuhvaća niz klasa kojima se definiraju različiti elementi prema [100], kao što su klase: *Organizacijski elementi IS-a*, *Sigurnosni kriteriji otvorenosti sustava*, *Sigurnosni kriteriji pristupa korisnika* te *Razvoj sigurnosne svijesti, edukacija i obuka*. Klasa *Informacijski sustav* predstavlja specijalizaciju navedenih klasa koje definiraju atribute informacijskih sustava bitne za politiku informacijske sigurnosti te se povezuje s kategorijama korištenih podataka definiranim u PS6. Klasa *Sigurnosni kriteriji otvorenosti sustava* predstavlja proširenje kriterija sigurnosnog načina rada sustava uvedenog za zatvorene klasificirane informacijske sustave prema [100]. Zbog specifičnih sigurnosnih zahtjeva, klasa *Klasificirani informacijski sustav* predstavlja daljnju specijalizaciju opće klase *Informacijski sustav*, koja istovremeno nasljeđuje i svojstva klase *Dodatni elementi povjerenja u IS* iz PS15 u izvršnom dijelu metamodela.

Klasa *Kibernetički prostor* obuhvaća klase: *Dimenzija kibernetičkog prostora*, *Taksonomija sigurnosnih incidenata* i *Kibernetičke prijetnje*. Klasom *Dimenzija kibernetičkog prostora* uvodi se taksonomija ključnih aspekata kibernetičkog prostora: društveni aspekti (uloga CERT hijerarhije), ekonomski aspekti (uloga regulatora tržišta elektroničkih komunikacija, kibernetička obrana (vojno obrambeno područje), kibernetička sigurnost (problematika kibernetičkog kriminala, terorizma, kritične informacijske infrastrukture i sl.) [5]. Klasa *Kibernetičke prijetnje* specijalizira se u tri klase: *Prijetnje korisnicima računala*, *Prijetnje informacijskim sustavima* i *Napredne metode kombiniranih prijetnji* (engl. *Advanced Persistent Threat – APT*), a klasa *Kibernetičke prijetnje* koristi klasu *Povreda sigurnosti* iz PS2. Klasa *Prijetnje informacijskim sustavima*, modelirana je prema taksonomiji iz [13], tako da se specijalizira u klasu *Sigurnosni događaj*, koja obuhvaća atribute veza prema klasama *Aktivnost* i *Meta*, te se dalje specijalizira klasom *Sigurnosni napad*, koja atributima dodaje veze prema klasama *Alat za iskorištavanje ranjivosti*, *Ranjivost sustava* i *Neovlašteni rezultat* te završava specijalizacijom u klasu *Sigurnosni incident*, koja dodaje atribute veza prema

klasama *Napadač* i *Motiv*. Atributi veza ovih klasa modelirani su kao podklase u hijerarhiji klase *Taksonomija sigurnosnih incidenata* [13].

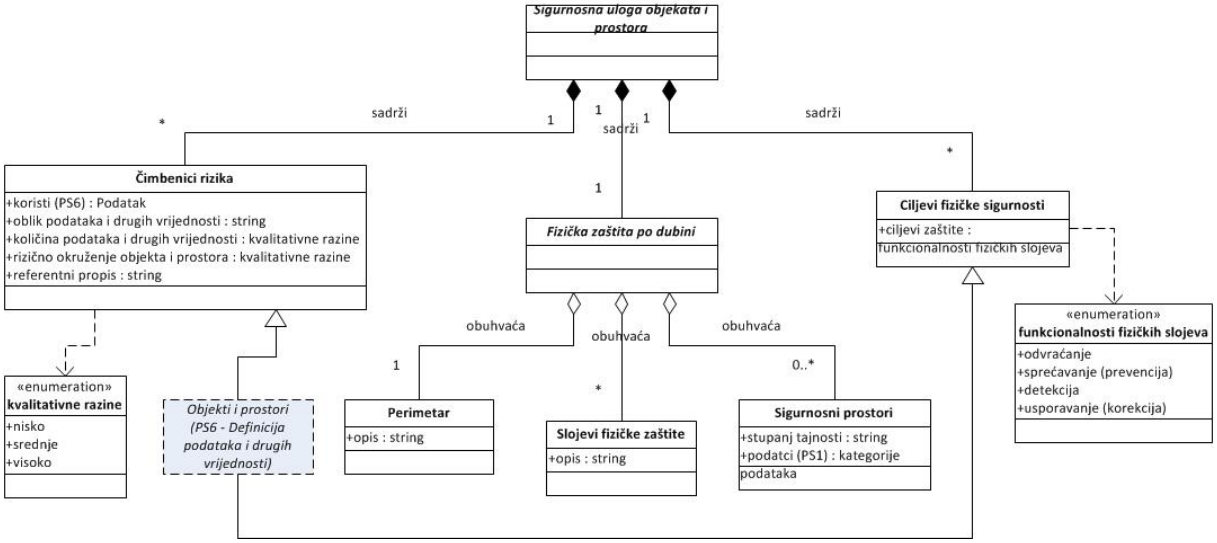



**Slika 6.12:** Podsustav definicije informacijskih sustava (PS9), UML dijagram klasa

### 6.5.3. Podsustav definicije fizičke sigurnosti

Podsustav definicije fizičke sigurnosti prikazan je na slici 6.13, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od tri podsustava na III. upravljačkoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje definicije fizičke sigurnosti s obzirom na sigurnosna obilježja, ciljeve i čimbenike te ulogu fizičke sigurnosti u okviru politike informacijske sigurnosti.

Modeliranje podsustava provedeno je preko vršne klase *Sigurnosna uloga objekata i prostora*, koja se povezuje s klasom *Objekti i prostori* definiranom u PS6, a sadrži tri klase: klasu *Čimbenici rizika*, koja se za potrebe politika državnog sektora dalje razrađuje klasom matrična metoda upravljanja rizikom u PS13, zatim klasu *Ciljevi fizičke sigurnosti* i klasu *Fizička zaštita po dubini* (engl. *Defence-in-Depth*). Klasa *Fizička zaštita po dubini*, obuhvaća klasu *Perimetar*, klasu *Slojevi fizičke zaštite* i klasu *Sigurnosni prostori*. Ove klase se također dodatno razrađuju za potrebe definiranja fizičke sigurnosti za zaštitu klasificiranih podataka u PS13.




**Slika 6.13:** Podsustav definicije fizičke sigurnosti (PS10), UML dijagram klasa

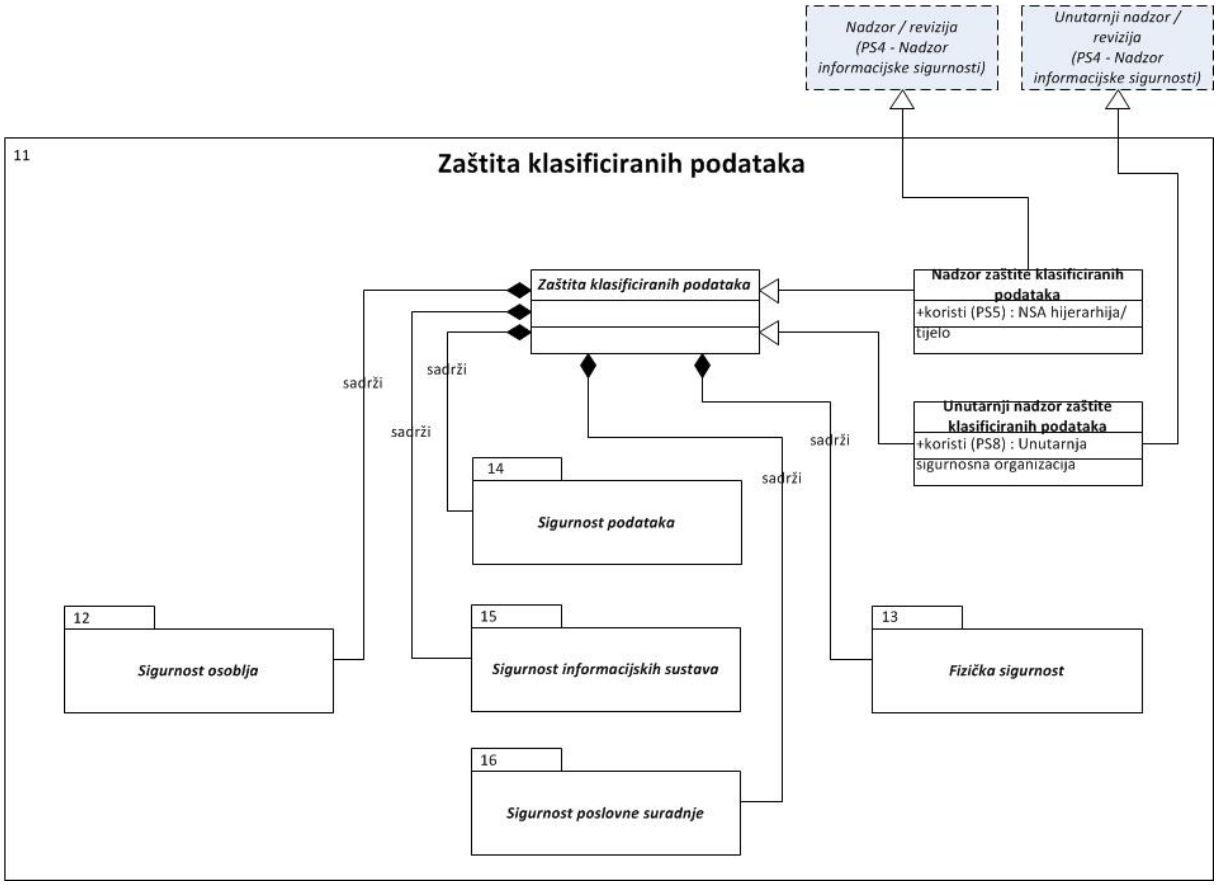
## 6.6. Razina izvršnog dijela konceptualnog metamodela

Razina izvršnog dijela konceptualnog metamodela (označena s IV.), prema slici 6.1, modelira segment unutar kojeg se provodi politika informacijske sigurnosti, a koji definira sigurnosne

mjere i kontrole u politikama informacijske sigurnosti prema slici 5.4 i za koji su u metamodelu odabrani podsustav zaštite klasificiranih podataka (PS11), koji obuhvaća dodatnih pet podsustava (PS12 do PS16), zatim podsustav sigurnosnih kontrola (PS17) i podsustav zaštite osobnih podataka (PS18).

### 6.6.1. Podsustav zaštite klasificiranih podataka

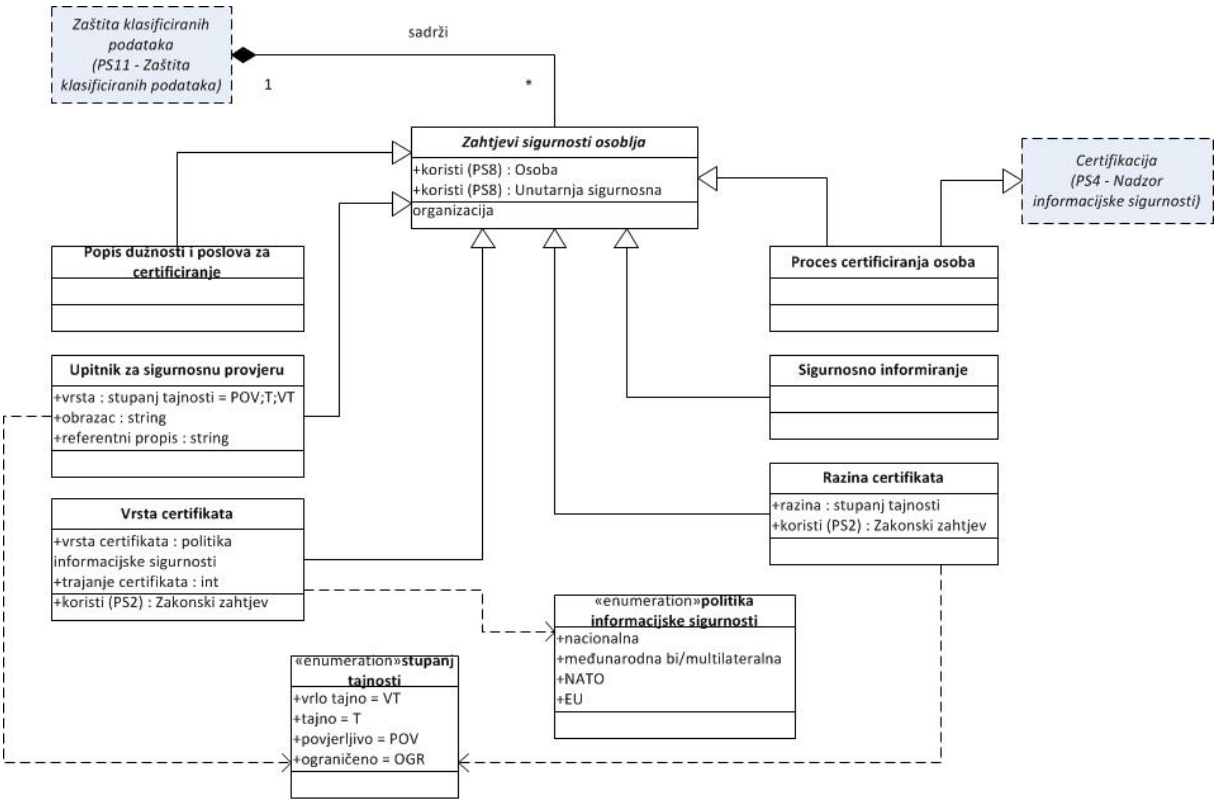
Podsustav zaštite klasificiranih podataka povezuje podsustave koji predstavljaju područja informacijske sigurnosti u politikama informacijske sigurnosti državnog sektora, podsustave: sigurnost osoblja (PS12), fizička sigurnosti (PS13), sigurnost podataka (PS14), sigurnost informacijskih sustava (PS15) i sigurnost poslovne suradnje (PS16). Ovaj podsustav, preko vršne klase *Zaštita klasificiranih podataka*, obuhvaća potrebne izvršne sigurnosne zahtjeve za pet navedenih podsustava i specijalizira se u potrebne klase nadzora zaštite klasificiranih podataka (vanjski i unutarnji).




**Slika 6.14:** Podsustav zaštite klasificiranih podataka (PS11), UML dijagram klasa

### 6.6.2. Podsustav sigurnosti osoblja

Podsustav sigurnosti osoblja, prikazan je na slici 6.15, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od pet podsustava, povezanih podsustavom zaštite klasificiranih podataka (PS11) na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje zahtjeva sigurnosti osoblja, s obzirom na sigurnosne zahtjeve koje postavlja politika informacijske sigurnosti državnog sektora u području sigurnosti osoblja kao jednom od pet područja informacijske sigurnosti, opisanom u poglavlju 4.7.3. (slika 4.9) prema [73, 75]. Zahtjevi definiraju proces sigurnosnog certificiranja i zahtjeve za certificirano osoblje tijekom vremena važenja sigurnosnog certifikata. Podsustav je modeliran preko vršne klase *Zahtjevi sigurnosti osoblja*, koja se specijalizira na niz klasa s različitim vrstama atributa (*Popis dužnosti i poslova za certificiranje*, *Upitnik za sigurnosnu provjeru*, *Vrsta certifikata*, *Razina certifikata*), klasu *Sigurnosno informiranje* te klasu *Proces certificiranja osoba*, koja je istovremeno i specijalizacija klase certifikacija iz PS4. Klasa *Zahtjevi sigurnosti osoblja* iz ovog podsustava povezuje se s klasama *Osoba* i *Unutarnja sigurnosna organizacija* iz PS8.

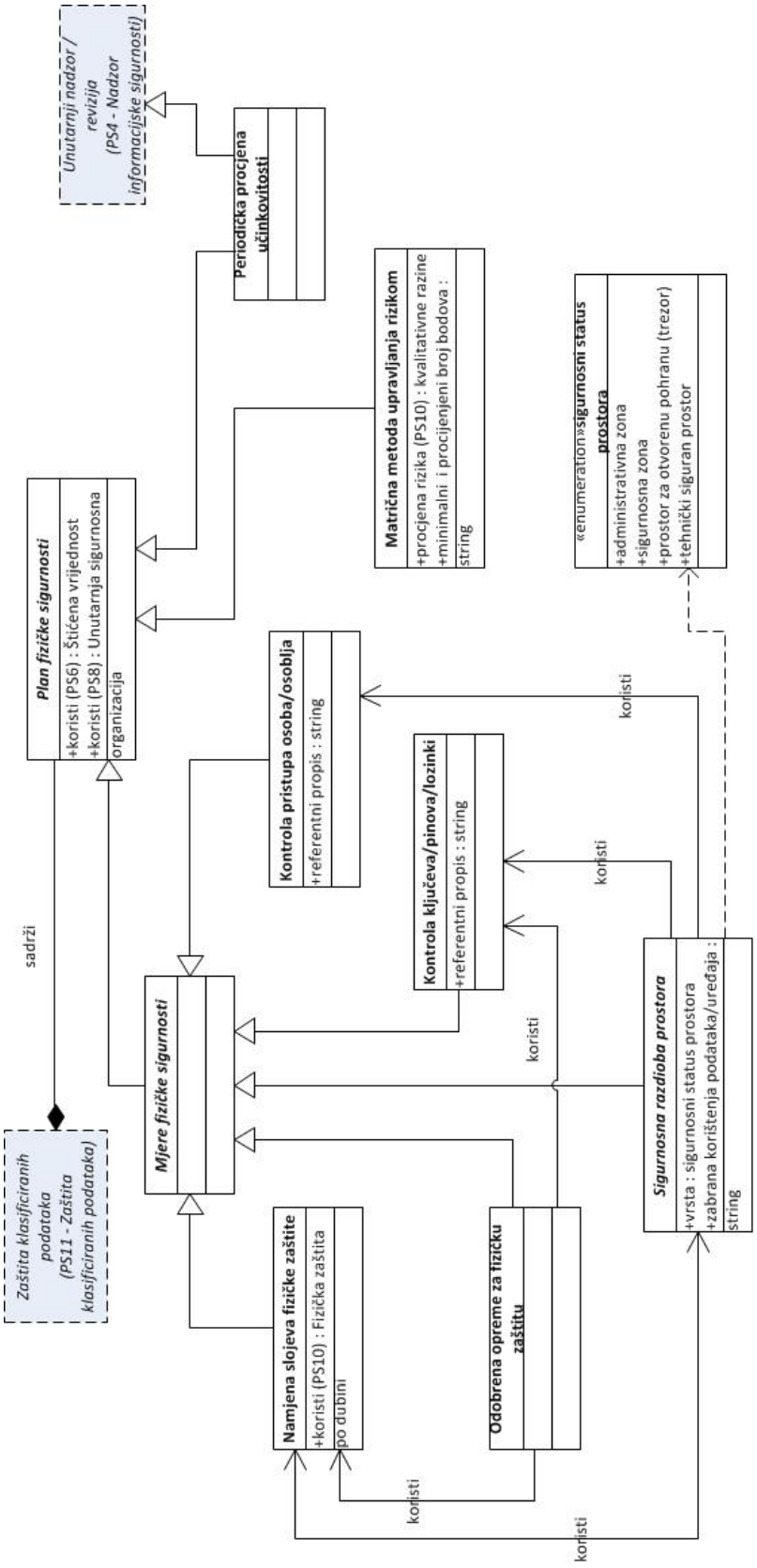



**Slika 6.15:** Podsustav sigurnosti osoblja (PS12), UML dijagram klasa

### 6.6.3. Podsustav fizičke sigurnosti

Podsustav fizičke sigurnosti, prikazan je na slici 6.16, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od pet podsustava, povezanih podsustavom zaštite klasificiranih podataka (PS11) na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje zahtjeva fizičke sigurnosti s obzirom na sigurnosne zahtjeve koje postavlja politika informacijske sigurnosti državnog sektora u području fizičke sigurnosti, kao jednom od pet područja informacijske sigurnosti, opisanom u poglavlju 4.7.2. (slika 4.8) prema [53, 73, 75]. Zahtjevi fizičke sigurnosti definiraju uspostavu fizičke zaštite po dubini, kao i pravila sigurnosne kategorizacije objekata i prostora te odgovarajućeg opremanja i kontrole uspostavljenih slojeva fizičke zaštite i sigurnosno kategoriziranih prostora, kao i određenu provedbu kontrola pristupa i korištenja sigurnosnih prostora i spremnika. Podsustav je modeliran preko vršne klase *Plan fizičke sigurnosti*, koja se specijalizira na više hijerarhija klasa kao što su klase: *Mjere fizičke sigurnosti*, *Matrična metoda upravljanja rizikom* i *Periodička procjene učinkovitosti*, koja je istovremeno i specijalizacija klase *Unutarnji nadzor/revizija* iz PS4.

Hijerarhija klasa ispod klase *Mjere fizičke sigurnosti*, obuhvaća modeliranje i međusobno povezivanje tipičnih mjera fizičke sigurnosti za ovo područje. Klasa *Namjena slojeva fizičke zaštite*, dalje razrađuje klasu *Fizička zaštita po dubini* iz podsustava PS10, koristeći pri tome klasu *Odobrena opreme za fizičke zaštitu*. Klasa *Sigurnosna razdioba prostora*, koristi klasu *Namjena slojeva fizičke zaštite*, obuhvaćajući pri tome podatkovni tip atributa *sigurnosni status prostora*. Klasa *Kontrola ključeva/pinova/lozinki* i klasa *Kontrola svih vrsta osoba/osoblja*, koriste klasu *Sigurnosna razdioba prostora*. Cjelokupni plan fizičke sigurnosti preko istoimene vršne klase povezan je s klasama *Štićena vrijednost* iz PS6 i *Unutarnja sigurnosna organizacija* iz PS8.

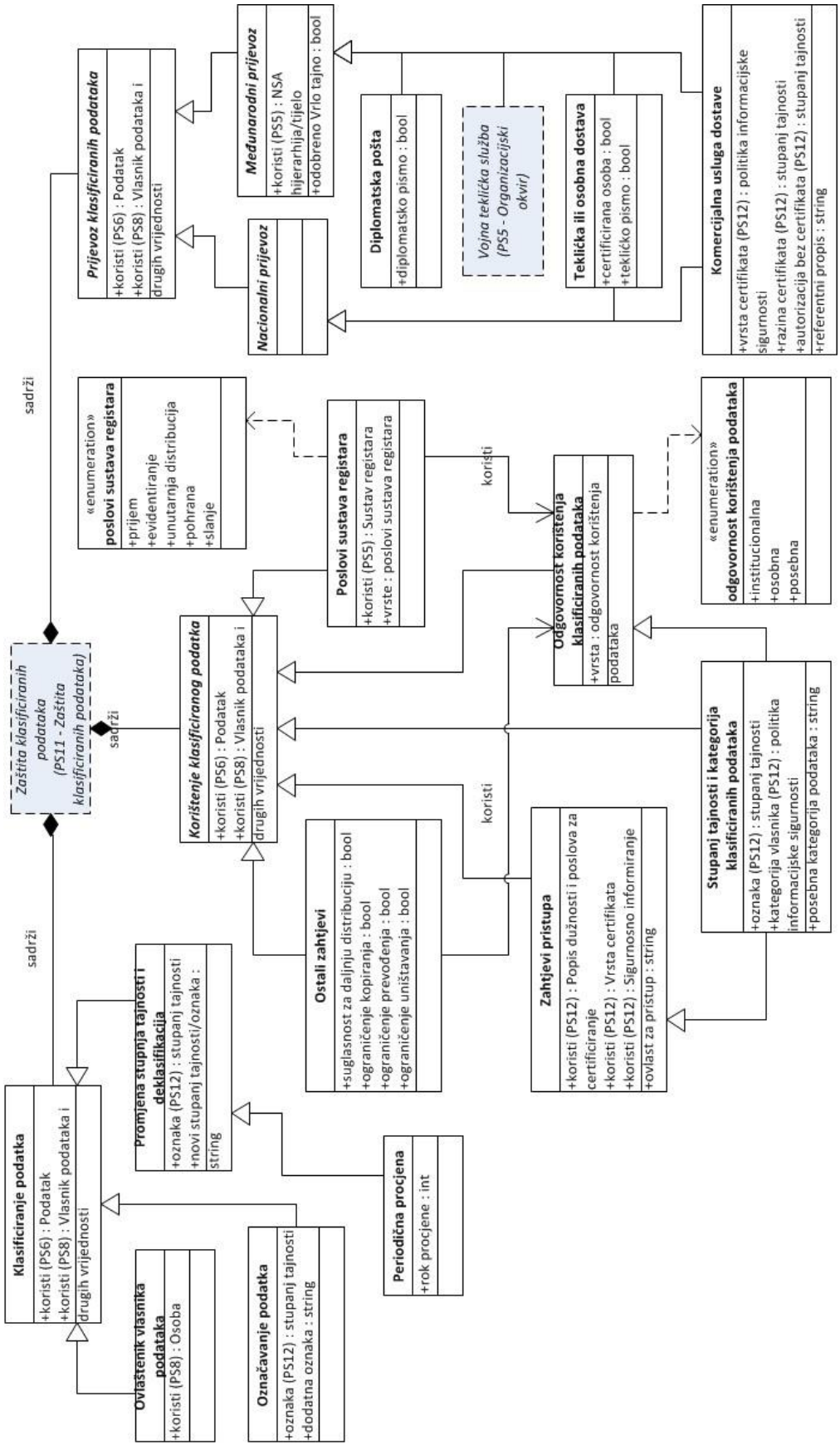



**Slika 6.16:** Podsustav fizičke sigurnosti (PS13), UML dijagram klasa

### 6.6.4. Podsustav sigurnosti podataka

Podsustav sigurnosti podataka, prikazan je na slici 6.17, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od pet podsustava, povezanih podsustavom zaštite klasificiranih podataka (PS11) na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje zahtjeva sigurnosti klasificiranih podataka s obzirom na sigurnosne zahtjeve koje postavlja politika informacijske sigurnosti državnog sektora u području sigurnosti podataka, kao jednom od pet područja informacijske sigurnosti opisanog u poglavljima 4.3.1. i 4.7.1. prema [73, 75]. Podsustav je modeliran preko tri vršne klase: *Klasificiranje podatka, Korištenje klasificiranog podatka* i *Prijevoz klasificiranih podataka,* koje se dalje razrađuju. Klasa *Klasificiranje podatka* sadrži klasu *Označavanje podatka*, klasu *Promjena stupnja tajnosti i deklasifikacija*, koja se koristi u klasi *Javni pristup* u podsustavu PS3, te klasu *Ovlaštenik vlasnika podatka*. Klasa *Korištenje klasificiranog podatka*, sadrži klasu *Stupanj tajnosti i kategorija klasificiranih podataka*, klasu *Zahtjevi pristupa*, klasu *Odgovornost korištenja klasificiranih podataka* te klasu *Ostali zahtjevi* i klasu *Poslovi sustava registara*, povezanu s podatkovnim tipom *poslovi sustava registara*. Ovim klasama definira se niz potrebnih grupa atributa koji se međusobno povezuju odgovarajućim relacijama.

Klasa *Prijevoz klasificiranih materijala* modelirana je specijalizacijom na dvije hijerarhije klasa, za nacionalni i međunarodni prijevoz. Različiti načini prijevoza klasificiranih podataka definirani su klasama: *Diplomatska pošta*, *Vojna teklićka služba* iz PS5, *Teklićka ili osobna dostava* i *Komercijalna usluga dostave*, pri čemu su ove klase specijalizacija nacionalnog, međunarodnog ili oba načina prijevoza, s dodatnim definiranim atributima.




**Slika 6.17:** Podsustav sigurnosti podataka (PS14), UML dijagram klasa

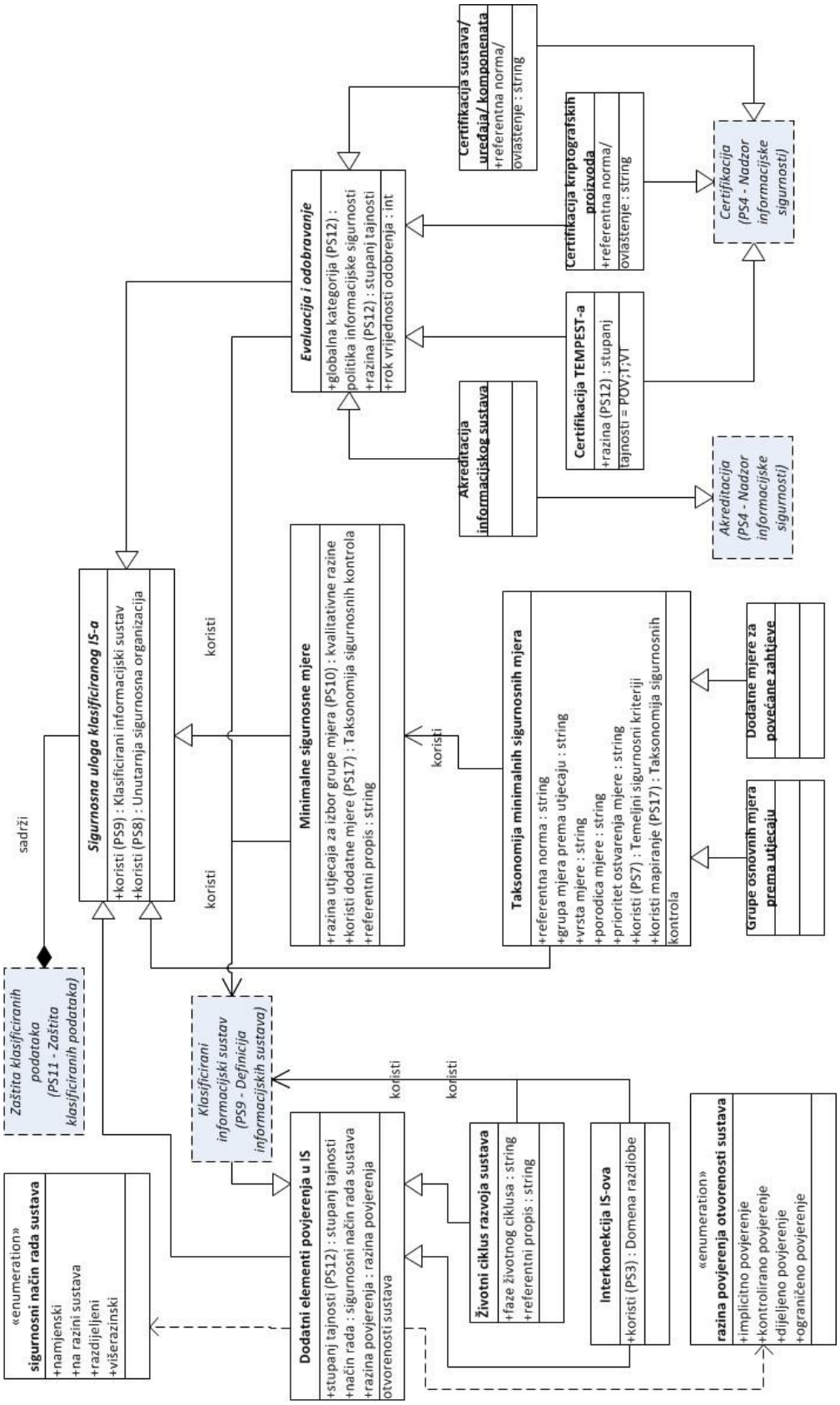
### 6.6.5. Podsustav sigurnosti informacijskih sustava

Podsustav sigurnosti informacijskih sustava, prikazan je na slici 6.18, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od pet podsustava, povezanih podsustavom zaštite klasificiranih podataka (PS11) na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje zahtjeva sigurnosti informacijskih sustava s obzirom na sigurnosne zahtjeve koje postavlja politika informacijske sigurnosti državnog sektora u području sigurnosti informacijskih sustava, kao jednom od pet područja informacijske sigurnosti, opisanom u poglavlju poglavlje 4.8. (slika 4.10) prema [73, 75, 82].

Podsustav je modeliran preko vršne klase *Sigurnosna uloga klasificiranog IS-a*, koja se specijalizira u zahtjeve definirane klasom *Evaluacija i odobravanje*, koja ima podklase različitih vrsta evaluacija i odobravanja, koje istovremeno predstavljaju specijalizaciju klasa *Akreditacija* i *Certifikacija* iz PS4. Ovdje su definirane klase *Akreditacija informacijskog sustava*, *Certifikacija TEMPEST-a* (neželjeno elektromagnetsko zračenje), *Certifikacija kriptografskih proizvoda* i *Certifikacija sustava/uređaja/komponenata*.

Klasa *Sigurnosna uloga klasificiranog IS-a*, specijalizira se i u klasu *Minimalne sigurnosne mjere*, koja koristi klasu *Taksonomija minimalnih sigurnosnih kontrola* razvijenu prema [85], zasnovanu na jednoj ili više grupa minimalnih sigurnosnih mjera, sukladno procjeni utjecaja povreda sigurnosti na ključne kategorije podataka koje se koriste na informacijskom sustavu. Ova taksonomija minimalnih sigurnosnih mjera obostrano je mapirana s klasom *Taksonomija sigurnosnih kontrola* iz PS17, zasnovanoj na međunarodnoj normi ISO 27001 [27].

Klasa *Dodatni elementi povjerenja u IS*, također je specijalizacija vršne klase ovog podsustava, koja koristi dvije grupe podatkovnih tipova atributa: *sigurnosni način rada sustava*, *razina povjerenja otvorenosti sustava*, prema [100], te se dalje specijalizira u klasu *Životni ciklus razvoja sustava* i klasu *Interkonekcija IS-ova*. Klasa *Klasificirani informacijski sustav* iz PS9, specijalizira se dodatno i iz klase *Dodatni elementi povjerenja u IS* (višestruko nasljeđivanje) te koristi ostale klase ovog podsustava u svrhu korištenja atributa definiranih u ovim klasama, ovisno o obilježjima ciljnih okruženja u kojim se provodi politika informacijske sigurnosti (*Minimalne sigurnosne mjere*, *Evaluacija i odobravanje*, *Životni ciklus sustava*, *Interkonekcija IS-ova*).



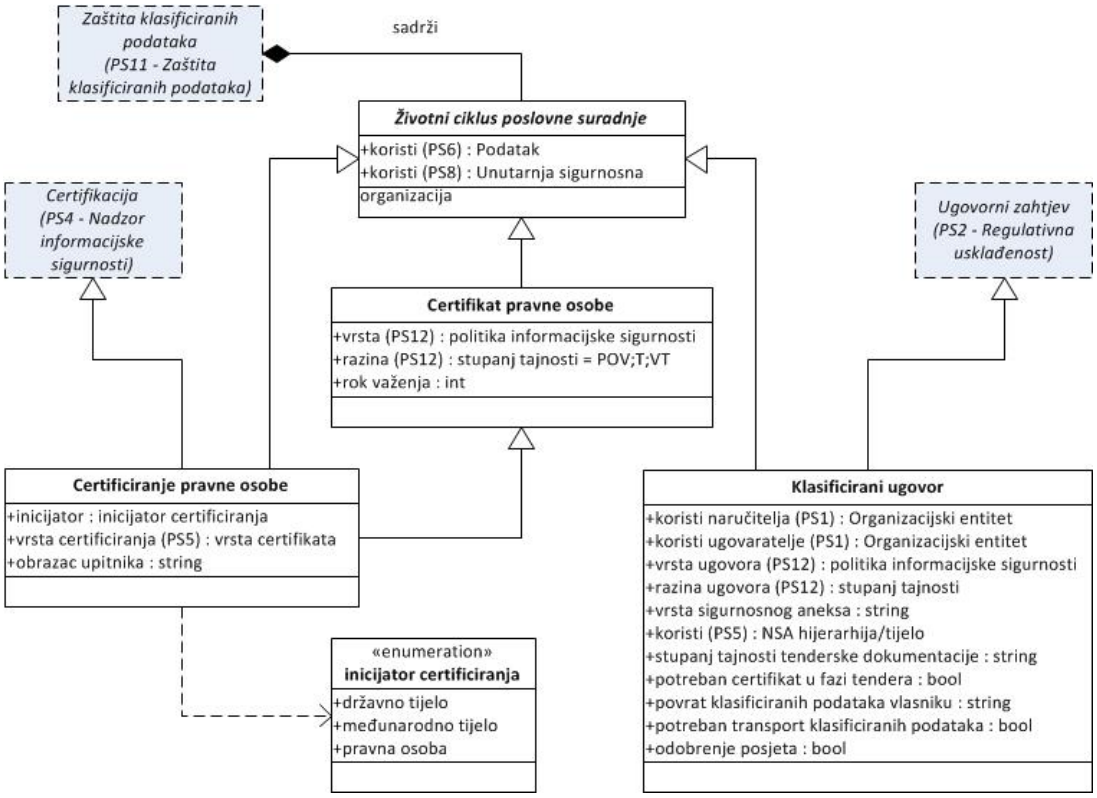

**Slika 6.18:** Podsustav sigurnosti informacijskih sustava (PS15), UML dijagram klasa

### 6.6.6. Podsustav sigurnosti poslovne suradnje

Podsustav sigurnosti poslovne suradnje, prikazan je na slici 6.19, a prema prikazu konceptualnog metamodela na slici 6.1, predstavlja jedan od pet podsustava, povezanih podsustavom zaštite klasificiranih podataka (PS11) na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje zahtjeva sigurnosti poslovne suradnje s obzirom na sigurnosne zahtjeve koje postavlja politika informacijske sigurnosti državnog sektora u području sigurnosti poslovne suradnje, kao jednom od pet područja informacijske sigurnosti, opisanom u poglavlju 4.7.3. prema [73, 75]. S obzirom da je klasificirani ugovor povezan s razdiobom, stvaranjem ili uvidom u klasificirane podatke, naručitelji klasificiranih ugovora mogu biti samo organizacijski entiteti koji su vlasnici klasificiranih podataka, a ugovaratelji mogu biti pravne osobe koje su odgovarajuće certificirane. Inicijatori certificiranja pri tome mogu biti i naručitelji i ugovaratelji.

Podsustav je modeliran preko vršne klase *Životni ciklus poslovne suradnje*, koja se specijalizira na klase *Certificiranje pravne osobe*, *Certifikat pravne osobe* i *Klasificirani ugovor*. Klasa *Certificiranje pravne osobe*, specijalizacija je i klase *Certifikacija* iz PS4 te koristi podatkovni tip atributa *inicijator certificiranja*. Klasa *Certificiranje pravne osobe*, predstavlja proces koji je specijalizacija klase *Certifikat pravne osobe*.

Klasa *Klasificirani ugovor*, predstavlja specijalizaciju klase *Ugovorni zahtjev* iz PS2 i vršne klase ovog podsustava te sadrži niz atributa specifičnih za ovu vrstu klasificiranih ugovora, s obzirom na specifične uvjete za naručitelja, ugovaratelja, vrstu i stupanj tajnosti ugovora, nadležna tijela, postupak javnog nadmetanja i izvođenje ugovora. Ova klasa sadrži niz atributa koji opisuju proces ostvarenja jednog klasificiranog ugovora (organizacijski entiteti kao naručitelj i ugovaratelji, vrsta i stupanj tajnosti klasificiranog ugovora, specifičnosti faze javnog nadmetanja i drugo).




**Slika 6.19:** Podsustav sigurnosti poslovne suradnje (PS16), UML dijagram klasa

### 6.6.7. Podsustav sigurnosnih kontrola

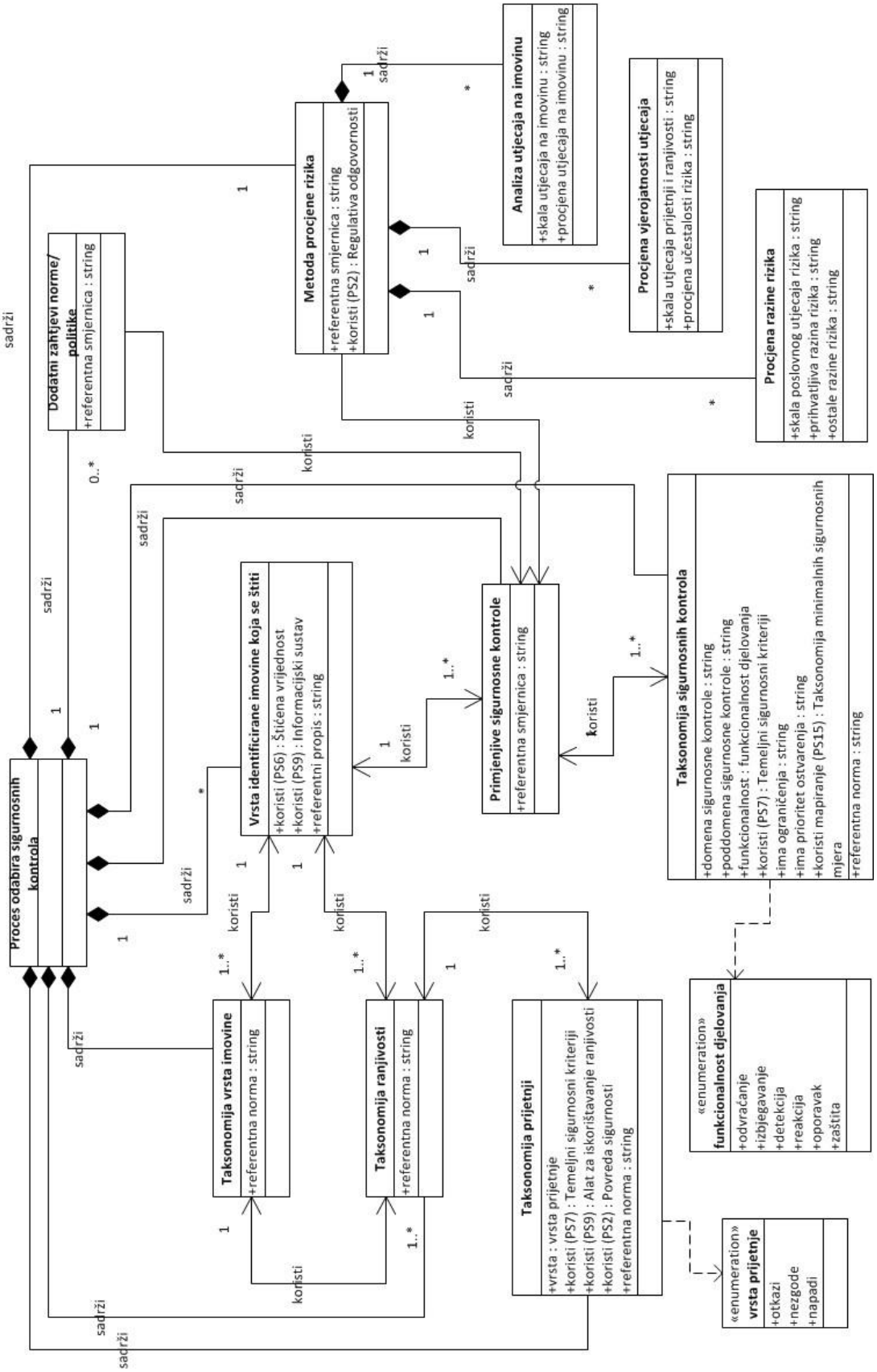
Sljedeći podsustav na IV. izvršnoj razini konceptualnog metamodela je podsustav sigurnosnih kontrola, koji je prikazan na slici 6.20. Uloga ovog podsustava je modeliranje primjenjivih sigurnosnih kontrola s obzirom na vrstu identificirane imovine, procijenjene ranjivosti imovine, moguće prijetnje, odnosno procijenjene rizike sukladno odabranoj metodi procjene rizika, ili dodatnim zahtjevima norme ili politike informacijske sigurnosti. Podsustav je modeliran za potrebe korištenja metoda upravljanja rizikom u svrhu izbora sigurnosnih kontrola prema ISO27001 zahtjevima u [27], opisanom u poglavlju 4.8 i prikazanom na slici 4.11.

Podsustav je modeliran preko vršne klase *Proces odabira sigurnosnih kontrola*, koja predstavlja ovojnicu osam glavnih klasa: *Vrsta identificirane imovine koja se štiti*,

*Taksonomija vrste imovine*, *Taksonomija ranjivosti*, *Taksonomija prijetnji*, *Primjenjive sigurnosne kontrole*, *Taksonomija sigurnosnih kontrola*, *Dodatni zahtjevi norme/politike*, kao i klasu *Metoda procjene rizika*, koja sadrži dodatne klase *Analiza utjecaja na imovinu*, *Procjena vjerojatnosti utjecaja* i *Procjena razine rizika*.

Podsustav PS17 modeliran je s ciljem sukladnosti s različitim načinima primjene međunarodne norme ISO 27001 u državnom i poslovnom sektoru. Modeliranje je provedeno relacijama između navedenih klasa, tako da primjerice *Vrsta identificirane imovine* koristi *Taksonomiju vrsta imovine* (katalog vrsta), koja je povezana s *Taksonomijom ranjivosti* za takvu imovinu (katalog ranjivosti), odnosno s *Taksonomijom prijetnji* za određene vrste ranjivosti (katalog prijetnji), pri čemu se koriste taksonomije prema [91]. *Vrsta identificirane imovine* koristi *Primjenjive sigurnosne kontrole*, za koje se koristi *Taksonomija sigurnosnih kontrola* (katalog kontrola) prema ISO 27001 [27]. Izbor primjenjivih kontrola koristi rezultate primjene klase *Metode procjene rizika* i klasu *Dodatni zahtjevi norme/politike* informacijske sigurnosti.

Ovako modelirani podsustav povezan je na klasu *Ranjivost sustava* iz PS9, koja koristi klasu *Taksonomija ranjivosti* iz PS17. *Taksonomija prijetnji* iz PS17 koristi klasu *Povreda sigurnosti* iz PS2 te klasu *Alat za iskorištavanje ranjivosti* iz PS9, čime su sve razine prijetnji i ranjivosti povezane od ove najniže, izvršne razine, do vršne razine globalnog okruženja modela. Također, gledajući razine općenitosti korištenih taksonomija, povezane su istovrsne taksonomije različite razine specijalizacije. Primjerice, povezane su klasa *Alat za iskorištavanje ranjivosti* iz PS9, kao taksonomija specijalizirane klase prijetnji informacijskim sustavima (sredstva za iskorištavanje računalne ili mrežne ranjivosti) [13], i klasa *Taksonomija prijetnji* iz PS17, koja predstavlja općenitu taksonomiju prijetnji na: otkaze (slučajne), nezgode (prirodne i okoliš) i napade (namjerne) [91].




**Slika 6.20:** Podsustav sigurnosnih kontrola (PS17), UML dijagram klasa

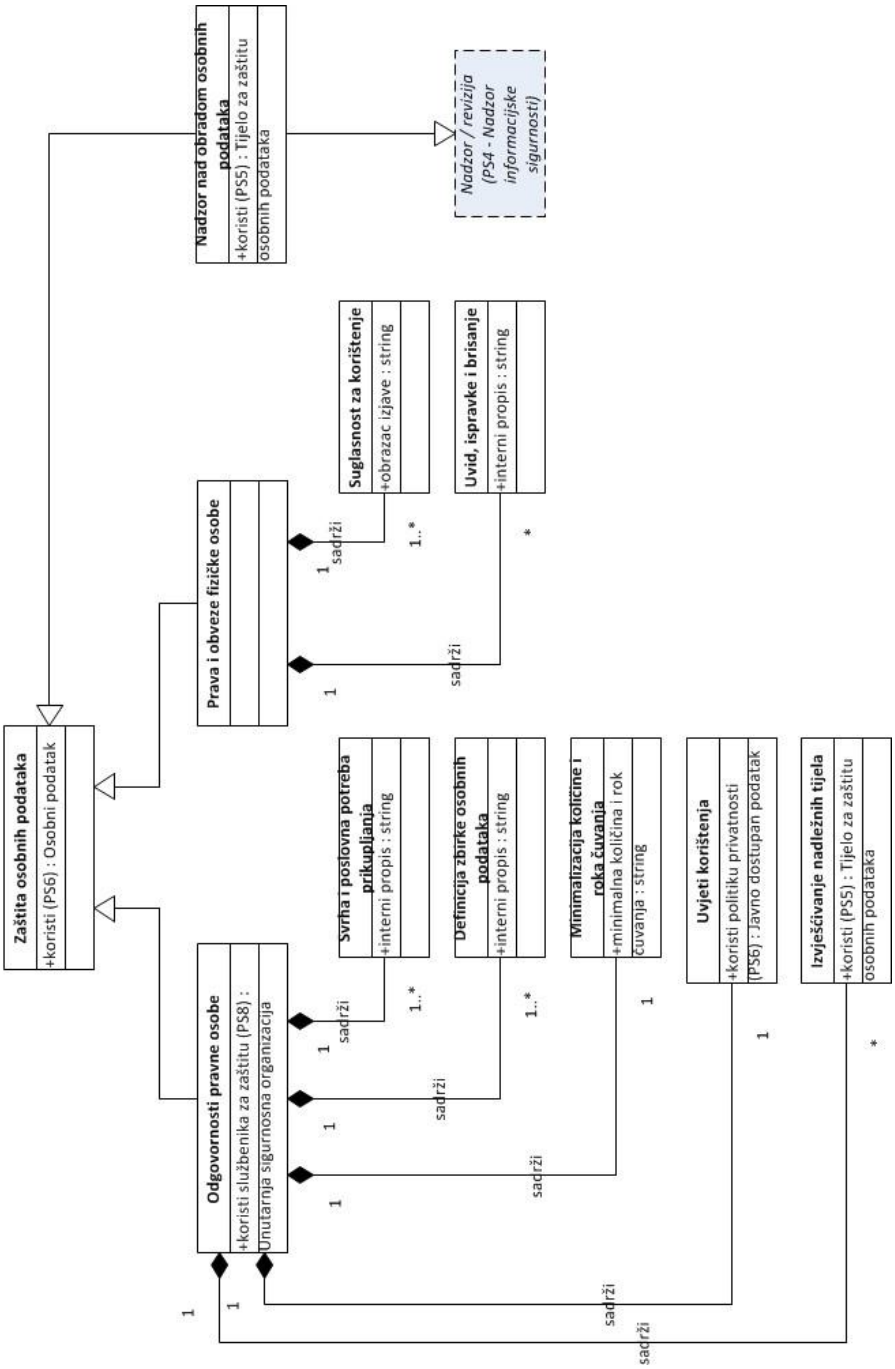
### 6.6.8. Podsustav zaštite osobnih podataka

Podsustav zaštite osobnih podataka, prikazan je na slici 6.21, a na slici 6.1 koja prikazuje konceptualni metamodel, predstavlja jedan od podsustava na IV. izvršnoj razini konceptualnog metamodela. Uloga ovog podsustava je modeliranje posebnih sigurnosnih mjera za zaštitu osobnih podataka koje su specifične za domenu osobnih podataka, opisanu u poglavlju 4.9.2. i nisu obuhvaćene konceptima modeliranim u prethodnim podsustavima konceptualnog metamodela.

Podsustav je modeliran preko vršne klase *Zaštita osobnih podataka*, koja se specijalizira u klase *Odgovornosti pravne osobe*, *Prava i obaveze fizičke osobe*, *Nadzor nad obradom osobnih podataka*. Ovo su tri temeljne grupe mjera koje su usmjerene prema odgovornostima pravne osobe - voditelja zbirke osobnih podataka, prema pravima i obavezama koja se moraju osigurati fizičkim osobama za njihove osobne podatke u uspostavljenim zbirkama osobnih podataka, kao i prema funkcionalnostima nadzora nad obradom osobnih podataka koje moraju biti uspostavljene.

Klasa *Odgovornosti pravne osobe* sadrži klase: *Svrha i poslovna potreba prikupljanja*, *Definicija zbirke osobnih podataka*, *Minimalizacija količine i roka čuvanja*, *Uvjeti korištenja* i *Izvješćivanje nadležnih tijela*. Klasa *Prava i obaveze fizičkih osoba* sadrži klasu *Suglasnost za korištenje* i klasu *Uvid, ispravke i brisanje*. Klasa *Nadzor nad obradom osobnih podataka* je specijalizacija klase *Nadzor/revizija* iz PS4 te koristi klasu *Tijelo za zaštitu osobnih podataka* iz PS5.

Kategorija osobnih podataka koja se definira kao instanca klase *Osobni podatak* iz PS6, koristi sve tri glavne klase ovog podsustava: *Odgovornosti pravne osobe*, *Prava i obaveze fizičke osobe* i *Nadzor nad obradom osobnih podataka*, dok ostale klase koje su sadržane u ovim klasama, primarno služe grupiranju atributa na način sukladan postavljenim sigurnosnim zahtjevima prema regulativi opisanoj u poglavlju 4.9.2. [93, 94, 95, 96].




**Slika 6.21:** Podsustav zaštite osobnih podataka (PS18), UML dijagram klasa

## 6.7. Namjena i korištenje konceptualnog metamodela

Predložena metoda modeliranja politika informacijske sigurnosti obuhvaća životni ciklus politike informacijske sigurnosti prikazan u globalnom okruženju i transformiran u hijerarhijsku taksonomiju domene koja je ostvarena i prikazana u prilogu B. U sljedećoj fazi modeliranja, pored osnovnog hijerarhijskog odnosa između koncepata, ostvarene su i relacije

između različitih koncepata, kao i atributi koncepata, čime je omogućeno ostvarenje konceptualnog metamodela koji se temelji na domenskom rječniku, sintaksi hijerarhijske domenske taksonomije i semantici uvedenoj relacijama i atributima klasa. Ovakav konceptualni metamodel zapisan je u UML-u dijagramima klasa i prikazan uz pomoć opisa i dijagrama klasa 18 podsustava od kojih se sastoji. Relacije između klasa konceptualnog metamodela dodatno su specificirane prema primjeru u tablici 6.2, a u cijelosti su prikazane u prilogu C. Relacije između klasa definirane su u konceptualnom UML metamodelu kao daljnja razrada hijerarhijske domenske taksonomije iz priloga B, zajedno s atributima koji su prikazani na dijagramima klasa. Za svaku relaciju prikazane su klase koje relacija povezuje, oznaka relacije na UML dijagramu klasa te opis značenja relacije, čime se osigurava domenski valjana interpretacija uvedenih relacija. Konceptualni metamodel suvremenih politika informacijske sigurnosti, specificiran na ovaj način, predstavlja okvir za upravljanje i komuniciranje znanjem domene, koji povezuje postojeće heterogeno i slabo povezano domensko znanje iz dominantnih politika i normi informacijske sigurnosti.

**Tablica 6.2:** Primjeri relacija između klasa definiranih u konceptualnom UML metamodelu kao daljnja razrada hijerarhijske domenske taksonomije

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| **PODSUSTAV PS3: RAZDIOBA PODATAKA** | | | |
| 1. | Poslovna razdioba – PS6/Podatak | *koristi* | *Poslovna razdioba povezuje se s kategorijom podataka na koju se odnosi;* |
| 2. | Poslovna razdioba – PS1/Organizacijski entitet | *koristi upravitelja* | *Poslovna razdioba povezuje se s organizacijskim entitetom koji je upravitelj poslovne razdiobe;* |
| 3. | Interesna skupina – PS1/Organizacijski entitet | *koristi članove* | *Interesna skupina za poslovnu razdiobu povezuje se s org. entitetima koji su članovi skupine;* |
| 4. | Domena razdiobe – PS2/Regulativni zahtjev | *koristi* | *Pridruživanje regulativnog zahtjeva kojim se definira domena razdiobe;* |
| 5. | Domena razdiobe – Organizacijska pravila | *ograničava* | *Pridruživanje organizacijskih pravila domeni razdiobe;* |
| 6. | Domena razdiobe – Semantička pravila | *ograničava* | *Pridruživanje semantičkih pravila domeni razdiobe;* |
| 7. | Domena razdiobe – Tehnička pravila | *ograničava* | *Pridruživanje tehničkih pravila domeni razdiobe;* |
| 8. | Tehnička pravila – PS15/Evaluacija i odobravanje | *koristi* | *Pridruživanje odgovarajućih zahtjeva za evaluaciju i odobravanje tehničkim pravilima domene razdiobe;* |
| 9. | Javna razdioba – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Svakoj javnoj razdiobi pridružuje se vlasnik podataka;* |
| 10. | Javna objava – PS6/Podatak | *koristi* | *Svakoj javnoj razdiobi pridružuje se definirani podatak;* |

Cilj ove razine modeliranja jest ostvarenje konceptualnog metamodela šire domenske razine u UML-u. Svrha konceptualnog metamodela u UML-u je upravljanje i komuniciranje znanjem

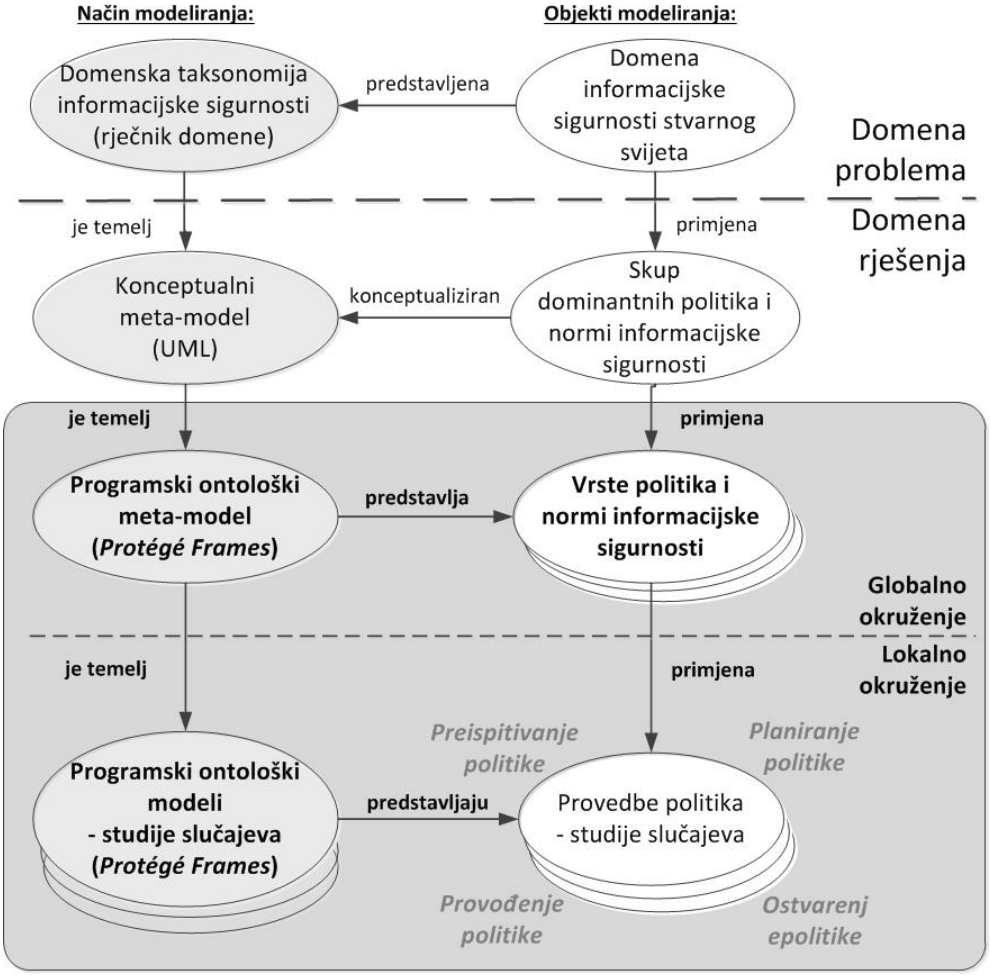
iz domene, a prvenstveno je namijenjen stručnjacima za informacijsku sigurnost kako bi im olakšao međusobnu komunikaciju o različitim sektorskim rješenjima politika i normi informacijske sigurnosti te pružio zajednički domenski jezik za komunikaciju, kao i alat za planiranje i logičko povezivanje utjecaja promjena u okruženju politike informacijske sigurnosti za koju su odgovorni. S obzirom da su stručnjaci za informacijsku sigurnost vrlo heterogenih stručnih profila te da su rasprostranjeni u organizacijama različitih profila i sektora poslovanja koje provode različite norme i politike informacijske sigurnosti, vizualni prikaz i razina detalja konceptualnog metamodela ostvarenog u UML-u, prilagođeni su opisanim namjenama i ciljevima korištenja (slika 6.2).

Namjena ostvarenog konceptualnog UML metamodela u svrhu komuniciranja znanjem domene, znači da ostvareni konceptualni UML metamodel omogućava vizualnu podlogu za raspravu stručnjaka o politikama informacijske sigurnosti u različitim poslovnim primjenama. Pri tome se na temelju prikazanog modela može vidjeti koncepte koji su ostvareni u nekoj politici informacijske sigurnosti i ukazati na neke druge sigurnosne koncepte koje tek treba ostvariti; zatim, uočiti razlike između planiranih i provedenih mjera, kao i između pristupa u različitim organizacijama koje trebaju surađivati ili razmjenjivati određenu vrstu osjetljivih podataka.

Namjena ostvarenog konceptualnog UML metamodela u svrhu upravljanja znanjem iz domene, omogućava rukovoditeljima sigurnosti u različitim pravnim osobama i državnim tijelima pregledan način prikaza širih domenskih koncepata, što je potrebno prilikom uvođenja politika i normi informacijske sigurnosti ili prilikom njihove dorade koja se provodi u različitim situacijama tijekom životnog ciklusa politika informacijske sigurnosti prikazanih prema slici 5.2. Pored toga, ostvareni konceptualni UML metamodel služi i kao formalna specifikacija za daljnje razine metode modeliranja prema slici 7.1, odnosno za programsko ostvarenje ontološkog metamodela, ali i kao koristan pomoćni, vizualni alat, prilikom ostvarenja ontoloških programskih modela za različite primjene politika prema prikazanim studijama slučajeva u sedmom poglavlju. Pomoću programskog ostvarenja ontološkog metamodela i instanci modela za odabrane studije slučajeva u sedmom poglavlju, provjerava se valjanost konceptualnog metamodela, kao i svojstva jednostavnosti, dosljednosti, sveobuhvatnosti i učinkovitosti upravljanja životnim ciklusom politika informacijske sigurnosti uporabom ostvarenog konceptualnog metamodela.

# 7. OSTVARENJE PROGRAMSKOG ONTOLOŠKOG MODELA

Na slici 7.1 prikazana je metoda modeliranja koja se predlaže u okviru ovog rada, s istaknutim razinama modeliranja prikazanim u sedmom poglavlju. Temelj za ostvarenje programskog ontološkog metamodela je konceptualni metamodel ostvaren u UML-u i opisan u šestom poglavlju. Ostvarenje ontološkog metamodela koje se opisuje u ovom poglavlju, uvodi daljnju razinu detalja u metodu modeliranja te prema slici 7.1 predstavlja vrste politika i normi informacijske sigurnosti, kao primjenu skupa dominantnih politika i normi informacijske sigurnosti.




**Slika 7.1:** Metoda modeliranja s istaknutim razinama programskog ontološkog modeliranja

Na ovoj razini, prema slici 7.1, modeliranje se usmjerava na daljnju razradu detalja konceptualnog metamodela, s ciljem ostvarenja programskog rješenja za modeliranje tipičnih politika informacijske sigurnosti, primjenjivih u najširem segmentu primjene u državnom i

poslovnom sektoru te s naglaskom na modeliranje aspekata međusobne suradnje organizacijskih entiteta iz ova dva sektora. Na ovaj način provjerava se valjanost rezultata metode modeliranja i ostvarenja konceptualnog metamodela u UML-u te se pokazuje kako upravljanje životnim ciklusom politika informacijske sigurnosti, pristupom zasnovanim na predloženoj metodi modeliranja i ostvarenom konceptualnom metamodelu, postaje jednostavnije, dosljednije, sveobuhvatnije i učinkovitije.

U okviru konceptualnog metamodela zapisanog u UML-u, razrađeni su svi potrebni podsustavi i ključni koncepti, pri čemu je razina detalja u modelu prilagođena potrebi konceptualizacije, odnosno upravljanju i komuniciranju znanjem među stručnjacima različitih profila koji se bave područjem informacijske sigurnosti. Stoga je konceptualni UML metamodel primarno usmjeren na širu domensku razinu, na općenite domenske koncepte prikazane klasama UML-a, njihovo međusobno povezivanje, razradu osnovnih atributa, odnosno na specijalizaciju koncepata do razine potrebnih modelskih klasa i grupiranja atributa, ali bez prikaza krajnjih instanci klasa namijenjenih konfiguriranju za definirana ciljna okruženja provedbe politika informacijske sigurnosti. Kao što je naznačeno u šestom poglavlju, preveliki broj detalja u konceptualnom UML modelu otežao bi njegovu čitljivost i narušio jasnoću i preglednost te je daljnja razrada detalja u okviru predložene metode modeliranja, predviđena u programskom alatu prikladnijem za ovu razinu složenosti domenskog znanja, u programskom razvojnom okruženju *Protégé Frames* [99]. Pored toga, programsko okruženje nužno je prema slici 7.1, jer se uz pomoć programskog ontološkog metamodela želi ostvariti potrebne programske ontološke modele lokalnog okruženja, koji se konfiguriraju unosom podataka za stvarne provedbene politike informacijske sigurnosti u odabranim studijama slučajeva (najniža razina modeliranja na slici 7.1).

Prema slici 7.1, može se reći da je metoda modeliranja u početnim koracima usmjerena na strukturu metamodela i općenite vršne pojmove konceptualnog metamodela, koji se ostvarenjem u UML-u razrađuju do razine potrebnih detalja globalnog okruženja i skupa dominantnih politika i normi informacijske sigurnosti. Nakon ostvarenja konceptualnog metamodela u UML-u, metoda se usmjerava prema lokalnom okruženju za što su potrebne ciljane vrste politika informacijske sigurnosti, zatim daljnja razrada detalja i specijalizacija nekih klasa metamodela, kao što su taksonomije sigurnosnih incidenata u podsustavu PS9, taksonomije minimalnih sigurnosnih mjera u podsustavu PS15, ili taksonomije prijetnji i ranjivosti u podsustavu PS17 konceptualnog metamodela u UML-u. Upravo stoga koriste se

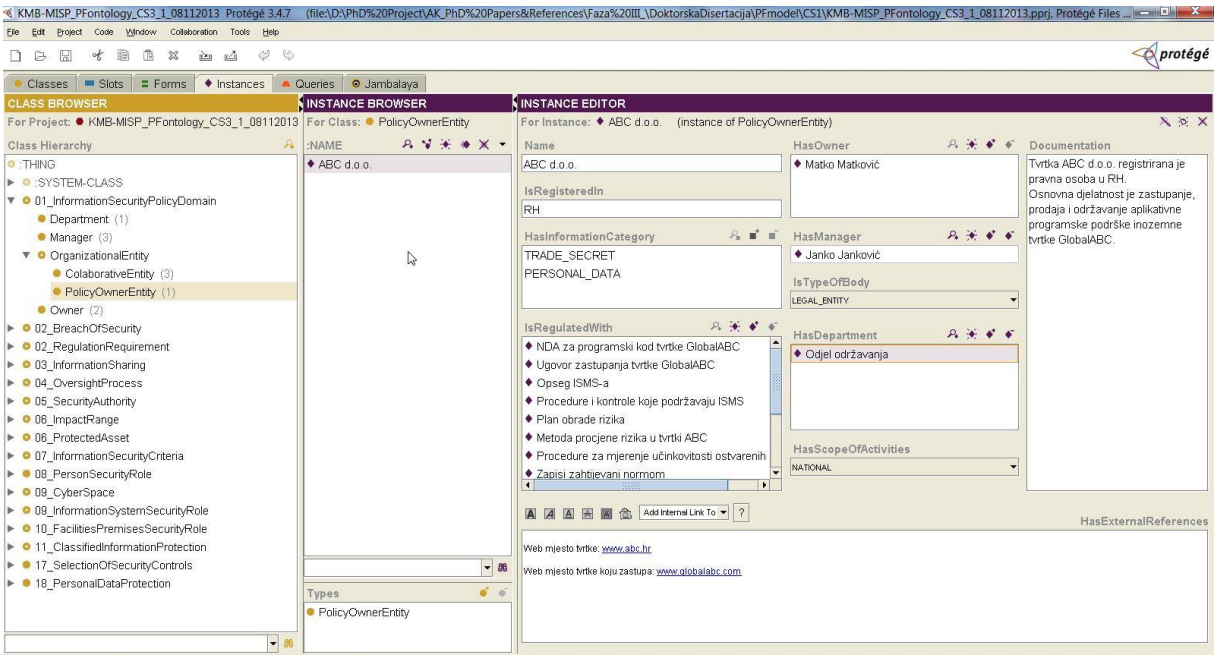
različiti alati koji imaju različite mogućnosti i služe različitim ciljevima u okviru iste metode modeliranja i iste ciljne domene interesa. Konceptualni metamodel u UML-u razrađen je do razine potrebne za konceptualizaciju ključnih koncepata općenitog metamodela zasnovanog na skupu dominantnih politika i normi informacijske sigurnosti i primarno je usmjeren na širu domensku problematiku. Tako razrađen model razinom detalja obuhvaća i osnovnu zadaću koja mu je namijenjena kao okviru za upravljanje i komuniciranje znanjem prema hipotezi H1 na slici 5.1. Na razini modeliranja koja je opisana u ovom poglavlju, ostvaruje se programski ontološki metamodel za koji su, pored postupka provjere valjanosti ostvarenog konceptualnog metamodela u UML-u, postavljeni širi ciljevi vezani za hipotezu H2 na slici 5.1. Ostvarenjem programskog ontološkog metamodela, razina detalja proširuje se i prilagođava ciljevima modeliranja na ovoj razini. Ciljevi modeliranja nemaju više ograničenje namjene u smislu jasnoće i vizualnih svojstava namijenjenih različitim profilima stručnjaka informacijske sigurnosti, već se modeliranje provodi programskim ostvarenjem, čitljivim i za ljude i za programske aplikacije, a vrste politika i normi informacijske sigurnosti sa slike 7.1 odgovaraju odabranim studijama slučajeva (poslovni i državni sektor u širem smislu).

## 7.1. Programsko razvojno okruženje Protégé Frames

Programsko razvojno okruženje *Protégé Frames* [99] koje se koristi u ostvarenju ontološkog metamodela politika informacijske sigurnosti, spada u sustave zasnovane na okvirima (engl. *Frame Based Systems*), a model znanja u *Protégé Frames* sukladan je OKBC protokolu (engl. *Open Knowledge Base Connectivity protocol* - *OKBC*), slika 2.3. Okviri pri tome predstavljaju osnovu za ostvarenje i klasa i atributa, pri čemu se atributima definiraju ne samo svojstva, već i relacije između klasa, što olakšava i ostvarenje specijalizacije, odnosno nasljeđivanja primjenjivog na klase, atribute i relacije između klasa. Programske ontologije razrađene u sustavu zasnovanom na okvirima obuhvaćaju skup klasa organiziran u domensku hijerarhiju koncepata, skup slotova povezanih s klasama u svrhu opisa njihovih svojstava i međusobnih relacija, kao i skup instanci klasa koje predstavljaju pojedinačnu primjenu općeg koncepta na kontekst okruženja i stoga imaju konkretne vrijednosti svojstava. Ovakav način predstavljanja znanja, odnosno konceptualizacije, zasnovan na strukturama znanja, vrlo je blizak načinu koncipiranja hijerarhije propisa prema slikama 4.1 i 4.4, odnosno načinu razrade sigurnosnih zahtjeva i pravila, te je stoga pogodan za modeliranje ovog područja politika i normi informacijske sigurnosti.

Programsko razvojno okruženje *Protégé Frames* (slika 7.2) koristi se u ovom istraživanju na više načina, kao:

- okruženje za razvoj programskog ontološkog metamodela na temelju konceptualnog modela u UML-u;
- baza operativnog znanja, odnosno znanja povezanog s vrstama politika i normi informacijske sigurnosti sa slike 7.1, kao što su primjerice predviđene taksonomije sigurnosnih incidenata u PS9 [13], taksonomije minimalnih sigurnosnih mjera u PS15 [85], ili taksonomije prijetnji i ranjivosti u PS17 [27, 91];
- alat za prikupljanje znanja za potrebe unosa podataka u okviru ostvarenja studija slučajeva (programski ontološki modeli), odnosno za definiranje politika informacijske sigurnosti zamišljenih organizacijskih okruženja te za praćenje znanja o provedbi politike informacijske sigurnosti u nekom okruženju tijekom faza životnog ciklusa politike informacijske sigurnosti.




**Slika 7.2:** Prikaz ekrana s ostvarenim programskim ontološkim modelom zamišljene studije slučaja tvrtke ABC d.o.o.

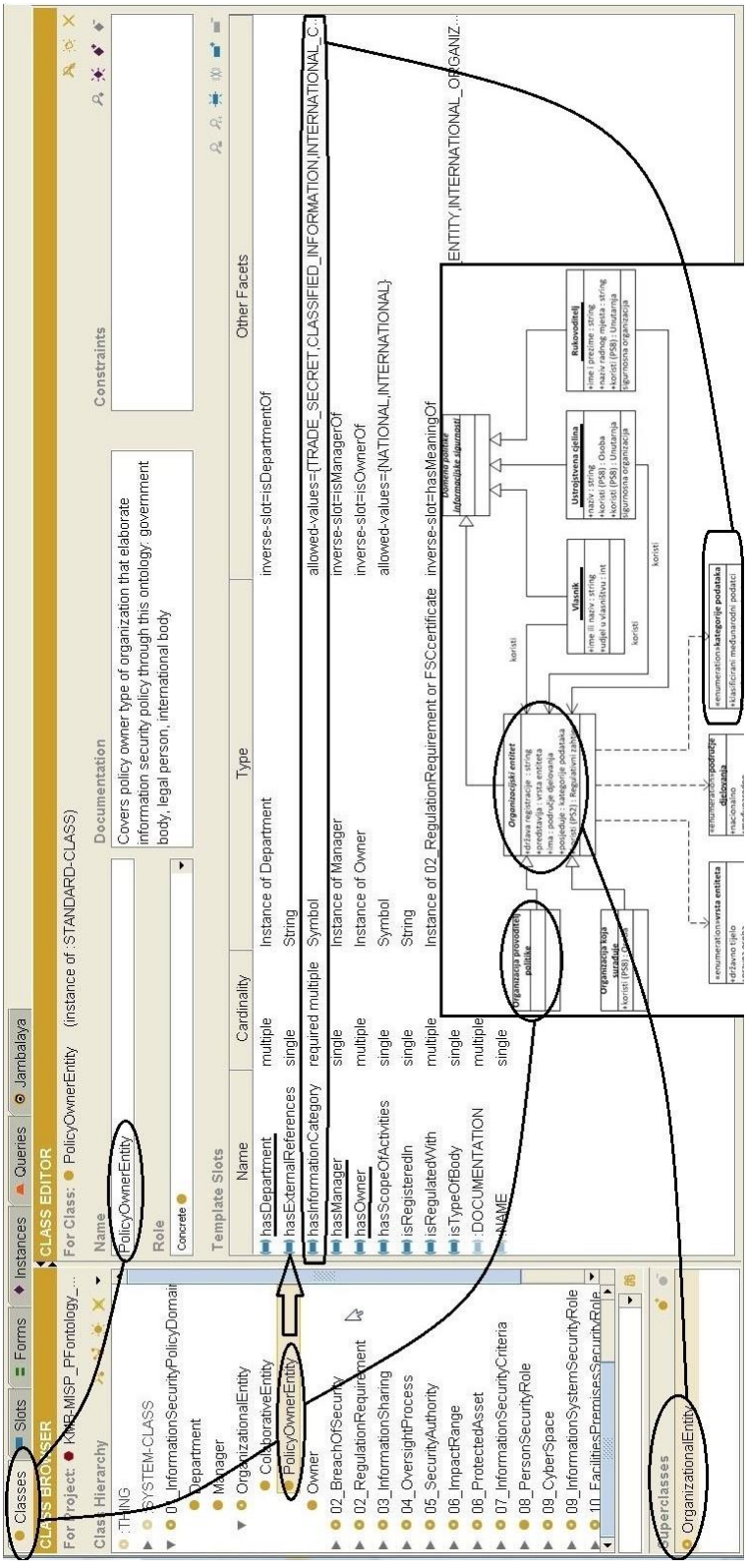
Na slici 7.2, s lijeve strane ekrana vidljiv je prozor s domenskom hijerarhijom klasa, ostvarenom na temelju konceptualnog metamodela u UML-u opisanom u poglavlju 7. U drugom prozoru s lijeve strane prikazane su ostvarene instance klasa iz prvog podsustava koji je odabran u krajnjem lijevom prozoru. U najvećem desnom prozoru vidi se sadržaj instance odabrane zamišljene tvrtke (*ABC d.o.o.*) dobivene na temelju klase organizacije provoditelja

politike informacijske sigurnosti (*PolicyOwnerEntity*), s unesenim podatcima i relacijama za ovaj primjer unutar modela. Kao što je vidljivo, koristi se više tipova podataka koji mogu biti različiti numerički tipovi, polja za slobodni unos, izbor modelom definiranih vrijednosti atributa, odnosno veze prema drugim instancama (mali romb ispred naziva označava instancu druge klase u modelu s kojom je klasa povezana). Opće domenske klase definirane konceptualnim metamodelom UML-a, ostvarene su okvirima (engl. *Frames*) u programskom ontološkom metamodelu razvojnog okruženja *Protégé Frames*, korištenjem engleskih naziva (lijevi prozor ekrana na slici 7.2), dok su ontološki modeli s krajnjim instancama za lokalna okruženja, razrađeni u odabranim studijama slučajeva u ovom radu, prikazani korištenjem hrvatskih naziva i u dijelu imenovanja instanci klasa i u dijelu tekstualnih komentara i opisa.

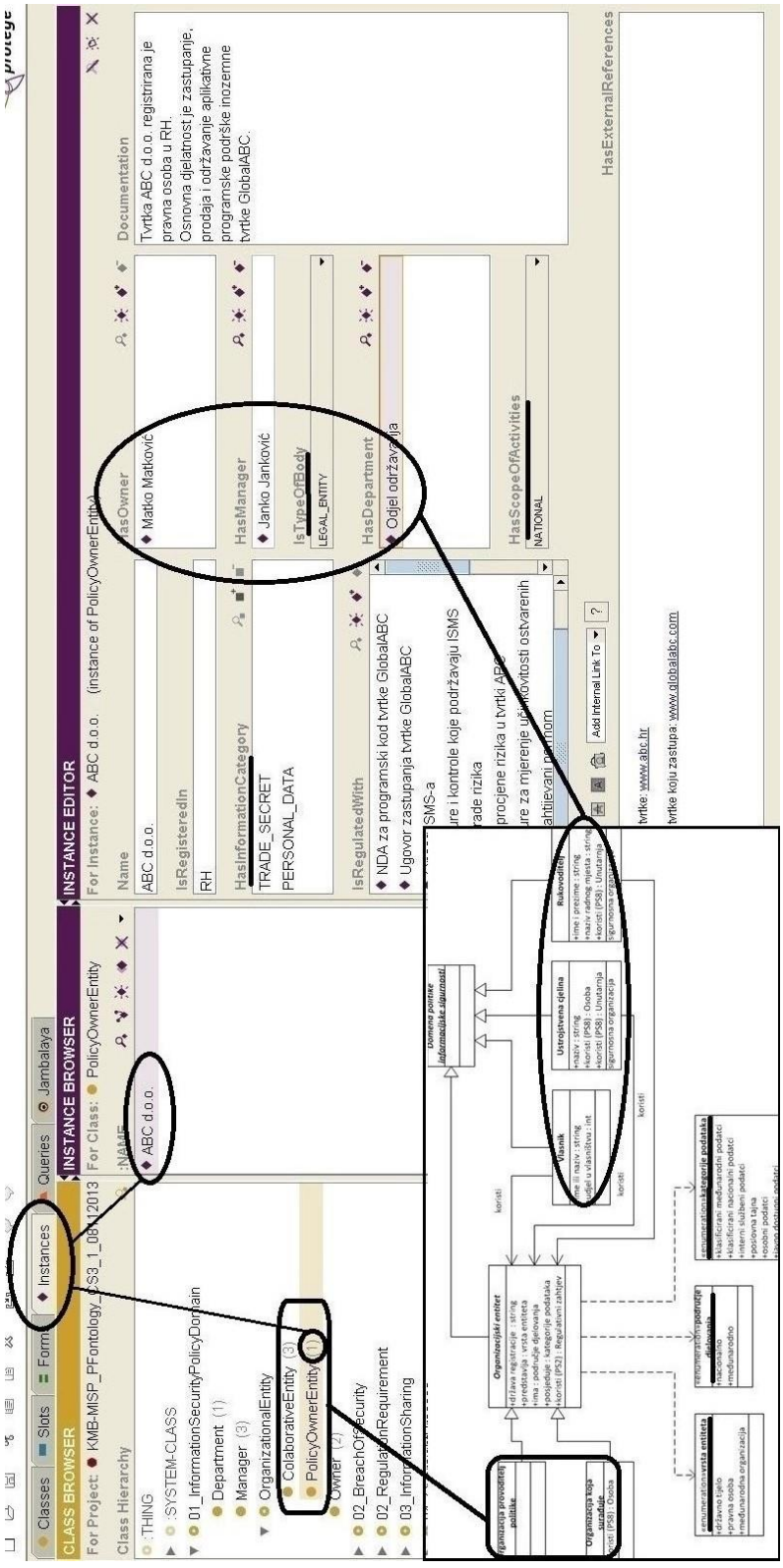
## 7.2. Programsko ostvarenje ontološkog metamodela

Programsko ostvarenje ontološkog metamodela zasnovano je na prethodno ostvarenom konceptualnom UML metamodelu. Na slici 7.3 prikazan je primjer podsustava domene informacijske sigurnosti (PS1) u obliku UML dijagrama klasa konceptualnog metamodela i u obliku programskog ontološkog metamodela ostvarenog u *Protégé Frames*. Pojedini elementi UML prikaza zaokruženi su i povezani s odgovarajućim elementima programskog ostvarenja u *Protégé Frames*. U *Protégé Frames* prikazan je izgled prozora s odabranim podsustavom PS1 te klasom *PolicyOwnerEntity*, odabranom iz hijerarhije ostvarenih klasa u lijevom prozoru. Odabrana klasa sastoji se od niza slotova vidljivih u desnom prozoru, kojima se ostvaruju potrebni atributi UML klasa, što je prikazano na slici 7.3 povezivanjem odgovarajućih elemenata UML prikaza s elementima programskog ostvarenja.

Programski ontološki metamodel prema slici 7.1, predstavlja temelj za ostvarenje programskih ontoloških modela i studija slučajeva, zamišljenih u radu za potrebe provjere rezultata modeliranja. Na slici 7.4 prikazan je način ostvarenja instanci klasa na primjeru prethodno razmatrane klase *PolicyOwnerEntity*, sa slike 7.3. I ovdje je radi jasnoće prikazan i UML dijagram klasa podsustava PS1 konceptualnog metamodela te su istovrsni elementi UML konceptualnog metamodela povezani s elementima programskog ontološkog metamodela (lijevi prozor) te s elementima ontološkog modela studije slučaja, za odabranu instancu klase *PolicyOwnerEntity*, instancu ABC d.o.o. i slotove ove instance s konfiguriranim podatcima ciljanog okruženja za provedbu politike informacijske sigurnosti.

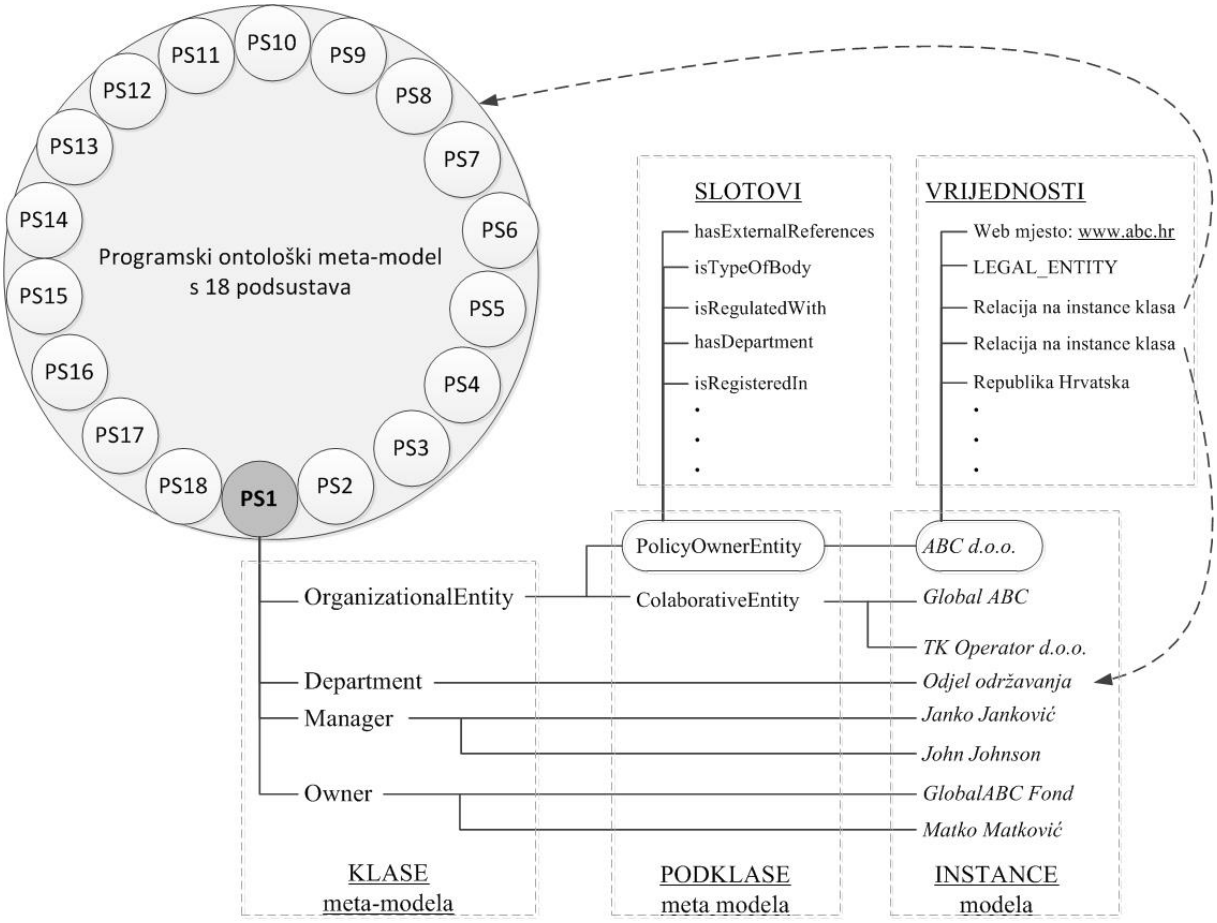



**Slika 7.3:** Ostvarenje programskog ontološkog metamodela na temelju konceptualnog UML metamodela (primjer podsustava domene politike informacijske sigurnosti, PS1)



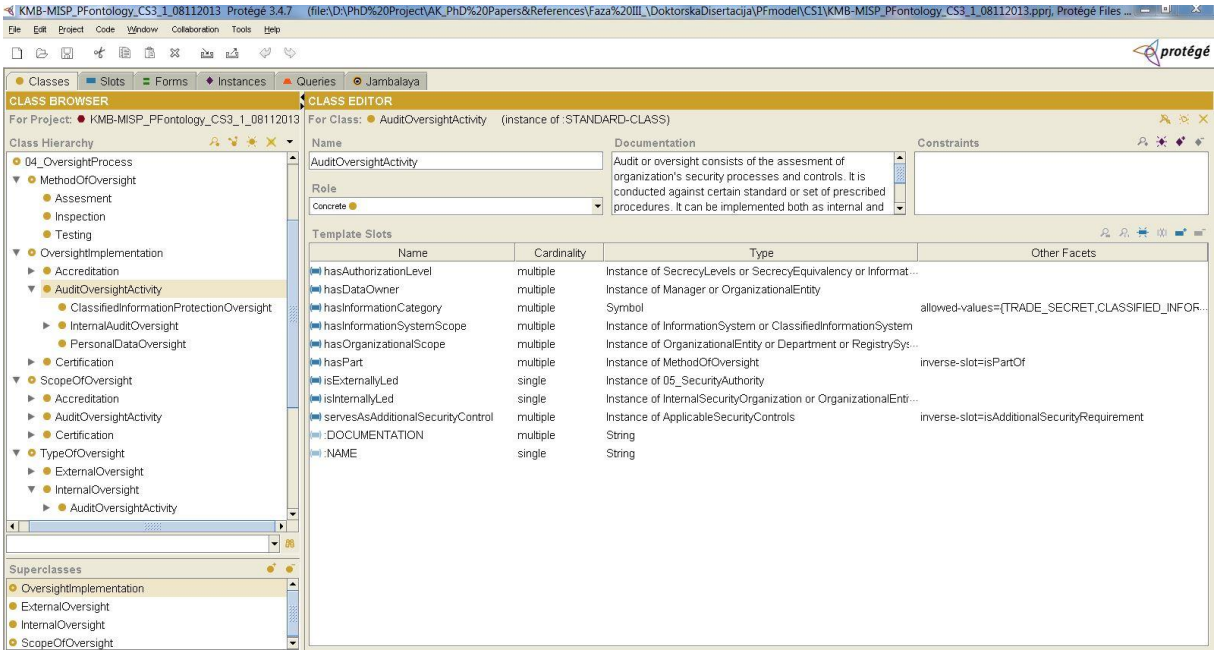
**Slika 7.4:** Ostvarenje programskog ontološkog modela studije slučaja zamišljene tvrtke na temelju programskog ontološkog metamodela, odnosno konceptualnog UML metamodela (primjer podsustava domene politike informacijske sigurnosti, PS1)

Programski ontološki metamodel koji se sastoji od 18 podsustava i korišteni programski elementi, prikazani su simbolički na slici 7.5. Slika prikazuje odabrani podsustav domene politike informacijske sigurnosti (PS1) te ostvarene klase i podklase podsustava PS1. Odabrana je klasa *PolicyOwnerEntity* za koju su prikazani ostvareni slotovi. Također je prikazana instanca klase *PolicyOwnerEntity*, instanca *ABC d.o.o.* te su prikazane vrijednosti slotova klase *PolicyOwnerEntity* za instancu *ABC d.o.o.* te relacije slotova ove instance sa instancama drugih klasa modela.




**Slika 7.5:** Programski ontološki metamodel i korišteni programski elementi

Principijelni prikaz programskog ostvarenja ontološkog metamodela u *Protégé Frames*, nastavlja se na primjeru PS4, nadzor informacijske sigurnosti, prethodno prikazanog na slici 2.2, u obliku hijerarhijske domenske taksonomije, a zatim na slici 6.7, u obliku ostvarenog konceptualnog metamodela u UML-u. Na slici 7.6, ovaj isti podsustav prikazan je u obliku ostvarenog programskog ontološkog metamodela u *Protégé Frames*.

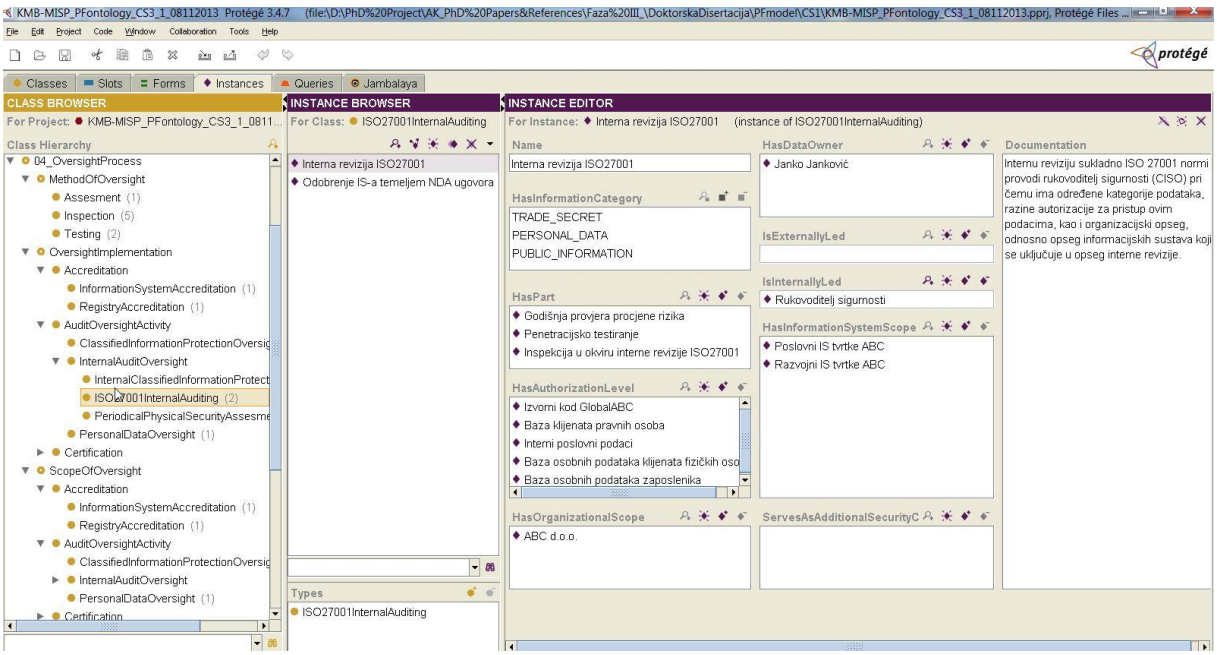



**Slika 7.6:** Prikaz ekrana s ostvarenim programskim ontološkim metamodelom za podsustav nadzora informacijske sigurnosti (UML klasa *Nadzor/revizija*)

Na slici 7.6 prikazan je ekran razvoja klasa u *Protégé Frames*, s otvorenim segmentom ostvarene domenske hijerarhije klasa, u dijelu programskog ontološkog metamodela koji pripada podsustavu nadzora informacijske sigurnosti (PS4), sa slike 6.7. Prozor ekrana na lijevoj strani prikazuje hijerarhiju klasa ovog podsustava, a u njegovom donjem dijelu vide se nadklase izabrane klase *AuditOversightActivity*. U većem prozoru s desne strane slike ekrana, u gornjem dijelu prozora, vidljivi su osnovni podatci o klasi (naziv, vrsta, opis), a u donjem dijelu prozora prikazan je sadržaj slotova ove klase, koji predstavljaju atribute i relacije klase. Slotovi se prenose hijerarhijskim nasljeđivanjem od klasa u višim dijelovima hijerarhije (npr. slot *hasInformationCategory*), ili višestrukim nasljeđivanjem, koje može uključiti i druge odabrane klase modela. Odabirom drugih klasa ostvaruje se prikazana relacija ograničenja sa slike 6.6, koja tako prenosi željeni slot, npr. *isExternallyLed*, naslijeđen od klase *ExternalOversight*. Korištenje pojedinih metoda, ostvarenih kao krajnje instance klase *MethodOfOversight*, odnosno njenih podklasa *Assesment*, *Inspection* i *Testing*, ostvareno je slotom *hasPart*, koji sadrži relacije prema instancama klase *MethodOfOversight*. Radi olakšavanja unosa podataka, većina ovakvih relacija, ostvarena je korištenjem inverznih slotova. Inverzni slotovi, kao npr. *hasPart* klase *AuditOversightActivity* i *isPartOf* klase *MethodOfOversight*, omogućavaju unos i konfiguriranje slota jedne klase, dok se slot druge klase programski sadržajno usklađuje s odabranim unosom inverznog slota. Nasljeđivanje se može koristiti i u odnosu na ostvarene krajnje instance jedne klase modela kojima se može

dodavati dodatna nadklasa iz neke druge hijerarhije klasa modela. Ovim načinom modelira se primjerice podsustav organizacijskog okvira (PS5), prema slici 6.8, zbog potrebe pridjeljivanja različitih, klasama definiranih hijerarhijskih organizacijskih funkcionalnosti različitim državnim tijelima.

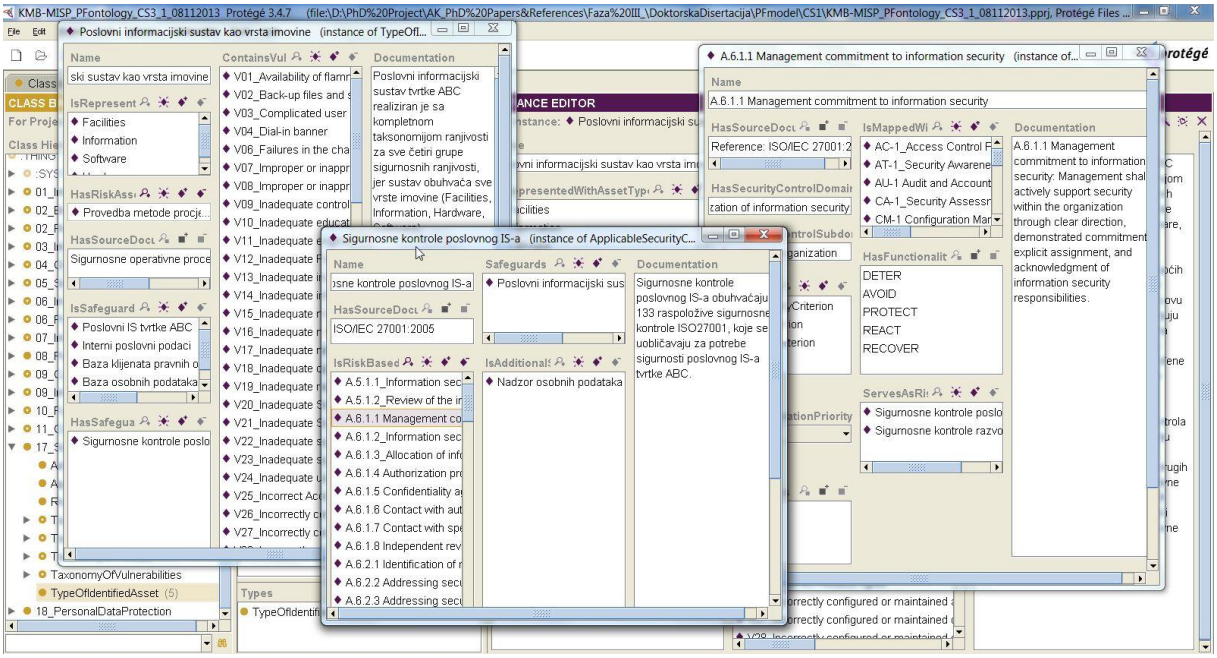
Programsko ostvarenje ontološkog metamodela zasnovano je na domenskoj hijerarhiji klasa te se elementi konceptualnog metamodela u UML-u, kao što su združivanja i sastavljanja klasa (tablica 6.1), ostvaruju prethodno opisanim mogućnostima nasljeđivanja i koriste jednostavnim grupiranjem atributa i relacija. U konceptualnom metamodelu politika informacijske sigurnosti, uloga ovih elemenata UML-a je jasniji i slikovitiji prikaz atributa klasa, neovisno radi li se o sastavljanju koncepata koji postoje neovisno o ovom modelu, ili združivanju koncepata koji su interni dio modela. Ova razlika je korištena u konceptualnom metamodelu prvenstveno radi jasnoće i vizualizacije šireg domenskog prikaza. Za programsko ostvarenje ontološkog metamodela ova razlika nije važna, već je cilj grupiranje atributa i ostvarivanje odgovarajućih relacija između klasa, kao i omogućavanje potrebnog unosa podataka u tako grupirane atribute i relacije klasa, s ciljem opisivanja politike informacijske sigurnosti ciljanog okruženja. Ovo je na slici 7.7 prikazano za isti podsustav nadzora informacijske sigurnosti, na temelju UML klase *ISO 27001 interna revizija* sa slike 6.7, koja je ostvarena klasom *ISO27001InternalAuditing* prikazanom na slici 7.7.




**Slika 7.7:** Prikaz ekrana s ostvarenim programskim ontološkim metamodelom za podsustav nadzora informacijske sigurnosti i UML klasu ISO 27001 interna revizija sa slike 6.6

Klasa *ISO27001InternalAuditing*, prikazana na slici 7.7 u lijevom prozoru ekrana, ima instancu *Interna revizija ISO27001*, prikazanu u srednjem prozoru, a u desnom prozoru vidljiv je sadržaj ove instance klase za ciljano okruženje provedbe politike informacijske sigurnosti, odabrano u studiji slučaja s unesenim i konfiguriranim podatcima i relacijama za ovaj primjer stvarnog okruženja provedbe.

Programski ontološki metamodel, prema slici 7.1, predstavlja vrste politika informacijske sigurnosti koje primjenjujemo u okruženjima odabranih studija slučajeva. Modeliranje stvarnih politika informacijske sigurnosti, osim pokazanih općih koncepata, njihove specijalizacije i međusobnog povezivanja te definiranja atributa, traži i dodatne taksonomije, odnosno potrebne baze operativnog znanja, kao što su taksonomija sigurnosnih incidenata u PS9, taksonomije minimalnih sigurnosnih mjera u PS15, ili taksonomije prijetnji i ranjivosti u PS17. U PS9 stoga je unesena taksonomija sigurnosnih incidenata prema [13], u PS15 taksonomije minimalnih sigurnosnih mjera prema [85], a u PS17 taksonomije prijetnji i ranjivosti prema [91] i taksonomija sigurnosnih kontrola prema [27].




**Slika 7.8:** Prikaz ekrana s PS17 i otvorenim prozorima sa detaljnijim prikazom vrste imovine, pripadnih sigurnosnih kontrola te odabirom sigurnosne kontrole A.6.1.1. iz ISO 27001 taksonomije sigurnosnih kontrola

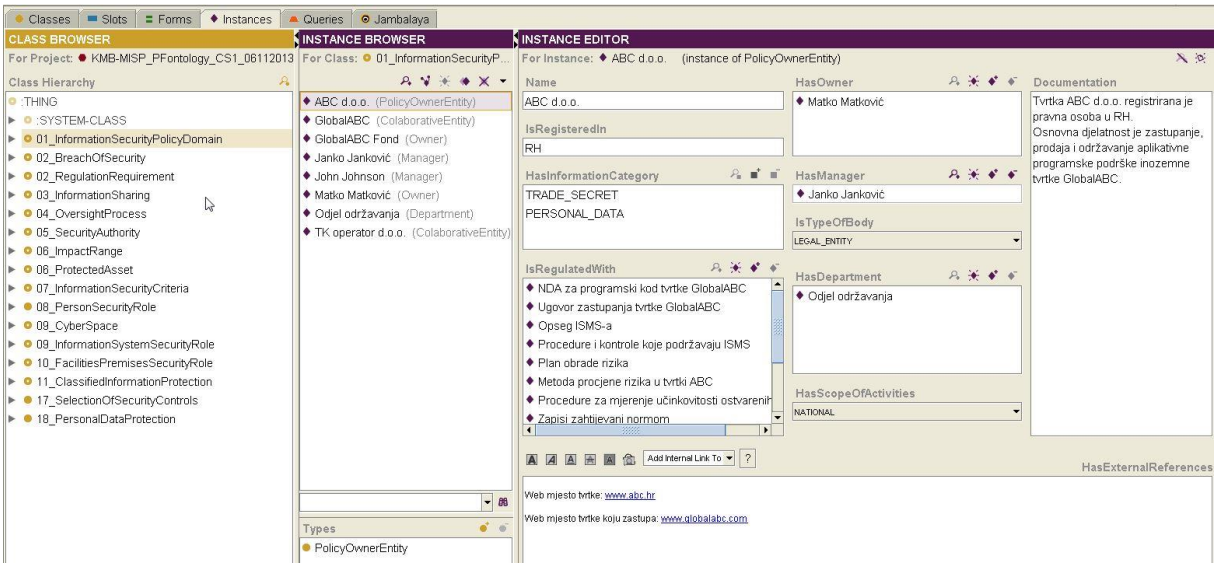
Prema slici 7.8, vidljiva je baza operativnog znanja koja predstavlja sigurnosne kontrole iz norme ISO 27001 [27] te je korištenjem inverznog slota *isMappedWith*, povezana s PS15 i

taksonomijom minimalnih sigurnosnih mjera prema [85]. Programski ontološki model omogućava logički povezan pristup ovim taksonomijama, preko vrste identificirane imovine, uz pomoć koje se koriste povezane ranjivosti, odnosno prijetnje iz taksonomija te se oblikuju sukladno procjeni rizika i prema potrebi lokalnog okruženja.

Za potrebe ostvarenja ovog programskog ontološkog metamodela u *Protégé Frames* programskom okruženju, korištene su smjernice i preporuke iz [18, 99].

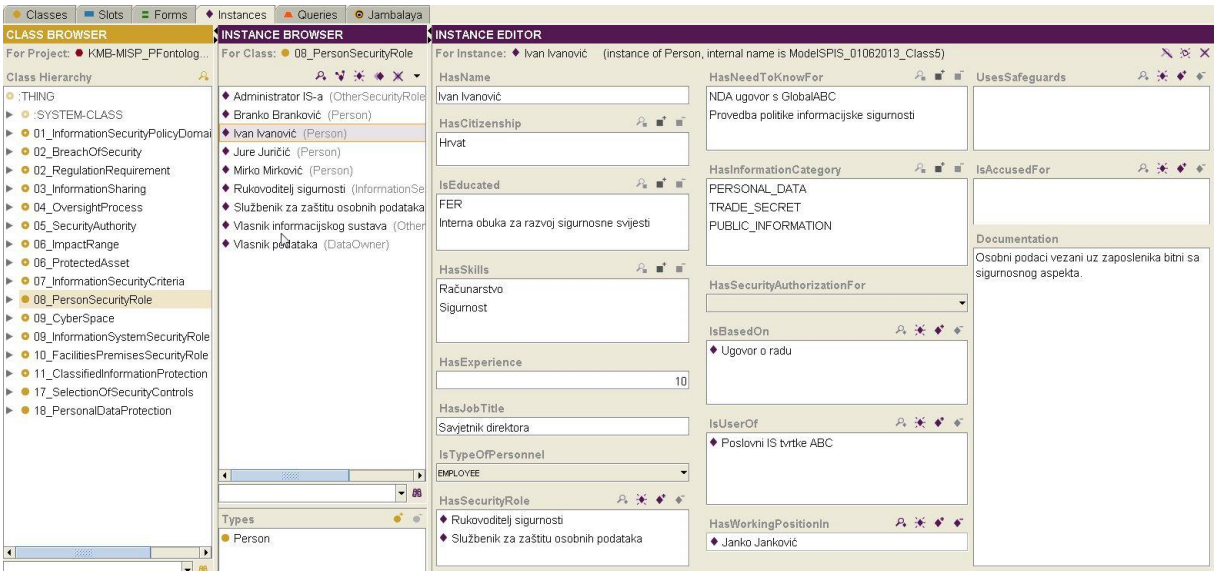
## 7.3. Studija slučaja 1 – modeliranje politike informacijske sigurnosti pravne osobe

Studija slučaja modeliranja politike informacijske sigurnosti pravne osobe, zasnovana je na zamišljenom slučaju tvrtke ABC d.o.o. Politika informacijske sigurnosti utvrđuje potrebe sigurnosti i sigurnosne ciljeve koje je definirala uprava tvrtke ABC, u svrhu podrške poslovnoj viziji, misiji i ciljevima. Politika informacijske sigurnosti provodi se korištenjem norme ISO/IEC 27001 u obliku interne revizije, za što je zadužen rukovoditelj sigurnosti. Svrha sigurnosti je zaštita imovine tvrtke koja je značajna za uspješno poslovanje tvrtke, zaštita imovine tvrtke GlobalABC, za čiju aplikativnu programsku podršku je tvrtka ABC lokalni zastupnik te zaštita povezane imovine i podataka korisnika.




**Slika 7.9:** Prikaz ekrana s ontološkim modelom politike informacijske sigurnosti zamišljene tvrtke ABC d.o.o., koji prikazuje instance klasa iz prvog podsustava definicije domene i instancu klase organizacije provoditelja politike informacijske sigurnosti

Na slici 7.9 prikazani su svi modelirani podsustavi programskog ontološkog metamodela (prozor s lijeve strane ekrana), sve modelirane instance klasa iz prvog podsustava definicije domene (drugi prozor s lijeve strane ekrana) te atributi i relacije instance klase organizacije provoditelja politike informacijske sigurnosti, same tvrtke ABC d.o.o. U donjem dijelu desnog prozora ekrana vidljiva je i mogućnost poveznica s vanjskim ili unutarnjim Web mjestima tvrtke, što se koristi za pristup javnim podatcima o pravnim i fizičkim osobama, odnosno kao mogućnost stvaranja poveznica s datotekama koje sadrže dokumente propisane odgovarajućom normom ili politikom informacijske sigurnosti s kojom se usklađuje provedba politike informacijske sigurnosti. Popis regulativnih propisa i drugih zahtjeva, kao i potrebnih dokumenata politike informacijske sigurnosti modeliran je i vidljiv u slotu *isRegulatedWith* na slici 7.9. Svaki od ovih elemenata je relacija prema instanci klase odgovarajućeg podsustava modela. Na slici 7.9 također se vide i ključne osobe i organizacijske jedinice koje su modelirane. Detaljnije modeliranje osoba i sigurnosnih uloga provedeno je u podsustavu definicija osoba (PS8) i prikazano je na slici 7.10.

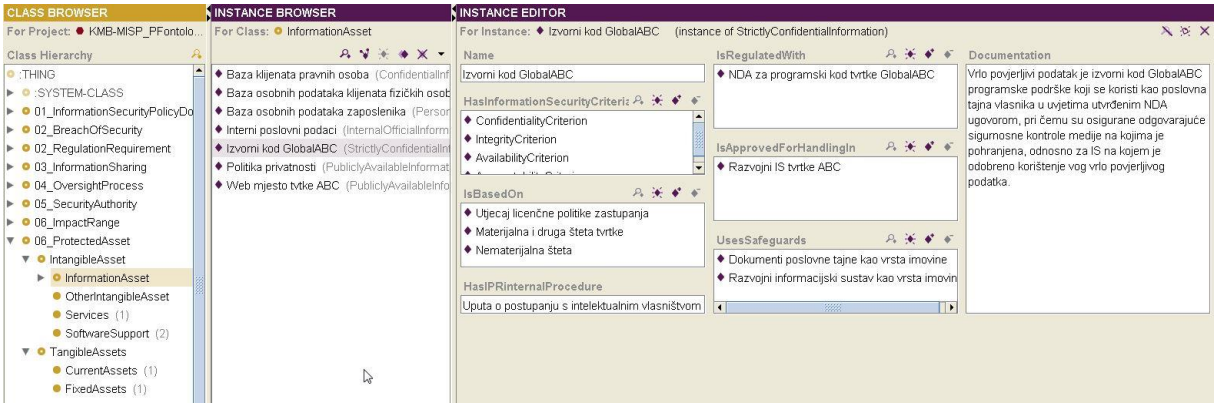



**Slika 7.10:** Prikaz ekrana s instancama klasa iz podsustava definicije osoba (PS8), kao i podatcima instance osobe kojoj je pridijeljena uloga rukovoditelja sigurnosti

Prema slici 7.10 prikazan je ekran sa svim instancama klasa iz podsustava definicija osoba. Odabrana klasa prikazuje osobu kojoj su dodijeljene uloge rukovoditelja sigurnosti i službenika za zaštitu osobnih podataka, a koja je odgovorna osobi za koju se na prethodnoj slici vidi da obnaša dužnost direktora tvrtke. Uloge kao što je rukovoditelj sigurnosti,

povezane su relacijama prema instanci klase kojom su modelirane odgovornosti ovih uloga (npr. nadzor ili informacijski sustavi i sl.).

Informacijska imovina tvrtke modelirana je u skladu s poslovnim ciljevima i regulativnim sigurnosnim zahtjevima i prikazana je na slici 7.11. Modelirane su različite kategorije podataka, koje, poput na slici odabrane instance, imaju svojstvo povjerljivosti, ali i kategorije poput Web mjesta tvrtke ABC, koje imaju svojstvo cjelovitosti. Svaka kategorija imovine povezana je slotovima s instancama potrebnih klasa u drugim podsustavima.

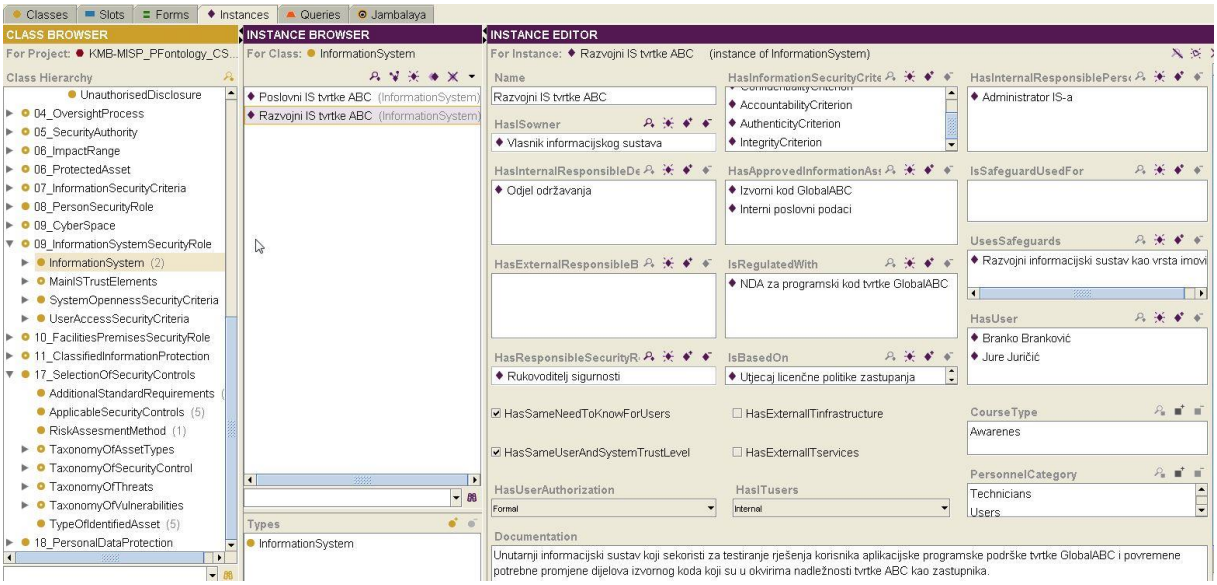



**Slika 7.11:** Prikaz ekrana s instancama klasa iz podsustava definicija podataka i drugih vrijednosti (PS6), kao i podatcima odabrane instance *Izvorni kod GlobalABC*, koja pripada klasi *StrictlyConfidential* (poslovna tajna)

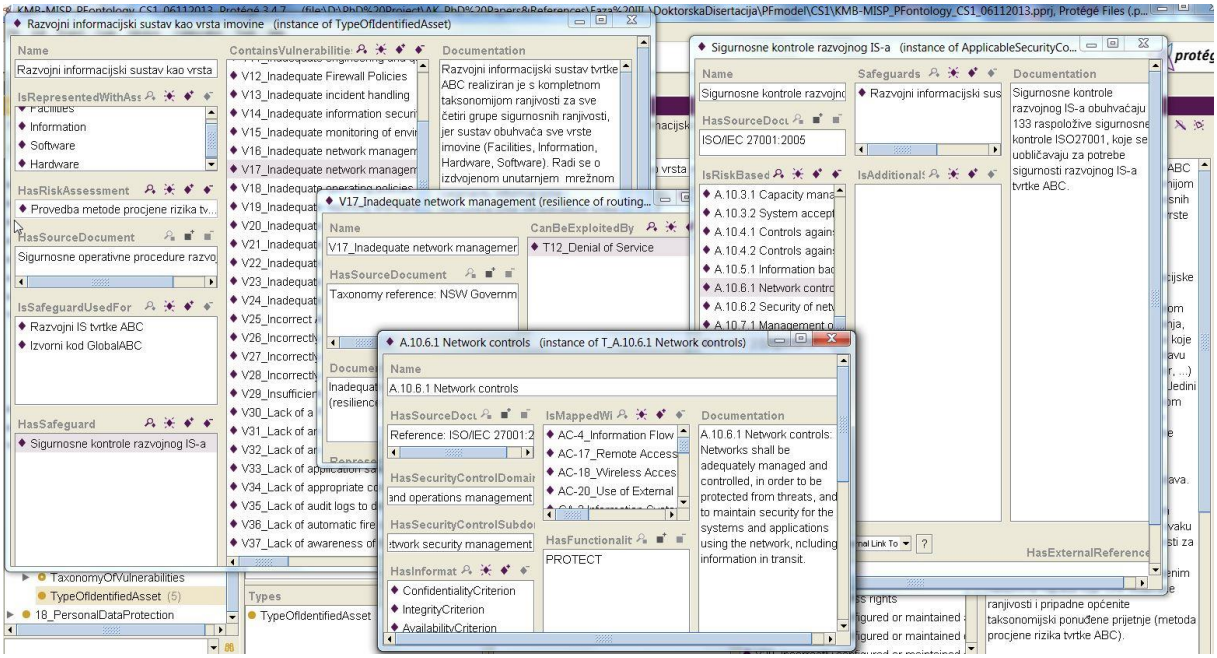
Primjerice, na slici 7.11, izvorni tekst programa kao podatkovna vrijednost, povezan je s kriterijima informacijske sigurnosti iz PS7 (slot *hasInformationSecurityCriteria*), dosegom utjecaja povreda sigurnosti iz PS6 (slot *isBasedOn*), regulativnim zahtjevima iz PS2 (slot *isRegulatedWith*), ili korištenjem sigurnosnih mjera iz podsustava 17 (slot *usesSafeguards*).

Nadalje, na slici 7.12 prikazane su instance klasa dva informacijska sustava tvrtke ABC, od kojih se poslovni informacijski sustav koristi za opće poslovne namjene i kategorije informacijske imovine, dok se razvojni informacijski sustav koristi za segment poslovanja povezan s podatcima zaštićenim kao poslovna tajna (*Izvorni kod GlobalABC* sa slike 7.8). Na slici je prikazana instanca klase za razvojni informacijski sustav, gdje se vidi povezanost čitavog niza instanci različitih klasa kojima su konceptualizirani pojmovi povezani s informacijskim sustavom (vlasnik, odgovorna ustrojstvena cjelina, rukovoditelj sigurnosti, informacijske kategorije odobrene za korištenje na IS-u, regulativni zahtjevi, administrator IS-a, korisnici IS-a te uvjeti povjerenja). Pored toga vidljive su i sigurnosne mjere koje su slotom

*usesSafeguards* povezane s PS17 i instancom klase *Razvojni informacijski sustav kao vrsta imovine*.

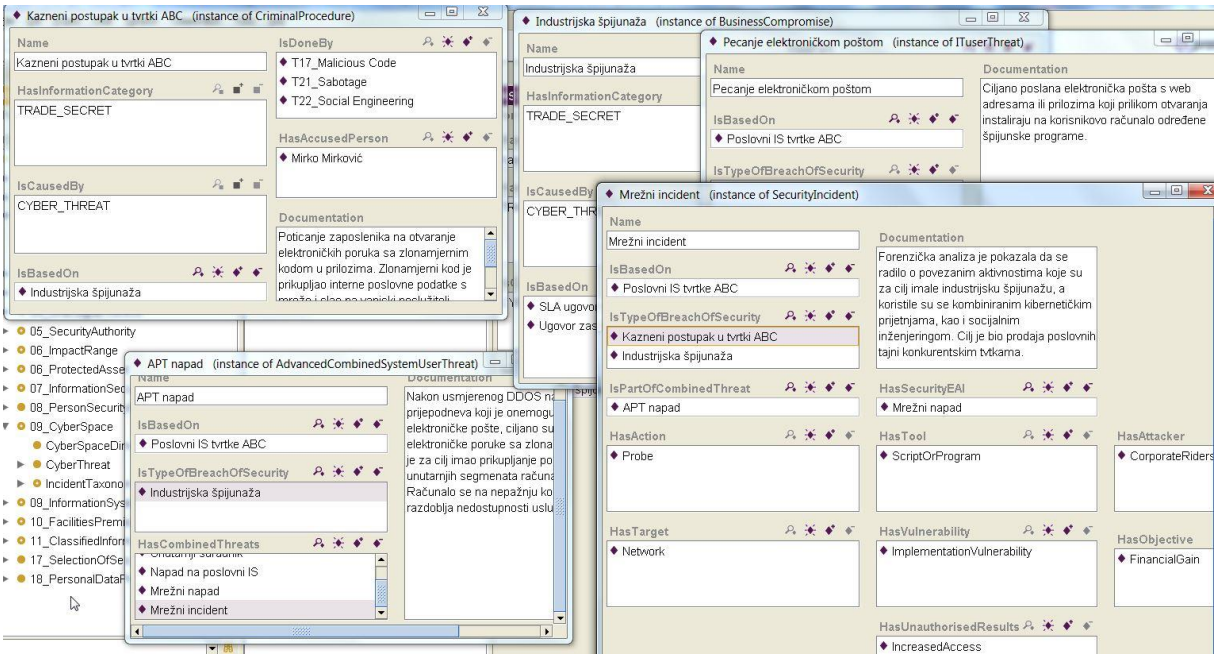



**Slika 7.12:** Prikaz ekrana s instancama klasa iz podsustava definicija informacijskih sustava (PS9), kao i podatcima odabrane instance *Razvojni IS tvrtke*




**Slika 7.13:** Prikaz ekrana s instancama klase *TypeOfIdentifiedAsset* iz PS17 i odabranom instancom *Razvojni informacijski sustav kao vrsta imovine* te otvorenom instancom jedne ranjivosti iz taksonomije (*V17*) i prozorom sa instancom klase *Sigurnosne kontrole razvojnog IS-a* i otvorenom instancom jedne od kontrola (*A.10.6.1*)

Instanca klase *Razvojni IS kao vrsta imovine* iz PS17, prikazana je detaljnije na slici 7.13, gdje se korištenjem taksonomija ranjivosti i prijetnji, ugrađenih u ontološki metamodel, procjenjuje rizik pojedinih vektora napada, na temelju kojeg se odabire, odnosno konfigurira odgovarajuća sigurnosna kontrola i ostvaruje skup kontrola primjenjiv za razvojni informacijski sustav. Nakon ostvarenja modela politike informacijske sigurnosti kao što je prikazano u ovoj studiji slučaja, sve kasnije dorade i proširenja provode se u okvirima programskog ontološkog modela ostvarenog preko instanci klasa iz programskog ontološkog metamodela, koristeći mogućnosti kopiranja pojedinih podataka, kao i samih instanci klasa, za modeliranje nove kategorije podataka i sl. Tijekom faze provođenja politike informacijske sigurnosti, na slici 7.14 prikazan je način praćenja i povezivanja aktivnosti u slučaju povreda sigurnosti iz PS2.




**Slika 7.14:** Prikaz ekrana s instancama klasa koje pokazuju način praćenja i povezivanja aktivnosti u slučaju povreda sigurnosti iz PS2 s međusobno povezanim klasama po različitim slojevima modela

Na slici 7.14 u gornjem lijevom kutu otvoren je prozor s instancom *Kazneni postupak u tvrtki ABC*, koji se temelji na instanci *Industrijska špijunaža* (doseg utjecaja iz PS6) u prozoru u gornjem desnom kutu slike 7.14. Instanca *Industrijska špijunaža* kao vektor napada prepoznaje instancu *Pecanje elektroničkom poštom* ostvarenu preko instance *Poslovni IS tvrtke ABC*. Istragom se ustanovilo da je instanca *Pecanje elektroničkom poštom*, dio složenijeg APT napada s instancom prikazanom u donjem lijevom kutu slike 7.14. Sve

pokazane instance klasa u konačnici su prikazane uz pomoć taksonomije sigurnosnih incidenata u PS9, na strukturiran način preko povezujuće instance *Mrežni incident*.

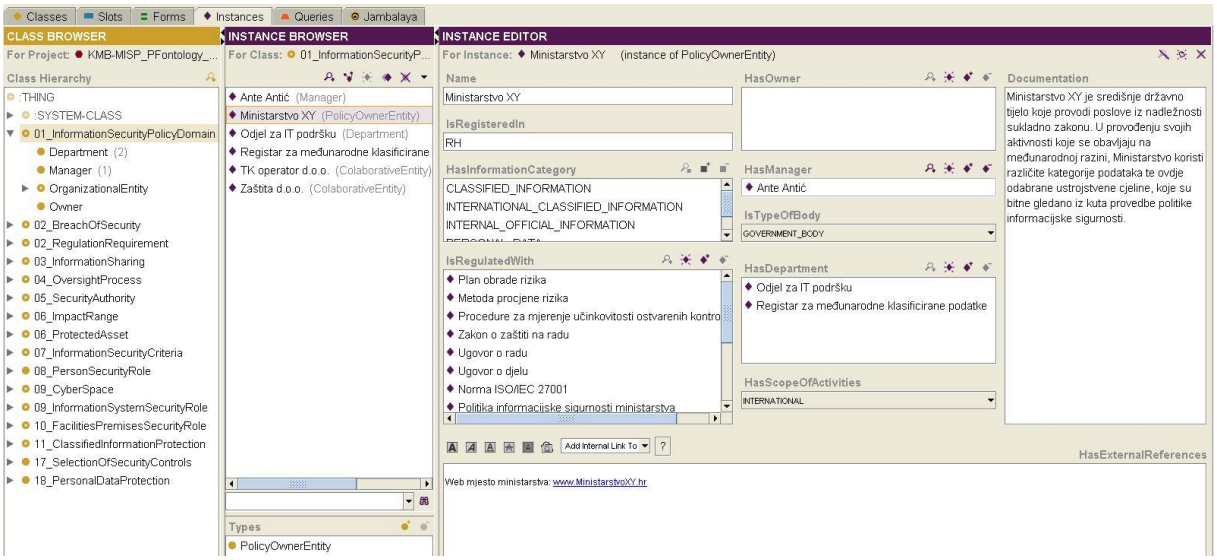
Cilj studije slučaja je opisati mogućnosti modeliranja politike informacijske sigurnosti pravne osobe, pri čemu se na odabranim primjerima pokazuju mogućnosti modeliranja životnog ciklusa politika informacijske sigurnosti u segmentu:

- planiranja, uz pomoć stvaranja instanci gotovih klasa ontološkog metamodela, unosa podataka, konfiguriranja i povezivanja instanci, sukladno zahtjevima ciljnog okruženja;
- ostvarenja, uz pomoć korištenja uspostavljenih i povezanih mjera i kontrola modela te njihovog opisivanja ili kopiranja u tražene popise i formate dokumenata, sukladno zadanim normama ili propisima, nakon čega se takvi dokumenti povezuju s pripadnim instancama modela u svrhu daljnjeg centraliziranog pristupa i održavanja;
- provođenja, uz pomoć stvaranja instanci za nove osobe, imovinu, ili povrede sigurnosti, na temelju klasa ontološkog metamodela ili kopiranjem istovrsnih instanci, te po potrebi ažuriranjem povezanih dokumenata norme ili propisa;
- preispitivanja, uz pomoć praćenja modelirane politike informacijske sigurnosti kroz međupovezane podsustave, klase i instance modela, uspoređujući ostvarene instance s ažuriranom procjenom rizika ili drugim poslovnim zahtjevima.

## 7.4. Studija slučaja 2 – modeliranje politike informacijske sigurnosti državnog tijela

Studija slučaja modeliranja politike informacijske sigurnosti državnog tijela zasnovana je na zamišljenom slučaju Ministarstva XY. Politika informacijske sigurnosti utvrđuje potrebe sigurnosti i sigurnosne ciljeve koji proizlaze iz provedbe zakonskih obaveza zaštite klasificiranih i drugih podataka u vlasništvu i nadležnosti Ministarstva XY, odnosno iz potrebe provedbe aktivnosti i poslovnih procesa Ministarstva XY, u kojima je potrebno koristiti zaštićene vrste podataka. Politika informacijske sigurnosti provodi se korištenjem mjera informacijske sigurnosti u okviru pet područja informacijske sigurnosti (sigurnost osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost poslovne suradnje), propisanih odgovarajućim zakonima i podzakonskim aktima. U području

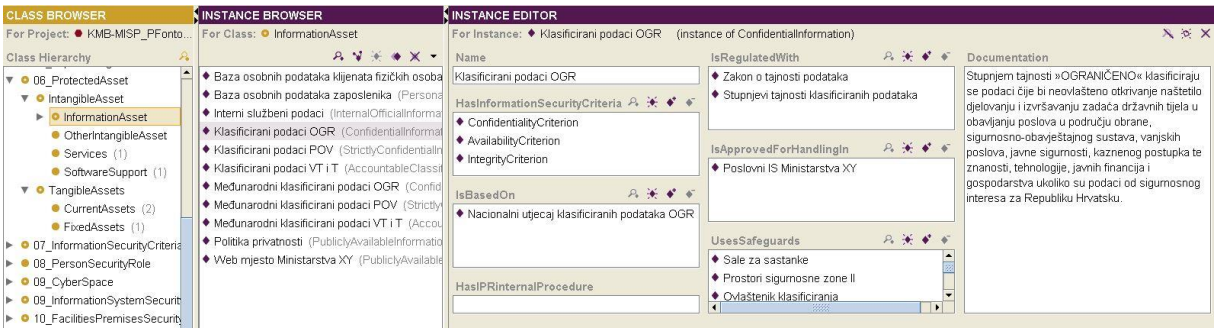
sigurnosti informacijskih sustava koristi se skup minimalnih sigurnosnih mjera prema normi NIST [85], uz mogućnost provedbe dodatnih mjera sukladno provedenoj procjeni rizika.




**Slika 7.15:** Prikaz ekrana s ontološkim modelom zamišljene studije slučaja politike informacijske sigurnosti Ministarstva XY, koji prikazuje instance klasa iz prvog podsustava definicije domene informacijske sigurnosti i instancu klase organizacije provoditelja politike informacijske sigurnosti

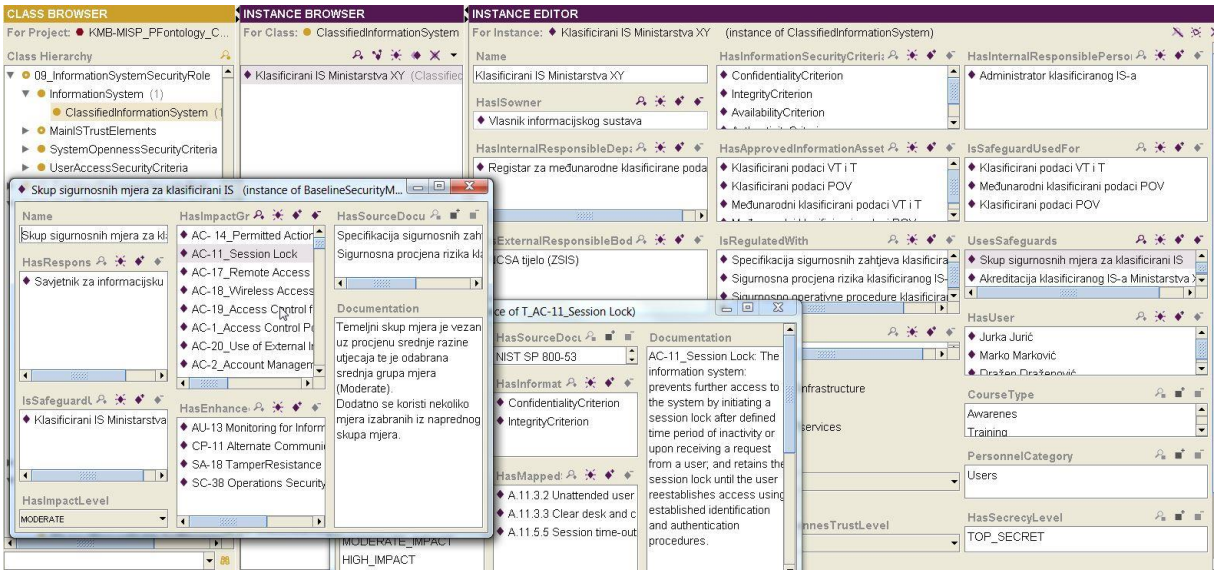
Za sliku 7.15 vrijedi sve što i za prethodno opisanu sliku 7.9 u studiji slučaja 1, gdje je ovaj isti prikaz napravljen za tvrtku ABC d.o.o., a jedino su, sukladno pojašnjenju u uvodnom odlomku teksta ovog poglavlja, modelirane instance ovdje prilagođene potrebama i zahtjevima politike informacijske sigurnosti državnog sektora. To znači da u obje studije slučaja koristimo potpuno isti programski ontološki metamodel, stvarajući potrebne modele sukladno vrsti politike koju želimo provesti (slika 7.1). Stoga će se u daljnjem tekstu studije slučaja Ministarstva XY više usmjeriti na povezanost s podsustavima tipičnim za politike informacijske sigurnosti državnog sektora (PS11 do PS16).

Informacijska imovina Ministarstva modelirana je u skladu sa zakonskim zahtjevima za državni sektor i prikazana je na slici 7.16. Modelirane su različite kategorije podataka koje, poput odabrane instance *Klasificirani podatci OGR*, imaju svojstvo povjerljivosti, ali i kategorije poput web-mjesta Ministarstva XY, koje imaju svojstvo cjelovitosti i raspoloživosti. Svaka kategorija imovine slotovima je povezana s instancama potrebnih klasa u drugim podsustavima.




**Slika 7.16:** Prikaz ekrana s instancama klasa iz podsustava definicija podataka i drugih vrijednosti (PS6), kao i podatcima odabrane instance *Klasificirani podatci OGR*

Nadalje, na slici 7.17 prikazana je definicija informacijskih sustava Ministarstva XY, od kojih se poslovni informacijski sustav koristi za opće poslovne namjene i kategorije informacijske imovine (ISO 27001 pristup s internom revizijom), dok se klasificirani informacijski sustav koristi za segment poslovanja povezan s klasificiranim podatcima, prema kategorijama podataka sa slike 7.16. Sigurnosne kontrole poslovnog informacijskog sustava ostvarene su po istom modelu kao razvojni informacijski sustav tvrtke ABC u studiji slučaja 1 prema slikama 7.12 i 7.13.

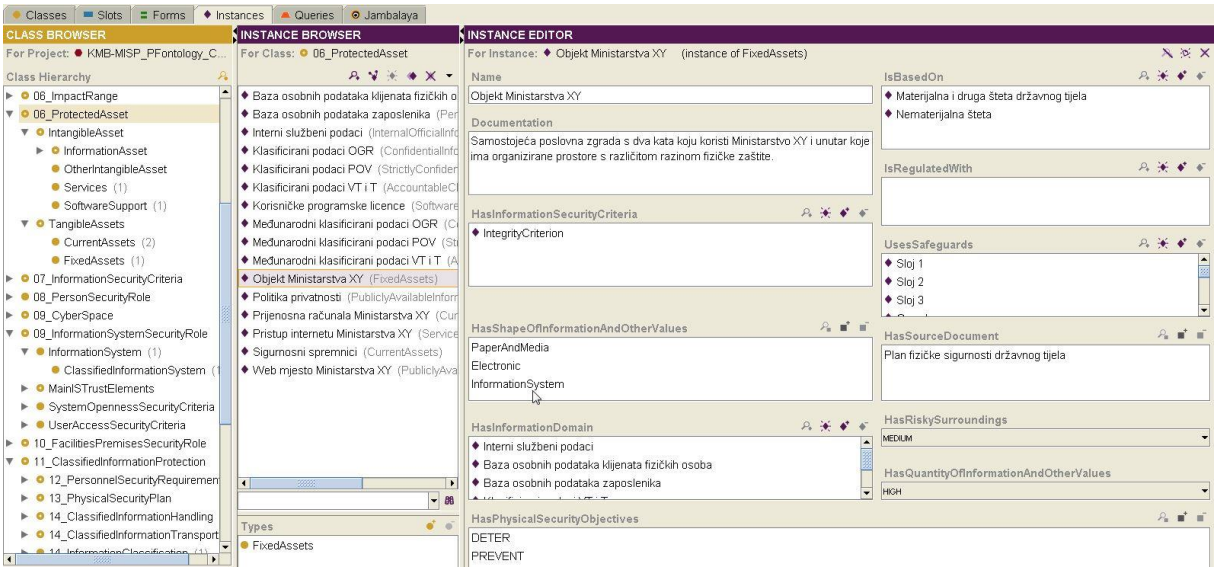



**Slika 7.17:** Prikaz ekrana s instancama klasa iz podsustava definicija informacijskih sustava (PS9), kao i podatcima odabrane instance *Klasificirani IS Ministarstva XY* te *Skupom sigurnosnih mjera za klasificirani IS*, i prikazom mjere *AC-11* iz NIST taksonomije

Na slici 7.17 prikazana je instanca klase za klasificirani informacijski sustav Ministarstva XY, koja koristi povezanost niza instanci različitih klasa (vlasnik, odgovorna ustrojstvena cjelina,

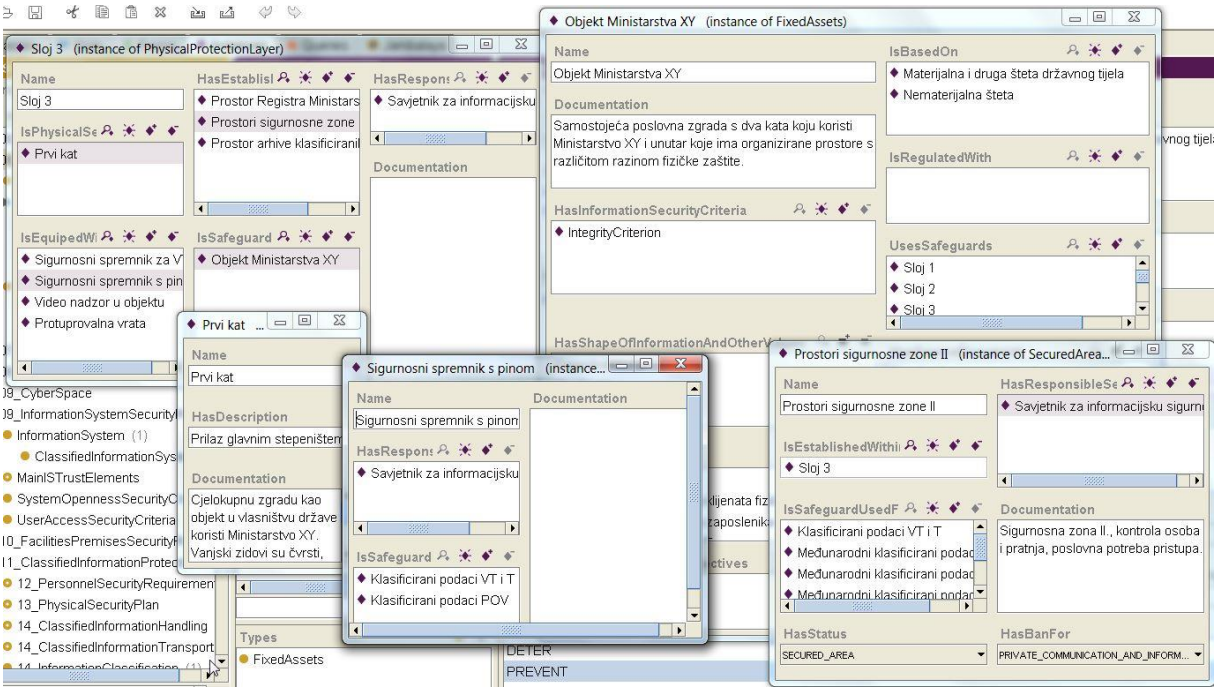
rukovoditelj sigurnosti, informacijske kategorije odobrene za korištenje na IS-u, regulativni zahtjevi, administrator IS-a, korisnici IS-a te uvjeti povjerenja). Pored toga vidljive su i sigurnosne mjere koje su ovdje, zbog klasificiranih podataka, slotom *usesSafeguards* povezane s PS15 i instancom klase *Skup sigurnosnih mjera za klasificirani IS*, koja je zasnovana na NIST normi [85] i prikazana u prozoru s donje, lijeve strane slike 7.17.

Programski ontološki metamodel u podsustavu PS6 omogućava definiranje objekata i prostora, koji se koriste uz pomoć klasa iz drugih podsustava (PS10 i PS13) te se također povezuju s ostalim klasama modela prema slici 7.18.

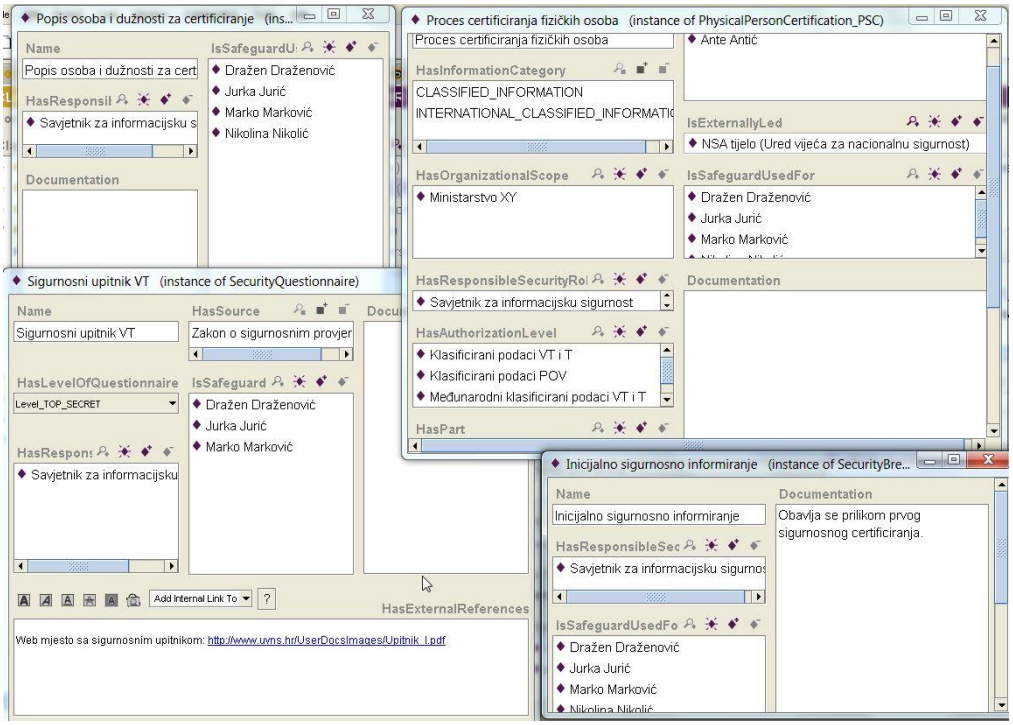



**Slika 7.18:** Prikaz ekrana s instancama klasa iz PS6 i odabranom instancom *Objekt Ministarstva XY*

Slot *usesSafeGuards* koristi koncept zaštite po dubini koji se temelji na slojevima fizičke sigurnosti, a koji se pridružuju stvarnim objektima (perimetar, zgrada, sigurnosna oprema, sigurnosno definirani prostori, kategorije podataka, odgovornost i sl.). Ovo povezivanje ilustrirano je na slici 7.19. za instancu *Objekt Ministarstva XY*, te povezane instance: *Sloj 3*, *Prvi kat*, *Sigurnosni spremnik s pinom*, *Prostori sigurnosne zone II*. Na slici 7.20, prikazana je razlika pristupa prema osobama koje pristupaju klasificiranim podatcima stupnja tajnosti POV i više (popis osoba i dužnosti, sigurnosni upitnik, proces sigurnosnog certificiranja).




**Slika 7.19:** Prikaz ekrana s instancom *Objekt Ministarstva XY* i povezanim instancama: *Sloj 3*, *Prvi kat*, *Sigurnosni spremnik s pinom*, *Prostori sigurnosne zone II*




**Slika 7.20:** Prikaz ekrana s instancama klasa u podsustavu sigurnost osoblja (PS12)

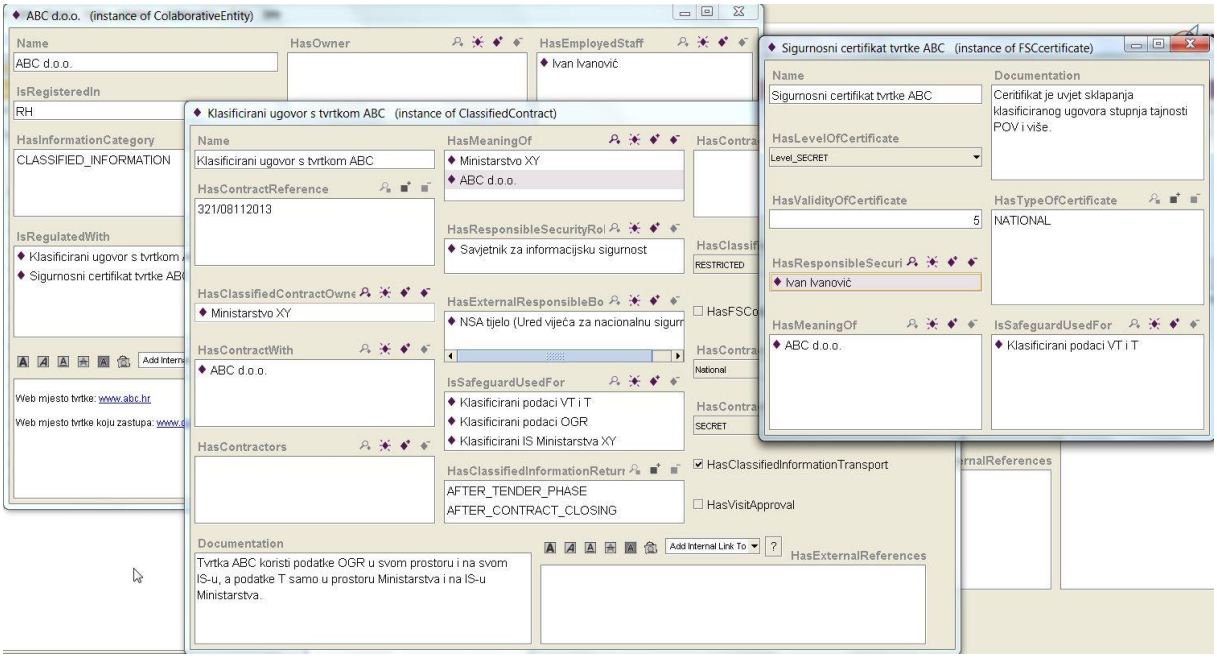
## 7.5. Studija slučaja 3 – dorada modeliranih politika informacijske sigurnosti u svrhu povezane uporabe

U poglavlju 7.3 i 7.4, opisane su dvije studije slučaja, u okviru kojih su pokazane mogućnosti modeliranja politike informacijske sigurnosti na temelju ostvarenog programskog ontološkog metamodela. Prva studija slučaja iz poglavlja 7.3, predstavlja primjer politike informacijske sigurnosti pravne osobe, zasnovan na poslovnim potrebama i primjeni norme ISO 27001 preko interne revizije. Druga studija slučaja iz poglavlja 7.4, predstavlja primjer politike informacijske sigurnosti državnog tijela, zasnovan na zakonskim propisima o zaštiti različitih kategorija podataka u državnom sektoru i primjeni tradicionalne politike informacijske sigurnosti u državnom sektoru.

U ovom poglavlju prikazana je treća studiju slučaja u kojoj će se prethodno prikazane modele politika informacijske sigurnosti pravne osobe i državnog tijela, koristiti u svrhu dodatnog modeliranja potrebnog za sklapanje klasificiranog ugovora o poslovnoj suradnji između državnog tijela i pravne osobe. Klasificirani ugovor sastoji se od razvoja programske podrške koja će na produkcijskom informacijskom sustavu Ministarstva XY koristiti klasificirane podatke stupnja tajnosti T. Pri tome se ostvarenje projekta može obavljati na testnom informacijskom sustavu sa simuliranim podatcima, koji zadovoljava uvjete za stupanj tajnosti OGR. U svrhu ostvarenja ovakvog klasificiranog ugovora savjetnik za informacijsku sigurnost Ministarstva XY mora isplanirati potrebne prilagodbe politike informacijske sigurnosti Ministarstva XY i pokrenuti odgovarajuće aktivnosti sigurnosnog certificiranja tvrtke ABC te utvrditi mogućnosti koje tvrtka ABC ima za ostvarenje ovakvog klasificiranog projekta. Nadležna osoba tvrtke ABC za pripremu ostvarenja klasificiranog projekta je rukovoditelj sigurnosti.

Na temelju korištenja konceptualnog metamodela u UML-u, svaka od ove dvije osobe nadležne za sigurnost u državnom tijelu i pravnoj osobi, može jednostavno predočiti elemente politike informacijske sigurnosti koji su sadržani i koji se primjenjuju na svakoj ugovornoj strani. Na taj način je razvidno da tvrtka ABC uz minimalne izmjene, može svoj razvojni informacijski sustav prilagoditi za potrebe testnog okruženja ovog klasificiranog projekta, dok će produkcijsko okruženje biti postojeći klasificirani informacijski sustav Ministarstva XY. Potrebne izmjene uključuju se u proces certificiranja pravne osobe, a zahtjev za certificiranje inicira savjetnik za informacijsku sigurnost Ministarstva XY.

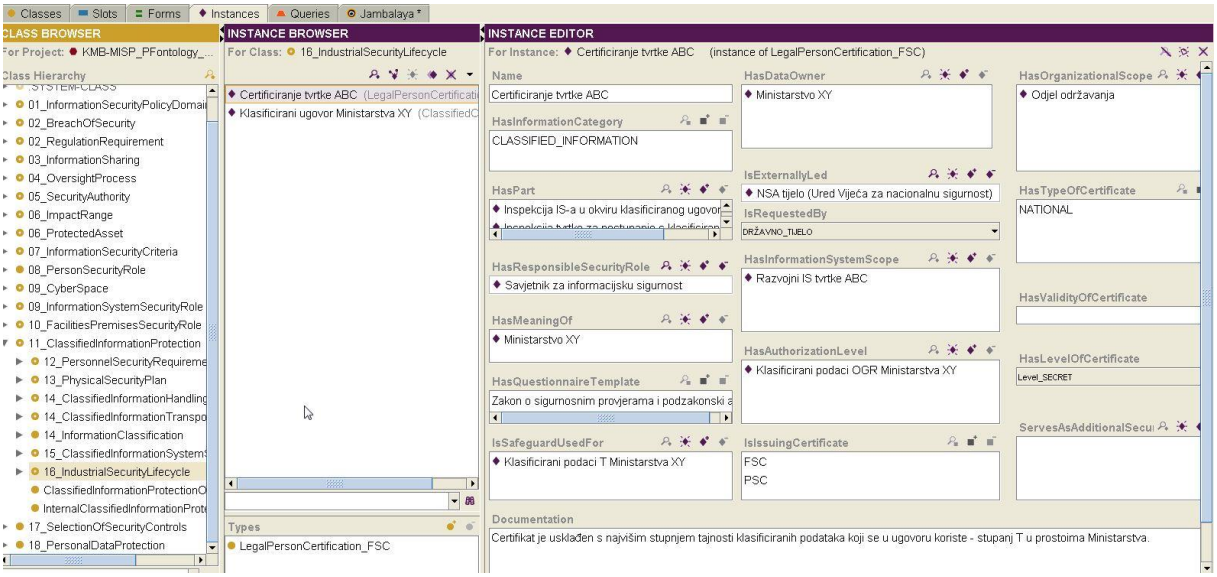
Ukoliko obje strane koriste politiku informacijske sigurnosti modeliranu na temelju istog programskog ontološkog metamodela, svaka od osoba zaduženih za sigurnost može započeti s definiranjem instanci klasa koje se moraju dodati na osnovni model prikazan u poglavlju 7.3, odnosno 7.4. Savjetnik u Ministarstvu XY mora krenuti od definicije organizacije s kojom surađuje (tvrtka ABC) te definirati tražene instance klasificiranog ugovora i sigurnosnog certifikata tvrtke, odnosno odgovorne osobe u tvrtci za sigurnost, prema slici 7.21.




**Slika 7.21:** Prikaz ekrana s instancama zamišljenog Ministarstva XY, modeliranim u svrhu sklapanja klasificiranog ugovora

Tvrtka ABC mora na isti način u svom programskom ontološkom modelu politike informacijske sigurnosti definirati državno tijelo s kojim surađuje, odgovornu osobu i klasificirani ugovor, ali je uz to potrebno modelirati instancu *Certificiranje tvrtke ABC* prema slici 7.22. Ovim izmjenama u podsustavu PS16 zadovoljeni su zahtjevi politika informacijske sigurnosti obje organizacije koje surađuju. Tvrtka u okviru procesa certifikacije ima dodatne izmjene jer mora u domeni klasificiranih podataka prepoznati izmjene koje proizlaze iz zahtjeva klasificiranog projekta i procesa certificiranja. Izmjene je najlakše provesti prateći zahtjeve modeliranih instanci, kao što je instanca *Certificiranje tvrtke ABC* na slici 7.22. Modeliranje ove instance na slici 7.22 traži prethodno modeliranje svih instanci s kojima je povezana te se unoseći potrebne podatke za slotove ove instance postupno definira druge instance s odgovornim tijelima, ulogom savjetnika za informacijsku sigurnost, postupcima

unutarnjeg i vanjskog nadzora, kategorijama podataka, opsegom certificiranja unutar tvrtke (npr. odabran je Odjel održavanja), kao i stupanj i vrsta certifikata. Modeliranje ovih instanci otvara potrebu za još nekim instancama koje nedostaju tvrtki ABC, a prikazane su u modelu politike informacijske sigurnosti Ministarstva XY (npr. certificiranje osoba, vođenje evidencija o certifikatima i sl.). Logika međusobne povezanosti klasa i podsustava programskog ontološkog metamodela upravlja potrebom stvaranja instanci prilikom modeliranja.

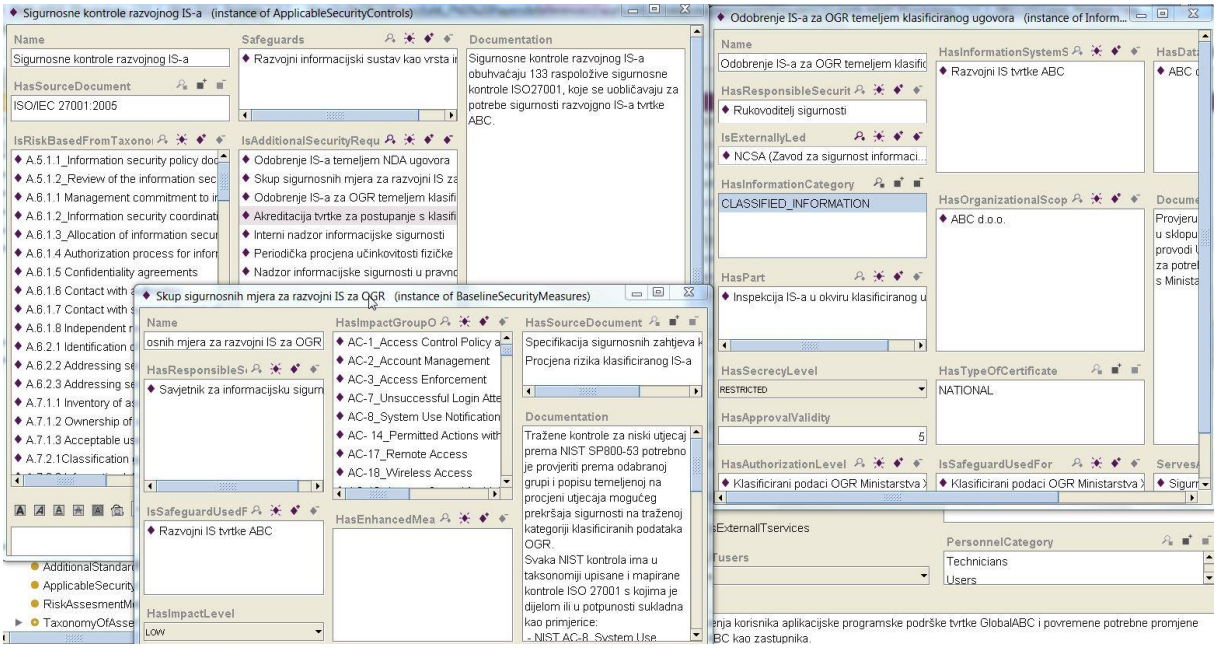



**Slika 7.22:** Podsustav PS16 s instancom *Certificiranje tvrtke ABC*, modeliranom u svrhu sklapanja klasificiranog ugovora

Uvođenje novih instanci u modelu politike informacijske sigurnosti tvrtke ABC, u dijelu PS12, vezanom za osobe koje pristupaju klasificiranim podatcima, prikazano je na slici 7.23.


**Slika 7.23:** Nove instance u podsustavu PS16 zamišljene tvrtke ABC, s prikazanom instancom *Nacionalni certifikat*, modelirane u svrhu prilagodbe politike informacijske sigurnosti na temelju sklapanja klasificiranog ugovora

U svrhu prilagodbe razvojnog informacijskog sustava tvrtke ABC, za potrebe nove kategorije podataka (klasificirani podatci stupnja tajnosti OGR), na slici 7.24 prikazane su potrebne preinake na postojećim instancama koje opisuju razvojni informacijski sustav tvrtke ABC. S jedne strane to su dodatni sigurnosni zahtjevi prikazani u instanci *Sigurnosne kontrole razvojnog IS-a*, u lijevom gornjem kutu slike 7.24, a s druge strane to je potreba usporedbe ostvarenih sigurnosnih kontrola iz norme ISO 27001 sa odabranim skupom minimalnih sigurnosnih mjera za nisku razinu utjecaja prema NIST normi. U tu svrhu, u dnu slike 7.24, prikazana je modelirana instanca *Skup sigurnosnih mjera za razvojni IS za OGR*, koja preko mapiranja ove dvije norme pojednostavljuje postupak provjere.




**Slika 7.24:** Instance klasa povezane s razvojnim informacijskim sustavom zamišljene tvrtke ABC i preinake potrebne za korištenje klasificiranih podataka stupnja tajnosti OGR

## 7.6. Rasprava o rezultatima prikazanih studija slučajeva programskog ontološkog modeliranja politika informacijske sigurnosti

U sedmom poglavlju pokazano je kako programski ontološki metamodel, ostvaren predloženom metodom modeliranja, unatoč definiranju visoke razine detalja u ovoj posljednjoj fazi programskog ostvarenja i dalje posjeduje visoku razinu općenitosti u odnosu

na širu domensku primjenjivost. Time se potvrđuje valjanost predloženog pristupa modeliranju šire domenske razine politika i normi informacijske sigurnosti, jer je ostvarena široka primjenjivost i jednostavna prilagodljivost različitim lokalnim okruženjima, koristeći taksonomije operativnog znanja, kao što je propis ili norma s popisom sigurnosnih kontrola.

Ostvarenje programskih ontoloških modela za odabrane studije slučajeva na temelju prethodno ostvarenog programskog ontološkog metamodela, sastoji se od modeliranja potrebnih instanci klasa iz metamodela za opisane primjene. U tablici 7.1 prikazana je usporedba broja potrebnih instanci klasa koje je trebalo ostvariti prilikom modeliranja studija slučajeva 1, 2 i 3 iz poglavlja 7.3, 7.4 i 7.5. Broj klasa (792), slotova (246) i instanci (530) od kojih se sastoji programski ontološki metamodel, prikazan u stupcima sa sivom pozadinom, ne mijenja se prilikom modeliranja i ostvarenja ontoloških programskih modela u prikazanim studijama slučajeva. Ontološki programski modeli zamišljenih organizacijskih okruženja stvaraju se isključivo modeliranjem instanci postojećih klasa iz metamodela i korištenjem istog ontološkog programskog metamodela prema slici 7.1.

**Tablica 7.1:** Usporedba broja ostvarenih programskih elemenata korištenih u programskom ontološkom metamodelu i ontološkim modelima ostvarenih studija slučajeva

| **Promatrano programsko ostvarenje:** | | **Programski ontološki metamodel s ukupno 1568 programskih elemenata** | | | **Programski ontološki modeli** | |
|---|---|---|---|---|---|---|
| | | Broj: | | | Ukupan broj programskih elemenata | Povećanje broja instanci klasa pri modeliranju |
| | | Klasa | Slotova | Instanci klasa | | |
| 1.a) | **Studija slučaja 1**, pravna osoba, **programski ontološki model 1**. | **792** | **246** | **530** | 1672 | **104** |
| 1.b) | **Studija slučaja 3**, pravna osoba u suradnji s državnim tijelom, **programski ontološki model 2**. | | | | 1706 | **34** |
| 2.a) | **Studija slučaja 2**, državno tijelo, **programski ontološki model 3**. | | | | 1754 | **186** |
| 2.b) | **Studija slučaja 3**, državno tijelo u suradnji s pravnom osobom, **programski ontološki model 4**. | | | | 1758 | **4** |

Iz tablice 7.1 vidljivo je da programski ontološki metamodel nosi najveću težinu u složenosti ostvarenja, jer su u njemu ostvarene sve potrebne klase (792), svi potrebni slotovi (246) te najveći broj instanci klasa (530). Programski ontološki metamodel sastoji se ukupno od 1568 programskih elemenata: klasa, slotova i instanci klasa. Klase u programskom ontološkom metamodelu (okviri u *Protégé Frames*), predstavljaju sve potrebne opće i posebne koncepte prepoznate na široj domenskoj razini (prilog B) i razrađene kroz opisane faze metode modeliranja. Slotovi u programskom ontološkom modelu (okviri u *Protégé Frames*), ostvaruju relacije između klasa i instanci klasa (prilog C) te različite vrste atributa klasa (UML dijagrami klasa u šestom poglavlju) potrebnih u modelu i instancama klasa, koje se modeliraju za potrebe konkretnog okruženja. Instance klasa u programskom ontološkom metamodelu predstavljaju baze operativnog znanja za metamodelom predviđene taksonomije sigurnosnih incidenata u PS9 [13], taksonomije minimalnih sigurnosnih mjera u PS15 [85], odnosno taksonomije sigurnosnih kontrola, prijetnji i ranjivosti u PS17 [27, 91].

Prema tablici 7.1, redak 1.a), za ostvarenje programskog ontološkog modela politike informacijske sigurnosti pravne osobe u studiji slučaja 1 (poglavlje 7.3.), bilo je potrebno dodatno modelirati 104 instance klasa na temelju klasa metamodela, dok je u slučaju ostvarenja ontološkog modela politike informacijske sigurnosti državnog tijela (redak 2.a) u studiji slučaja 2 (poglavlje 7.4), bilo potrebno dodatno modelirati 186 instanci klasa na temelju klasa metamodela. Rezultat je sukladan očekivanjima i analizi provedenoj u četvrtom poglavlju, gdje se vidi veća složenost sigurnosnih zahtjeva informacijske sigurnosti u državnom sektoru. Nadalje je vidljivo kako je u studiji slučaja 3, za ostvarenje dopune modela politike informacijske sigurnosti u svrhu poslovne suradnje državnog tijela i pravne osobe, u modelu državnog tijela trebalo modelirati samo 4 dodatne instance klasa metamodela (redak 2.b), dok je u modelu pravne osobe bilo potrebno modelirati 34 dodatne instance klasa metamodela (redak 1.b). Ovaj rezultat također je u skladu s očekivanjima i složenošću sigurnosnih zahtjeva politika informacijske sigurnosti u državnom sektoru. Ukupno manji broj instanci klasa u pravnoj osobi (138), u odnosu na državno tijelo (190), rezultat je ograničenih zahtjeva politike informacijske sigurnosti državnog sektora, koji se preko klasificiranih ugovora postavljaju na tvrtku u najužem mogućem segmentu, nužnom za provedbu klasificiranog ugovora (npr. samo dio osoblja, korištenje nižeg stupnja tajnosti OGR u tvrtki ABC, a stupnja tajnosti T u prostorima Ministarstva XY, odobrenje pogodnijeg, razvojnog informacijskog sustava tvrtke ABC na ovaj niži stupanj tajnosti OGR i sl.).

Usporedbom podataka iz tablice 7.1, omjer složenosti ostvarenja procesa modeliranja u ovom radu, može se prikazati kao omjer ukupno potrebnih programskih elemenata (klase, slotovi, instance) u završnom povezanom modelu složenije studije slučaja 3 u odnosu na ostvareni programski ontološki metamodel. Tako je u slučaju modeliranja politike informacijske sigurnosti pravne osobe, ukupno potreban broj programskih elemenata 1706, što znači da 1568 programskih elemenata metamodela čini oko 92% rješenja modeliranja za primjer pravne osobe. U slučaju modeliranja politike informacijske sigurnosti državnog tijela, ukupno je potreban broj programskih elemenata 1758, što znači da 1568 programskih elemenata metamodela čini oko 89% rješenja modeliranja za primjer državnog tijela.

Pored prethodnog usporednog prikaza učinkovitosti i jednostavnosti postupka modeliranja, važno je istaknuti i praktičnu funkcionalnost ostvarenog programskog ontološkog metamodela, osobito u usporedbi s pristupima koji danas prevladavaju u praksi. Najčešći pristup u praktičnoj primjeni informacijske sigurnosti još uvijek predstavljaju različiti oblici tekstualnih dokumenata sa smjernicama i preporukama za provedbu normi i procedura prema slici 4.1 [105, 106]. U odnosu na vrlo općenite sigurnosne zahtjeve koji se postavljaju normama i regulativnim okvirom i koji u primjeni često ne daju dovoljno informacija za provedbu, svrha ovakvih smjernica je ili dodatno pojašnjavanje izvornih sigurnosnih zahtjeva [105], ili smjernice za provedbu sigurnosnih zahtjeva u nekom posebnom sektoru [91, 107, 108]. Niz godina su u primjeni i različiti oblici pomoćnih programskih alata koji olakšavaju ostvarenje dokumentacije potrebne za certificiranje prema određenoj normi [109] i koji se sastoje od djelomično popunjenih obrazaca u obliku tekstualnih datoteka, ili od tablica s djelomično automatiziranim unosom podataka u liste za provjeru stanja, inventurne liste opreme i sl. U praksi su prisutne i neke programske aplikacije koje olakšavaju odabir sigurnosnih kontrola [110], ostvarene u obliku baze podataka sigurnosnih kontrola s mogućnošću izvoza podataka i korištenja odabranih kontrola u obrascima dokumenata kakve omogućavaju pomoćni programski alati, primjerice u [109]. Uspoređujući funkcionalnost takvih rješenja s programskim ontološkim metamodelom koji je ostvaren u ovom radu, može se reći da ovakva rješenja predstavljaju uskonamjenske baze operativnog znanja, s funkcionalnošću sličnoj taksonomiji minimalnih sigurnosnih mjera u podsustavu PS15 metamodela ostvarenog u ovom istraživanju. Također, gledajući uski dio funkcionalnosti ostvarenog programskog ontološkog metamodela, u podsustavu PS17 u kojem se koristi logički model povezivanja taksonomija sigurnosnih kontrola, prijetnji i ranjivosti prema slici 4.11, može se reći da postoje programska rješenja za podršku metodama upravljanja rizikom

koje ovaj uski segment ostvaruju na sličan način, ali u potpuno drugačijem i užem kontekstu metode upravljanja rizikom, kao primjerice u [111].

Najvažnije obilježje predložene metode modeliranja i ostvarenog konceptualnog metamodela te programskog ontološkog metamodela, za razliku od prethodno spomenutih pristupa, jest mogućnost sveobuhvatnog modeliranja politike informacijske sigurnosti neke organizacije u punom obimu životnog ciklusa politike informacijske sigurnosti (slika 5.2), kao što je pokazano na primjeru studije slučaja 1 i pojašnjeno na kraju poglavlja 7.3.

U okviru ove analize rezultata prikazanih studija slučajeva, potrebno je naglasiti kako korištenje programskog ontološkog metamodela za planiranje politike informacijske sigurnosti, osigurava provedbu još jednog problema uočenog u motivaciji ovog istraživanja u poglavlju 1.2. To je nepovezan i nekoordiniran pristup sektorskim sigurnosnim zahtjevima. Ako se pogleda slika 7.10, vidljivo je kako su sigurnosne uloge koordinirane preko iste osobe izvorno postavljene za rukovoditelja sigurnosti i službenika za zaštitu osobnih podataka, procesom modeliranja u studiji slučaja 3, proširene i na ulogu savjetnika za informacijsku sigurnost. Postoje slučajevi u kojima se ove različite, ali međusobno usko povezane sigurnosne uloge, u nekim složenijim slučajevima mogu razdvojiti na različite osobe. Proces modeliranja uz pomoć metamodela i u ovim razdvojenim slučajevima sigurnosnih uloga na različite osobe i dalje je koordiniran i povezan u odnosu na kategorije podataka, informacijske sustave i druge elemente, preko klasa metamodela u kojima su ostvarene potrebne međusobne relacije (slike 7.12, 7.15, 7.19, 7.20).

Najvažniji rezultati studija slučajeva u prvom redu su uspješno prikazana mogućnost korištenja programskog ontološkog metamodela, kao zajedničkog metamodela za politike informacijske sigurnosti organizacija koje pripadaju različitim sektorima društva. Time je pokazano svojstvo sveobuhvatnosti predloženog načina modeliranja politika informacijske sigurnosti koje je u zadovoljavajućoj mjeri zadržano unatoč više razina metode modeliranja u kojima su primijenjene apstrakcije domene informacijske sigurnosti stvarnog svijeta (slika 5.1).

Pristup modeliranju studija slučajeva, pokazuje također omogućavanje jednostavnijeg procesa planiranja politika, jer klase ostvarenog programskog ontološkog metamodela svojom strukturom i međusobnom povezanošću navode korisnika na definiranje atributa i relacija,

potrebnih za instance klasa koje definiraju određeno lokalno okruženje. Jednostavnost postupka još je očitija u slučajevima promjena politika informacijske sigurnosti, odnosno uvođenja novih funkcionalnosti kao što je poslovna suradnja prema trećoj studiji slučaja. Tada se uz pomoć konceptualnog metamodela u UML-u, može vizualnim putem lako utvrditi koji podsustavi i u kojim klasama traže dodatno modeliranje. U takvom procesu modeliranja u programskom ontološkom modelu, mogu se koristiti kopiranja prije unesenih podataka, kopiranja istovrsnih instanci, kao i raspoložive taksonomije operativnog znanja, sadržane u ostvarenom programskom ontološkom metamodela (sigurnosni incidenti, prijetnje, ranjivosti i kontrole).

Ostvareni programski ontološki metamodel, omogućava i visoku učinkovitost u ponovnoj primjeni postojećeg ontološkog modela jedne organizacije na drugu organizaciju ili na novo okruženje iste organizacije (npr. preseljenje ili povećanje tvrtke). Određeni broj prije korištenih instanci klasa, u takvom slučaju treba se djelomično korigirati i prilagoditi nazivlju i podatcima lokalnog okruženja, ali je proces prilagodbe svakom novom primjenom sve učinkovitiji, jer se broj raspoloživih polaznih obrazaca modeliranih politika informacijske sigurnosti primjenom multiplicira i puno je lakše pronaći sličan početni model za novo okruženje.

Opis svojstva učinkovitosti navodi na drugo svojstvo koje je još važnije od prethodno opisane učinkovitosti, a to je svojstvo dosljednosti. Ovakav pristup pokazuje i svojstvo dosljednosti, jer se prilagodbom razvijenih obrazaca modela, prilagođavaju vanjska obilježja, poput nazivlja ili obilježja fizičkog prostora, dok potrebne relacije štićenih vrijednosti i temeljnih kriterija i čimbenika informacijske sigurnosti ostaju zadržane. U nekim situacijama novih okruženja u kojima se planira politika informacijske sigurnosti svojstvo dosljednosti je iznimno važno. Ovo svojstvo traži se u različitim slučajevima koji su tijekom uvodnih poglavlja više puta spominjani. Primjer zahtjeva dosljednosti u praćenju vršne politike informacijske sigurnosti predstavlja međunarodna politika informacijske sigurnosti u slučajevima međunarodnih organizacija NATO i EU u odnosu na zemlje članice i zemlje partnere, ali i u odnosu na decentralizirana tijela ovih međunarodnih organizacija. Sljedeći primjer zahtjeva dosljednosti je i svaka nacionalna politika državnog sektora koja se prema istim sigurnosnim zahtjevima primjenjuje na sva državna tijela koja koriste klasificirane podatke. Zaštita osobnih podataka na razini EU-a je također dobar primjer u kojem se postavljaju zahtjevi dosljednog praćenja sigurnosnih zahtjeva definiranih na nadnacionalnoj

razini EU-a, za sve pravne osobe u svim zemljama članicama EU-a (poglavlje 4.9.2.). Sličan primjer mogu biti sektorska regulatorna tijela koja u sektoru javnih elektroničkih komunikacija reguliraju i ujednačavaju norme u zaštiti sigurnosti i cjelovitosti mreža i usluga, kao i u procedurama prijave sigurnosnih incidenata [76]. Isto tako, poslovni sektor koristi zahtjev dosljednosti politike informacijske sigurnosti u poslovnoj suradnji u kojoj provodi neke od prethodno navedenih politika informacijske sigurnosti (npr. studija slučaja 3. iz poglavlja 7.5), ali i u slučajevima koji su vrlo česti u poslovnom sektoru, kao što su spajanja različitih tvrtki, odnosno udruživanja tvrtki za potrebe zajedničkog rada na velikim projektima.

Gledajući iz kuta upravljanja životnim ciklusom politika informacijske sigurnosti, na primjerima studija slučajeva može se uočiti niz praktičnih prednosti koje se ostvaruju primjenom doprinosa ovog rada u svim fazama životnog ciklusa politike informacijske sigurnosti. Faza planiranja, na temelju korištenja pristupa predloženog u ovom radu, temelji se na jednostavnom stvaranju instanci gotovih klasa programskog ontološkog metamodela kojima se opisuje politika informacijske sigurnosti organizacije, a stvaranjem repozitorija gotovih modela politika, ovaj proces može biti još puno učinkovitiji. Faza ostvarenja koristi već uspostavljene i povezane sigurnosne elemente modela, ostvarene u fazi planiranja, koji se mogu izravno opisati ili kopirati u traženi oblik dokumentacije, sukladno zadanim normama ili propisima. Tako dobiveni dokumenti jednostavno se povezuju s pripadnim instancama modela u svrhu daljnjeg centraliziranog pristupa i održavanja. Faza provođenja koristi mogućnost dnevnog praćenja sigurnosno relevantnih promjena uz pomoć brzog i jednostavnog stvaranja instanci za nove osobe, ugovore, štićenu imovinu, povrede sigurnosti i sl., jednostavnim kopiranjem i prilagodbom već postojećih istovrsnih instanci te slijednim ažuriranjem potrebnih dokumenata kao zahtjeva normi ili propisa, povezanih s odgovarajućim instancama modela (veza na datoteku). Faza preispitivanja ostvaruje mogućnost praćenja i simuliranja svih promjena modelirane politike informacijske sigurnosti kroz međusobno logički povezane razine, podsustave, klase i instance modela, primjerice, uspoređujući postojeće instance klasa s ažuriranom procjenom rizika, s novim poslovnim zahtjevima, ili s promjenom nekog od zahtjeva globalnog okruženja. Ovakvim postupkom preispitivanja, štićene vrijednosti, temeljni čimbenici i kriteriji informacijske sigurnosti, međusobno su logički povezani na način modeliran za određeno stvarno organizacijsko okruženje te se željene promjene na bilo kojoj razini modela mogu logički slijediti kroz model prateći povezane posljedice promjena.

# 8. ZAKLJUČAK

Politike i norme informacijske sigurnosti prisutne su već desetljećima u poslovanju različitih organizacijskih entiteta u državnim sektorima zemalja i međunarodnim organizacijama, a tijekom tog razdoblja postale su redovita praksa i u poslovnim sektorima. Globalni procesi kao što su stvaranje kibernetičkog prostora i društvena globalizacija, preko zajedničke komunikacijske i informacijske infrastrukture te povećanjem potreba i zahtjeva za različitim vidovima suradnje i razdiobe osjetljivih podataka, zahtijevaju od različitih vrsta organizacijskih entiteta sve veću razinu međusobnog razumijevanja različitih sigurnosnih mjera. Dosadašnji razvoj politika i normi informacijske sigurnosti uglavnom je bio usmjeren prema različitim, usko profiliranim sektorskim pristupima, te je doveo do stanja slabe međusobne povezanosti i koordinacije primjene između različitih politika i normi informacijske sigurnosti što rezultira slabom povezanošću znanja na široj domenskoj razini.

Za razliku od srodnih istraživanja, u ovom istraživanju primijenjen je različit pristup domenskoj razini informacijske sigurnosti. Umjesto analize pojedinih politika i normi informacijske sigurnosti ili nekih užih domenskih segmenata kao što su, primjerice, prijetnje i ranjivosti informacijskih sustava, u ovom radu pristupilo se analizi šireg domenskog područja informacijske sigurnosti. Cilj analize je prepoznavanje i poopćavanje koncepata koji predstavljaju zajednička obilježja različitih pristupa informacijskoj sigurnosti na široj domenskoj razini (npr. općeniti koncepti nadzora, akreditacije, primjene sigurnosnih kontrola, regulativnih zahtjeva i sl.). Kako bi se područje analize zadovoljavajuće ograničilo, a istovremeno ostalo dovoljno široko za mogućnost poopćavanja rezultata analize, utvrđen je skup dominantnih politika i normi informacijske sigurnosti u suvremenoj praksi uz pomoć kojeg se promatra šire domensko područje informacijske sigurnosti. Promatrajući na ovaj način širi domenski prostor, uočava se da je stanje razvoja došlo do faze u kojoj je veliki broj informacija uobličen u odgovarajuće procedure, odnosno politike i norme informacijske sigurnosti, no viša razina razumijevanja njihovog korištenja u širem i sveobuhvatnom domenskom smislu i u primjeni na različite organizacijske entitete u uvjetima suvremenog društva, nalazi se u početnoj fazi istraživanja. Ova viša razina razumijevanja korištenja suvremenih politika i normi informacijske sigurnosti u širem i sveobuhvatnom domenskom smislu cilj je analize provedene u radu. Ostvarena sistematizacija i integracija različitih

pristupa i zahtjeva dominantnih politika i normi informacijske sigurnosti, odnosno zahtjeva globalnog i lokalnog okruženja u kojima se provode ove politike i norme informacijske sigurnosti, predstavlja temelj za širu normizaciju područja informacijske sigurnosti.

Konceptualizacija koja proizlazi iz analize, dobivena razvojem zajedničkog rječnika domene te sistematizacijom i formalizacijom temeljnih obilježja dominantnih politika i normi informacijske sigurnosti, predstavlja nužan korak u povezivanju heterogenog i slabo povezanog domenskog znanja. Kako bi se na odgovarajući način sistematizirali i povezali utjecaji globalnog i lokalnog okruženja neke organizacije koja provodi politiku informacijske sigurnosti te osiguralo povezivanje različitih faza životnog ciklusa politika informacijske sigurnosti, kao i željena razina detalja s obzirom na potrebne sigurnosne sadržaje, u radu je predložena metoda modeliranja politika informacijske sigurnosti temeljena na upravljanju znanjem. Cilj modeliranja je ostvarenje konceptualnog metamodela politika informacijske sigurnosti, modeliranog kao složeni sustav koji obuhvaća niz podsustava na više organizacijskih razina. Predloženom metodom obuhvaća se sustavski prikaz životnog ciklusa politike informacijske sigurnosti u globalnom okruženju, transformiran u hijerarhijsku domensku taksonomiju uz pomoć koje se razrađuje sadržaj modela u obliku rječnika pojmova, njihove kategorizacije, unutarnjih hijerarhijskih odnosa te međusobnih relacija i atributa, za odabrane i pojmovima pridružene domenske koncepte.

Konceptualni metamodel politika informacijske sigurnosti, kao okvir za upravljanje i komuniciranje znanjem domene, ostvaren je uz pomoć UML-a (engl. *Unified Modelling Language*). Na taj način dobiven je metamodel koji je formalno specificiran (rječnik, sintaksa, semantika) i istovremeno izražen na razumljiv i vizualno opisan način, namijenjen prvenstveno komunikaciji između različitih profila stručnjaka koji se bave ovim multidisciplinarnim područjem politika i normi informacijske sigurnosti. Konceptualni metamodel daje odgovor na prvi postavljeni istraživački problem, jer se na temelju analize koja normira šire domensko područje i na temelju predložene metode modeliranja ostvaruje konceptualni metamodel kao okvir za upravljanje i komuniciranje znanjem, kojim se povezuje postojeće heterogeno i slabo povezano domensko znanje iz dominantnih politika i normi informacijske sigurnosti.

Drugo postavljeno istraživačko pitanje usmjereno je na mogućnosti jednostavnijeg, dosljednijeg, sveobuhvatnijeg i učinkovitijeg upravljanja životnim ciklusom politike

informacijske sigurnosti uporabom konceptualnog metamodela domene. Za rješavanje postavljenog istraživačkog problema, u drugoj fazi istraživanja ostvaren je programski ontološki metamodel, zasnovan na prethodno ostvarenom konceptualnom metamodelu zapisanom u UML-u. Programski ontološki metamodel ostvaren je u programskom razvojnom okruženju *Protégé Frames*, a koristi se za provjeru valjanosti konceptualnog metamodela te za provjeru svojstava koja se postižu njegovom primjenom. U svrhu ovih provjera, osmišljene su studije slučajeva za jedno zamišljeno državno tijelo i jednu zamišljenu tvrtku u okviru kojih su ostvareni programski ontološki modeli politika informacijske sigurnosti za ove zamišljene organizacijske entitete. Nakon toga je osmišljena dodatna studija slučaja poslovne suradnje državnog tijela i tvrtke (klasificirani ugovor) te je ostvarena koordinirana prilagodba dvaju, prethodno razvijenih programskih ontoloških modela politika informacijske sigurnosti, u svrhu ostvarenja dodatnih funkcionalnosti koje će omogućiti potrebne nove elemente modela suradnje ovih dviju organizacija. Programski ontološki modeli politika informacijske sigurnosti ostvareni u studijama slučajeva predstavljaju skupove instanci zajedničkog domenskog programskog ontološkog metamodela politika informacijske sigurnosti, ostvarene uz pomoć instanci potrebnih klasa raspoloživih u metamodelu.

Studijama slučajeva pokazana su svojstva koja se postižu primjenom ostvarenog konceptualnog metamodela. Proces planiranja politika informacijske sigurnosti postaje jednostavniji, jer je velika većina programskih elemenata: klasa, slotova i instanci klasa, sadržana u ostvarenom programskom ontološkom metamodelu (u odabranim studijama slučajeva čak 90%). Pri tome je modeliranje potrebnih instanci klasa modela ciljanog okruženja olakšano jednostavnim praćenjem povezanosti klasa metamodela koje navode korisnika na definiranje potrebnih instanci klasa, atributa i relacija za željeno lokalno okruženje. Pristup modeliranju dodatno olakšava ostvareni konceptualni metamodel u UML-u, koji pruža vizualni prikaz složenog metamodela koji se sastoji od 18 podsustava podijeljenih na četiri organizacijske razine. Izborom studija slučajeva pokazana je sveobuhvatnost metamodela koji se koristi za modeliranje politika informacijske sigurnosti organizacija koje pripadaju različitim sektorima društva i pri tome otvara mogućnost jednostavnih prilagodbi i proširenja takvih modela u svrhu međusektorske poslovne suradnje. Ostvareni programski ontološki metamodel, omogućava i visoku učinkovitost u ponovnoj primjeni postojećeg ontološkog modela razvijenog za potrebe jedne organizacije, u svrhu modeliranja druge organizacije. Proces prilagodbe svakom novom primjenom postaje sve učinkovitiji, jer se repozitorij modeliranih politika informacijske sigurnosti svakom novom

primjenom uvećava i olakšava pronalaženje sličnog početnog modela za novo okruženje. Ovakav pristup pokazuje i svojstvo dosljednosti, jer se prilagodbom razvijenih obrazaca modela, prilagođavaju vanjska obilježja, poput nazivlja ili obilježja fizičkog prostora, dok relacije između štićenih vrijednosti, temeljnih čimbenika i kriterija informacijske sigurnosti ostaju zadržane. Postoji čitav niz primjera zahtjeva dosljednosti u praksi kao što je praćenje središnje politike informacijske sigurnosti u slučajevima međunarodnih organizacija NATO-a i EU-a u odnosu na zemlje članice i zemlje partnere, nacionalna politika informacijske sigurnosti državnog sektora koja se primjenjuje na sva državna tijela, zaštita osobnih podataka na razini EU-a za sve pravne osobe u zemljama članicama EU-a, ili poslovni sektor u okviru poslovne suradnje u kojoj provodi neke od prethodno navedenih politika informacijske sigurnosti, ili u slučajevima spajanja različitih tvrtki, odnosno udruživanja više tvrtki za potrebe velikih projekata.

Gledajući iz kuta upravljanja životnim ciklusom politika informacijske sigurnosti, može se uočiti niz praktičnih prednosti koje se ostvaruju primjenom doprinosa ovog rada u svim fazama životnog ciklusa politike informacijske sigurnosti. Faza planiranja temelji se na jednostavnom stvaranju instanci gotovih klasa programskog ontološkog metamodela kojima se opisuje politika informacijske sigurnosti organizacije, a stvaranjem repozitorija gotovih modela politika, ovaj proces može biti još puno učinkovitiji. Faza ostvarenja koristi uspostavljene i povezane sigurnosne elemente modela, ostvarene u fazi planiranja, koji se mogu izravno opisati ili kopirati u traženi oblik dokumentacije, sukladno zadanim normama ili propisima. Tako dobiveni dokumenti jednostavno se povezuju s pripadnim instancama modela u svrhu daljnjeg centraliziranog pristupa i održavanja. Faza provođenja koristi mogućnost dnevnog praćenja sigurnosno relevantnih promjena stvaranjem instanci za nove osobe, ugovore, štićenu imovinu, povrede sigurnosti i sl., jednostavnim kopiranjem i prilagodbom postojećih istovrsnih instanci te slijednim ažuriranjem povezanih dokumenata. Faza preispitivanja ostvaruje mogućnost praćenja i simuliranja svih promjena modelirane politike informacijske sigurnosti kroz međusobno logički povezane organizacijske razine, podsustave, klase i instance modela, primjerice, uspoređujući postojeće instance klasa s ažuriranom procjenom rizika, s novim poslovnim zahtjevima, ili s promjenom nekog od zahtjeva globalnog okruženja. Ovakvim postupkom preispitivanja, štićene vrijednosti, temeljni čimbenici i kriteriji informacijske sigurnosti, međusobno su logički povezani na način modeliran za određeno stvarno organizacijsko okruženje te se željene promjene na bilo kojoj razini modela mogu logički slijediti kroz model prateći povezane posljedice promjena.

U okviru ovog rada ostvareni su sljedeći znanstveni doprinosi:

1. Provedena je analiza domene informacijske sigurnosti s ciljem šire domenske sistematizacije i integracije različitih pristupa i zahtjeva globalnog i lokalnog okruženja te dominantnih suvremenih politika i normi informacijske sigurnosti;
2. Predložena je metoda modeliranja politika informacijske sigurnosti temeljena na upravljanju znanjem koja obuhvaća sustavski prikaz životnog ciklusa politike informacijske sigurnosti u globalnom okruženju, transformiran u hijerarhijsku taksonomiju domene sa skupom pravila i relacija između različitih elemenata politika;
3. Ostvaren je konceptualni metamodel politika informacijske sigurnosti zapisan u UML-u, kao okvir za upravljanje i komuniciranje znanjem domene, čija je valjanost provjerena uz pomoć ostvarenja programskog ontološkog metamodela u *Protégé Frames* i ostvarenja programskih ontoloških modela za odabrane studije slučajeva.

Radom je pokazan način rješavanja postavljenih istraživačkih problema te su postignuti željeni ciljevi i znanstveni doprinosi postavljeni na razini domenskog modeliranja. Ostvarenje konceptualnog metamodela na predloženi način otvara i niz novih istraživačkih pitanja koja zahtijevaju daljnja istraživanja. Neka od ovih pitanja su istraživanje mogućnosti proširenja ostvarenog metamodela u smjeru daljnjeg modeliranja pojedinih elemenata u modelu, korištenih u obliku vanjskih elemenata (model crne kutije), kao što su akreditacijski i certifikacijski procesi, ili metode upravljanja rizikom. Ova proširenja mogu ići u smjeru konceptualizacije i modeliranja takvih procesa, ali i u smjeru mogućeg povezivanja s nekim od postojećih rješenja prikazanih u ovom radu. Također su moguća proširenja i prilagodbe ostvarenog metamodela za područje revizije politika i normi informacijske sigurnosti, osobito u nizu primjera istaknutih u okviru opisa svojstva dosljednosti ostvarenog metamodela.

## LITERATURA:


[1] Klaić, A., „Information Security in Business and Government Sectors", Proceedings of the International Convention MIPRO 2005, Opatija, Croatia, 2005, str. 193-198.

[2] Klaić, A., „Information Security Requirements in the Information Systems Planning Process", Proceedings of the International Conference on Information and Intelligent Systems (IIS), Varaždin, Croatia, 2006, str. 265-269.

[3] Klaić, A., Perešin, A., „Koncept regulativnog okvira informacijske sigurnosti", Zbornik radova međunarodne znanstvene konferencije „Dani kriznog upravljanja", Velika Gorica, Hrvatska, 2011., str. 678-707.

[4] Perešin, A., Klaić, A., „Povezanost koncepata kritične nacionalne infrastrukture i zaštite podataka", Zbornik radova međunarodne znanstvene konferencije „Dani kriznog upravljanja", Velika Gorica, Hrvatska, 2010., str. 13-29.

[5] Klaić, A., Perešin, A., „The Impact of the National Information Security Regulation Framework on Cyber Security in Global Environment", International Scientific Conference on Corporate Security in Dynamic Global Environment - Challenges and Risks, Institute for Corporative Security Studies, Ljubljana, Slovenia, 2012, str. 85-96.

[6] Kiely, L., Benzel, T., „Systemic Security Management", Institute for Critical Information Infrastructure Protection (ICIIP), USC Marschall School of Business, 2007, dostupno na: http://msbpwp01.marshall.usc.edu/assets/004/5347.pdf (30. rujna 2013.).

[7] Klaić, A., Hadjina, N., „Methods and Tools for the Development of Information Security Policy – A Comparative Literature Overview", Proceedings of the International Convention MIPRO 2011, Opatija, Croatia, 2011, str. 190-195.

[8] Smith, B., Ceusters, W., Temmerman, R., „Wusteria", Proceedings of Medical Informatics Europe 2005, Geneva, Switzerland, 2005, str. 647–652.

[9] Smith, B., „Ontology" in Blackwell Guide to the Philosophy of Computing and Information, L. Floridi (ed.), Oxford: Blackwell, 2003, str. 155–166.

[10] Mylopoulos, J., „Conceptual Modelling and Telos" in Conceptual Modelling, Databases and CASE: An Integrated View of Information Systems Development, Loucopoulos, P. and Zicari, R. (eds.), McGraw Hill, 1992.

[11] Fill, H. G., Burzynski, P., „Integrating Ontology Models and Conceptual Models using a Meta Modelling Approach“, Stanford Protégé Conference, Amsterdam, Holland, 2009.

[12] Hilliard, R., „Metamodels in 42010“, 2011, dostupno na: http://www.iso-architecture.org/ieee-1471/docs/Hilliard-On-Metamodels-in-42010.pdf (30. rujna 2013.).

[13] Howard, J. D., Longstaff, T. A., „A Common Language for Computer Security Incidents“, Sandia National laboratories, Albuquerque, New Mexico, U.S.A., 1998, dostupno na: http://www.osti.gov/scitech/biblio/751004 (30. rujna 2013.).

[14] U.S. Department of Defense, „Guidance for Implementing Net-Centric Data Sharing“, DoD 8320.02-G, April 2006, dostupno na: http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf (30. rujna 2013.).

[15] Gruber, T. R., „Toward Principles for the Design of Ontologies Used for Knowledge Sharing“, International Journal Human-Computer Studies 43, 1993, str. 907-928.

[16] Uschold, M., Gruninger, M., „Ontologies: Principles, Methods and Applications“ Knowledge Engineering Review, Volume 11, Number 2, June 1996.

[17] Uschold, M., Gruninger, M., „Ontologies and Semantics for Seamless Connectivity“, SIGMOD Record, Vol. 33, No. 4, December 2004, str. 58-64.

[18] Noy, N. F., McGuinness, D., „Ontology Development 101: A Guide to Creating Your First Ontology“, Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001, dostupno na: http://www.ksl.stanford.edu/people/dlm/papers/ontology-tutorial-noy-mcguinness-abstract.html (30. rujna. 2013.).

[19] Von Bertalanffy, L., „The History and Status of General Systems Theory“, The Academy of Management Journal, Vol. 15, No. 4, General Systems Theory (December 1972), str. 407-426, dostupno na: http://links.jstor.org/sici?sici=0001-427328197212%2915%3A4%3C407%3ATHASOG%3E2.O.C0%3B2-4 (30. rujna. 2013.).

[20] Laszlo, A., Krippner, S., „Systems Theories: Their Origins, Foundations, and Development“, in Systems Theories and A Priori Aspects of Perception, J. S. Jordan (Ed.), Amsterdam: Elsevier Science, 1998, Ch. 3, str. 47-74.

[21] Klaić, A., „Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies”, Proceedings of the International Convention MIPRO 2010, Opatija, Croatia, 2010, str. 136-141.

[22] Knapp, K.J., Morris, Jr. R.F., Marshall, T.E., Byrd, T.A., „Information security policy: An organizational-level process model“, Elsevier, Computers & Security 28 (2009), 2009, str. 493–508.

[23] Sherwood, J., Clark, A., Lynas, D., „Enterprise Security Architecture“, CMP Books, 2005.

[24] Von Roessing, R. M., „The Business Model for Information Security“, ISACA, 2010, dostupno na: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx (30. rujna. 2013.).

[25] Von Solms, R., Von Solms, S. H. (Basie), „Information Security Governance: A model based on the Direct–Control Cycle“, Elsevier, Computers & Security 25 (2006), 2006, str. 408–412.

[26] ISACA, „Control Objectives for Information and Related Technology (CoBIT)“, dostupno na: http://www.isaca.org/COBIT/Pages/default.aspx (30. rujna. 2013.).

[27] HRN ISO/IEC 27001:2005, dostupno na: http://www.hzn.hr ; ISO/IEC 27001:2005, http://www.iso.org (30. rujna. 2013.).

[28] Wang, J. A., Guo, M., „OVM: An Ontology for Vulnerability Management“, CSIIRW '09, April 13-15 2009, Oak Ridge, Tennessee, ACM.

[29] Kodeswaran, P., Kodeswaran, S.B., Joshi, A., Finin, T., „Enforcing security in semantics driven policy based networks“, Elsevier, Computer Standards & Interfaces (2010), 2010, doi:10.1016/j.csi.2010.03.010.

[30] Brinson, A., Robinson, A., Rogers, M., „A cyber forensics ontology: Creating a new approach to studying cyber forensics“, Elsevier, Digital Investigation, 3 S (2006), 2006, str. S37 – S43.

[31] Tsoumas, B., Gritzalis, D., „Towards an Ontology-based Security Management“, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA’06), IEEE, 2006, 1550-445X/06.

[32] Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina1, E., Toval, A., Piattini M., „A Systematic Review and Comparison of Security Ontologies“, The Third International Conference on Availability, Reliability and Security, IEEE, 2008, IEEE DOI 10.1109/ARES.2008.33.

[33] Nguyen, V., „Ontologies and Information Systems: A Literature Survey“, Australian Government, Defence Science and Technology Organisation – DSTO, June 2011, dostupno na: http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10144/1/DSTO-TN-1002%20PR.pdf (30. rujna. 2013.).

[34] Herzog, A., Shahmehri, N., Duma, C., „An Ontology of Information Security“, International Journal of Information Security and Privacy, Volume 1, Issue 4, 2007, str. 201-230.

[35] Fenz, S., Ekelhart, A., „Formalizing Information Security Knowledge“, ASIACCS'09, March 2009, Sydney, NSW, Australia, ACM, 2009, 2009 ACM 9781605583945/09/03.

[36] AURUM for Corporate Risk and Compliance Management, dostupno na: http://www.securityontology.com/ (30. rujna. 2013.).

[37] Cambridge University Press, „Cambridge Advanced Learner's Dictionary“, Second Edition, 2006.

[38] Anić, V., Brozović Rončević, D., Goldstein, I., Goldstein,S., Jojić, Lj., Matasović, R., Pranjković, I., „Hrvatski enciklopedijski rječnik“, Zagreb, 2004.

[39] Zakon o informacijskoj sigurnosti, NN 79/07, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/298919.html (30. rujna. 2013.).

[40] Brotby, W. K., „Information Security Management Metrics“, CRC Press, Auerbach, 2009.

[41] Arnason, S. T., Willet, K. D., „How to Achieve 27001 Certificate“, Auerbach Publications, 2008.

[42] National Institute of Standards and Technology (NIST), Special Publications (800 series), dostupno na: http://csrc.nist.gov/publications/PubsSPs.html (30. rujna. 2013.).

[43] Tatalović, S., Grizold, A., Cvrtila, V., „Suvremene sigurnosne politike“, GM - Tehnička knjiga, Zagreb, 2008.

[44] Peltier, T. R., „Information Security Policies and Procedures“, Auerbach Publications, 2004.

[45] Dunn, M., „A Comparative Analysis of Cybersecurity Initiatives Worldwide“, WSIS Thematic Meeting on Cybersecurity, ITU, June 2005, dostupno na: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (30. rujna. 2013.).

[46] Anderson, R., „Security Engineering“, Wiley, 2001.

[47] Harris, S., „CISSP All In One“, Third Edition, McGraw Hill/Osborne, 2005.

[48] Zakon o potvrđivanju sporazuma između stranaka Sjevernoatlantskog ugovora o sigurnosti podataka, NN MU 9/2009, 26.10.2009., dostupno na: http://narodne-novine.nn.hr/clanci/medunarodni/2009_10_9_113.html (30. rujna. 2013.).

[49] Commission communication COM(2005)229 final of 1 June 2005 to the Council (52005DC0229), the European Parliament, the European Economic and Social Committee and the Committee of the Regions on "i 2010 – a European Information Society for growth and employment", dostupno na: http://europa.eu/legislation_summaries/information_society/strategies/c11328_en.htm (30. rujna. 2013.).

[50] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, dostupno na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (30. rujna. 2013.).

[51] Council of Europe, Committee of Ministers, Recommendation Rec(2002)2 of the Committee of Ministers to Member States on Access to Official Documents (Adopted by the Committee of Ministers on 21 February 2002 at the 784th meeting of the Ministers' Deputies), dostupno na: https://wcd.coe.int/ViewDoc.jsp?id=262135 (30. rujna. 2013.).

[52] Nacionalni program informacijske sigurnosti (NPIS), Središnji državni ured za eHrvatsku (SDUeH), 2005., dostupno na: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-04-110.pdf (30. rujna. 2013.).

[53] Klaić, A., „Minimalni sigurnosni kriteriji i upravljanje rizikom informacijske sigurnosti", travanj 2010., FER, dostupno na: http://os2.zemris.fer.hr/ISMS/rizik/2010_klajic/SeminarskiRad_SRS_042010_AK.pdf (30. rujna. 2013.).

[54] Zakon o tajnosti podataka, NN 79/07, NN 86/2012, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_07_86_1969.html (30. rujna. 2013.).

[55] Common Criteria Standards ( ISO 15408), dostupno na: http://www.commoncriteriaportal.org/ (30. rujna. 2013.).

[56] Basel II, International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version, dostupno na: http://www.bis.org/publ/bcbs128.htm (30. rujna. 2013.).

[57] Rubin, M., „Asymmetrical Threat Concept and its Reflections on International Security", Strategic Research and Study Center, May 2007, dostupno na: http://www.meforum.org/1696/asymmetrical-threat-concept-and-its-reflections (30. rujna. 2013.).

[58] Klaić, A., Turek, F., „Nacionalna sigurnost i telekomunikacije“, Međunarodne studije, časopis za međunarodne odnose, vanjsku politiku i diplomaciju, II (2002), 4, 2002., str. 97-112.

[59] Uredba o mjerama informacijske sigurnosti, NN 46/08, 2008, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/339036.html (30. rujna. 2013.).

[60] Akerlof, G.A., “The Market for Lemons: Quality Uncertainty and Market Mechanism”, Quaterly Journal of Economics v 84, August 1970, str. 488-500.

[61] Anderson, R., University of Cambridge, Computer Laboratory, Economics and Security Resource Page, dostupno na: http://www.cl.cam.ac.uk/~rja14/econsec.html (30. rujna. 2013.).

[62] Anderson, R., Murdoch, S., Drimer, S., Bond, M., “Chip and Pin is Broken”, , 11. February 2010, dostupno na: http://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/ (30. rujna. 2013.).

[63] Odluka o primjerenom upravljanju informacijskim sustavom, HNB, NN 80/07, dostupno na: http://www.hnb.hr/propisi/odluke-nadzor-kontrola/odluke-zoki-ozujak-2010/h-odluka-primjereno-upravljanje-info-sustavom.pdf (30. rujna. 2013.).

[64] Pravilnik o tajnosti podataka obrane, MORH, NN 39/08, dostupno na: http://www.propisi.hr/print.php?id=7925 (30. rujna. 2013.).

[65] Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, HNB, ožujak 2006., dostupno na: http://www.hnb.hr/supervizija/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf (30. rujna. 2013.).

[66] Hrvatski zavod za norme (HZN), dostupno na: http://www.hzn.hr/ (30. rujna. 2013.).

[67] Internet Engineering Task Force (IETF), dostupno na: http://www.ietf.org/ (30. rujna. 2013.).

[68] Pfleeger, C. P., Pfleeger, S. L., „Security in Computing“, Prentice Hall, 2007.

[69] ISC$^2$ Code of Ethics, dostupno na: https://www.isc2.org/ethics/Default.aspx (30. rujna. 2013.)

[70] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, February 2013, dostupno na: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (2. studenog 2013.).

[71] Clapper, J.R., „How 9/11 Transformed the Intelligence Community, It's no longer about 'need to know.' Our guiding principle is 'responsibility to share.'“, The Wall Street Journal, 7. September 2011, dostupno na: http://online.wsj.com/news/articles/SB10001424053111904537404576554430822300352

(2. studenog 2013.).

[72] Katulić, T., „Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj“, Zagreb 2006., CARNet, dostupno na: http://bib.irb.hr/datoteka/529364.udzbenik1.pdf (2. studenog 2013.).

[73] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU), dostupno na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:EN:PDF (2. studenog 2013.).

[74] Zakon o potvrđivanju ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka, NN MU 9/06, dostupno na: http://narodne-novine.nn.hr/clanci/medunarodni/2006_10_9_109.html (2. studenog 2013.).

[75] Security Within the NATO, C-M(2002)49-COR9, 5 February 2013, dostupno na: http://www.nbu.cz/cs/pravni-predpisy/predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/ (2. studenog 2013.).

[76] Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga, NN 109/12, NN 33/13, NN 126/13, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_10_109_2379.html (2. studenog 2013.).

[77] Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka, NN 139/04, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2004_10_139_2433.html (2. studenog 2013.).

[78] Calder, A., Watkins, S. G., „Information Security Risk Management for ISO27001 / ISO17799“, IT Governance Publishing, 2007.

[79] Humphreys, E., „Implementing the ISO/IEC 27001 Information Security Management Standard“, Artech House, 2007.

[80] HM Treasury, The Orange Book – Management of Risk – Principles and Concepts, UK, October 2004, dostupno na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf (2. studenog 2013.).

[81] Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, UVNS, NN 30/11, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_03_30_654.html (2. studenog 2013.).

[82] Primary Directive on INFOSEC, NATO, AC/35-D/2004-REV2, 6 December 2010, dostupno na: http://www.nbu.cz/cs/pravni-predpisy/predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/ (2. studenog 2013.).

[83] Zakon o sigurnosnim provjerama, NN 85/08, NN 86/12, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_07_85_2729.html (2. studenog 2013.).

[84] Uredba o sadržaju, izgledu, načinu ispunjavanja i postupanju s upitnikom za sigurnosnu provjeru, NN 114/08, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_10_114_3300.html (2. studenog 2013.).

[85] National Institute of Standards and Technology, NIST, Special Publications, Information Security, Recommended Security Controls for Federal Information Systems, NIST SP 800-53, Revision 3, 1 May 2010, dostupno na: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (2. studenog 2013.).

[86] National Institute of Standards and Technology, „Standards for Security Categorization of Federal Information and Information Systems“, FIPS PUB 199, February 2004, dostupno na: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (2. studenog 2013.).

[87] National Institute of Standards and Technology, „Minimum Security Requirements for Federal Information and Information Systems“, FIPS PUB 200, March 2006, dostupno na: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (2. studenog 2013.).

[88] National Institute of Standards and Technology, NIST, Special Publications, Information Security, Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37, Revision 1, February 2010, dostupno na: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (2. studenog 2013.).

[89] The Committee on National Security Systems Instruction (CNSSI) No. 1253, „Security Categorization and Control Selection for National Security Systems”, CNSSI No. 1253, 15 March 2012, dostupno na: http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf (2. studenog 2013.).

[90] Jaquith, A., „Security Metrics“, Addison-Wesley, 2007.

[91] NSW Government, Department of Finance and Services, Australia, Information Security Guideline, Version 1.3, June 30, 2011, dostupno na:

http://www.finance.nsw.gov.au/sites/default/files/Information%20Security%20Guideline%202011.pdf (2. studenog 2013.).

[92] Fontanella-Khan , J., „Data protection ruled out of EU-US trade talks“, Financial Times, 4 November 2013, dostupno na: http://www.ft.com/cms/s/0/92a14dd2-44b9-11e3-a751-00144feabdc0.html#axzz2kNOoaQEL (4. studenog 2013.)

[93] European Commission, „Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century“, COM(2012) 9 final, Brussels, 25.1.2012, dostupno na: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf (4. studenog 2013.)

[94] Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008/977/JHA, 27 November 2008, dostupno na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0977:EN:NOT (4. studenog 2013.)

[95] Rules of Procedure on the Processing and Protection of Personal Data at EUROJUST, 2005/C 68/01, Text adopted unanimously by the college of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005, dostupno na: http://eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-EN.pdf (4. studenog 2013.)

[96] Sembhi, S., „Preparing for the New EU Data Protection Regulation“, IT in Europe, June 2012, Volume 2, Issue 5, str. 4-9.

[97] Schneier, B., „A Taxonomy of Social Networking Data“, IEEE Security & Privacy, July-August 2010, Volume 8, Issue 4, str 88.

[98] Unified Modeling Language Specification, Version 1.4.2, ISO/IEC 19501:2005(E), January 2005.

[99] Protégé Frames, The Stanford Center for Biomedical Informatics Research (BMIR) at the Stanford University School of Medicine, Version 3.4.7 (Build 620), 2011, dostupno na: http://protege.stanford.edu/ (2. studenog 2013.).

[100] Klaić, A., Golub, M., „Conceptual Modelling of Information Systems within the Information Security Policies”, International Conference on Computing and Business Management, ICCBM 2013, Paris, June 2013, published in Journal of Economics,

Business, and Management, JOEBM 2013 Vol.1(4), November 2013, ISSN: 2301-3567, str. 371-376, dostupno na: http://www.joebm.com/index.php?m=content&c=index&a=show&catid=33&id=349 (4. studenog 2013.).

[101] KATAKRI, The National Security Auditing Criteria, Finland, 2011, dostupno na: http://www.defmin.fi/en/administrative_branch/defence_security/national_security_auditing_criteria_(katakri) (4. studenog 2013.).

[102] Klaić, A., „Usporedba koncepata i metoda koje se koriste u područjima upravljanja informacijskim sustavima i upravljanja informacijskom sigurnošću“, lipanj 2010., FER, dostupno na: http://www.zpr.fer.hr/zpr/Portals/0/Predmeti/UIS/Koncepti%20i%20metode%20upravljanja%20IS.pdf (4. studenog. 2013.).

[103] Klaić, A., Golub, M., “Conceptual Information Modelling within the Contemporary Information Security Policies”, International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2013/ISS, Opatija, 2013, str. 1386-1391.

[104] Dillon, T., Chang, E., Hadzic, M., Wongthongtham, P., „Differentiating Conceptual Modelling from Data Modelling, Knowledge Modelling and Ontology Modelling and a Notation for Ontology Modelling“, APCCM 2008, Wollongong, NSW, Australia, January 2008, Vol. 79.

[105] ISO/IEC 27003:2010, „Information technology – Security techniques – Information security management system implementation guidance“, October 2010.

[106 ] ISO/IEC 27032:2012, „Information technology – Security techniques – Guidelines for cybersecurity“, July 2012.

[107] Commission Nationale de l'Informatique et des Libertes - CNIL, Methodology for Privacy Risk Management, dostupno na: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf (6. listopada 2013.).

[108] ITU-T, „Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002“, X.1051, February 2008.

[109] TheISO27k Forum, ISO 27001 Security Toolkit, dostupno na: http://www.iso27001security.com/html/iso27k_toolkit.html (6. listopada 2013.).

[110] National Institute of Standards and Technology, NIST SP_800-53_Rev-3_DB-R1.4.1-BETA, Reference Database for SP 800-53 2010, dostupno na: http://csrc.nist.gov/publications/PubsByLR.html (6. listopada 2013.).

[111] Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information (ANSSI), "Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS, Méthode de gestion des risques", 2010., dostupno na: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html (6. siječnja 2013.).

# **PRILOG A:** Domenska taksonomija informacijske sigurnosti - rječnik domene

| R.br. | **POJAM** | **OPIS PRIDRUŽENOG KONCEPTA (opći domenski koncepti)** |
|---|---|---|
| 1. | Informacijska sigurnost | *Željeno stanje povjerljivosti, cjelovitosti i raspoloživosti štićenih vrijednosti, koje se postiže organizacijskom podrškom i primjenom odgovarajućih mjera zaštite;* |
| 2. | Politika informacijske sigurnosti | *Skup procedura kojima se planira, ostvaruje, provodi i preispituje informacijska sigurnost u određenom opsegu primjene;* |
| 3. | Domena politike informacijske sigurnosti | *Obuhvaća politiku informacijske sigurnosti kroz životni ciklus (planiranje, ostvarenje, provođenje i preispitivanje) te globalno i lokalno sigurnosno okruženje organizacije koja provodi politiku informacijske sigurnosti;* |
| 4. | Opseg primjene politike informacijske sigurnosti | *Organizacijski entitet, ustrojstveni dio organizacije, informacijski sustav;* |
| 5. | Organizacijski entitet | *Organizacija koja provodi politiku informacijske sigurnosti ili organizacija koja surađuje;* |
| 6. | Regulativni zahtjev | *Sastoji se od taksonomije koja osigurava strukturirani pristup analizi i primjeni regulativnih zahtjeva kroz proces planiranja koji obuhvaća zakonske, sektorske i ugovorne zahtjeve;* |
| 7. | Povreda sigurnosti | *Svaka aktivnost ili neprovođenje mjera sigurnosti, protivno propisima, a koje je uzrokovalo ili može uzrokovati štetu za utvrđene štićene vrijednosti;* |
| 8. | Razdioba podataka | *Poslovna razdioba podataka koja se provodi u sklopu redovnih poslovnih aktivnosti organizacijskog entiteta ili javna razdioba podataka;* |
| 9. | Javna razdioba podataka | *Javna objava podataka, zahtjevi za javni pristup podatcima ili podatci nastali u kibernetičkom prostoru aktivnošću organizacijskog entiteta ili drugih subjekata;* |
| 10. | Proces nadzora | *Opća obilježja procesa nadzora kao vrsta, metode i opseg nadzora;* |
| 11. | Provedba nadzora | *Tipični procesi nadzora koji se koriste u različitim politikama i normama informacijske sigurnosti:akreditacija, certifikacija, nadzor/revizija;* |
| 12. | Akreditacija | *Odobrenje rada u segmentu poslovanja organizacije, čime organizacija preuzima odgovornost za poslovanje u skladu sa određenom normom ili politikom te odgovornost za rizike u ovom segmentu poslovanja;* |
| 13. | Certifikacija | *Sveobuhvatna procjena tehničkih, organizacijskih i administrativnih kontrola, kako bi se utvrdilo jesu li kontrole primijenjene sukladno normi kojom su propisane;* |
| 14. | Nadležno sigurnosno tijelo | *Sastoji se od taksonomije koja obuhvaća nacionalna i međunarodna tijela, razrade potrebnih hijerarhija nacionalnih sigurnosnih tijela, kao i tijela s koordinacijskim i operativnim zadaćama povezanim s područjem informacijske sigurnosti;* |
| 15. | Štićena vrijednost | *Obuhvaća podatke i druge poslovne vrijednosti za koje se osigurava zaštita sigurnosnih kriterija povjerljivosti, cjelovitosti i raspoloživosti;* |
| 16. | Podatak | *Zapis u obliku dokumenta ili nekom drugom obliku koji koriste politike i norme informacijske sigurnosti, a sastoji se od taksonomije koja obuhvaća podatke dominantne s obzirom na zahtjeve informacijske sigurnosti;* |
| 17. | Intelektualno vlasništvo | *Pravo na nematerijalnom objektu zaštite koje pravni poredak zemlje priznaje nositelju intelektualnog vlasništva, koje se za potrebe modeliranja promatra kao obilježje nematerijalnih vrijednosti (autorsko pravo, patent, žig, ...) ili kao podatak – štićenu vrijednost( poslovna tajna);* |
| 18. | Informacija | *Predstavlja podatak u kontekstu pojedine politike ili norme informacijske sigurnosti;* |
| 19. | Znanje | *Predstavlja organizirane informacije na domenskoj razini koje su na odgovarajući način pohranjene, kontrolirano distribuirane i pravno zaštićene (blisko konceptu intelektualnog vlasništva)* |
| 20. | Mudrost | *Viša razina razumijevanja o tome koje znanje se koristi s kojom namjerom, odnosno podrazumijeva dvije razine znanja, razinu poznavanja procedura i razinu razumijevanja razloga i načina korištenja procedura;* |
| 21. | Doseg utjecaja povreda sigurnosti | *Povezuje štićene vrijednosti definirane na razini organizacije s dosegom utjecaja koje povrede sigurnosti mogu imati na te štićene vrijednosti, a sastoji se od taksonomije usklađene s kategorijama štićenih vrijednosti;* |

| R.br. | POJAM | OPIS PRIDRUŽENOG KONCEPTA (opći domenski koncepti) |
|---|---|---|
| 22. | Kriteriji informacijske sigurnosti | *Predstavljaju svojstva štićenih vrijednosti koja se utvrđuju i štite sa stanovišta informacijske sigurnosti, a sastoje se od taksonomije koja se dijeli na sigurnosne, dodatne i ostale kriterije;* |
| 23. | Temeljni sigurnosni kriteriji | *Povjerljivost, cjelovitost i raspoloživost;* |
| 24. | Osoba | *Pripada organizacijskom entitetu kao zaposlenik tvrtke koja provodi politiku informacijske sigurnosti, ugovorni djelatnik ili zaposlenik ugovaratelja, a ima odgovarajuća obilježja i autorizacije;* |
| 25. | Unutarnja sigurnosna organizacija | *Skup sigurnosnih uloga koje organizacija koja provodi politiku informacijske sigurnosti treba utvrditi;* |
| 26. | Informacijski sustav (IS) | *Skup elemenata koji povezan u sustav ima novu funkcionalnost i vrijednost te podliježe posebnim pravilima politike informacijske sigurnosti (akreditacija/certifikacija, sustav/komponente, kategorije podataka);* |
| 27. | Sigurnosna uloga IS-a | *Obuhvaća obilježja IS-a bitna za politiku informacijske sigurnosti kao što su organizacijski elementi, pristup korisnika, otvorenost sustava, razvoj sigurnosne svijesti, edukacija i obuka;* |
| 28. | Dodatni elementi povjerenja u IS | *Obuhvaćaju obilježja kao što su sigurnosni način rada, interkonekcija, životni ciklus, kriteriji povjerenja otvorenosti sustava;* |
| 29. | Kibernetički prostor | *Suvremeno stanje informacijskog prostora koje uključuje široko korištenje informacijskih i komunikacijskih sustava te povezivanje različitih IS-ova i pohranjenih podataka u elektroničkom obliku putem Interneta* |
| 30. | Kibernetičke prijetnje | *Prijetnje povezane s kibernetičkim prostorom koje obuhvaćaju prijetnje korisnicima računala, prijetnje informacijskim sustavima i napredne metode kombiniranih prijetnji;* |
| 31. | Sigurnosni incidenti | *Sigurnosni incident obuhvaća sigurnosni napad i sigurnosni događaj koji se temelje na elementima taksonomije prema [13] (aktivnost, meta, alat, neovlašteni rezultat, napadač, motiv);* |
| 32. | Sigurnosna uloga objekata i prostora | *Obuhvaća ciljeve fizičke sigurnosti, čimbenike rizika i pristup fizičkoj zaštiti po dubini (slojevima);* |
| 33. | Zaštita klasificiranih podataka | *Specifičnosti politike informacijske sigurnosti državnog sektora prema područjima koja se koriste u dominantnim politikama informacijske sigurnosti državnih sektora (NATO, EU, zemlje članice);* |
| 34. | Sigurnosno certificiranje fizičkih osoba | *Vrsta certificiranja kao obvezujući uvjet pristupa klasificiranim podatcima u politikama informacijske sigurnosti državnog sektora;* |
| 35. | Klasificiranje podatka | *Utvrđivanje stupnja tajnosti određenog podatka koji se koristi u radu državnog sektora ili međunarodne organizacije, sukladno zakonom propisanim kriterijima klasificiranja;* |
| 36. | Minimalne sigurnosne mjere | *Utvrđuje svaka pojedina politika informacijske sigurnosti u državnom sektoru ili međunarodnoj organizaciji, kao jedan ili više skupova obaveznih sigurnosnih mjera koji se propisuje zakonom ili međunarodnim ugovorom;* |
| 37. | Evaluacija i odobravanje | *Različiti procesi određivanja razine povjerenja prema ključnim čimbenicima politika informacijske sigurnosti (osobe, procesi, tehnologija), temeljeni na određenoj vrsti provedbe nadzora;* |
| 38. | Sigurnosno certificiranje pravne osobe | *Vrsta certificiranja kao obvezujući uvjet pristupa klasificiranim podatcima u politikama informacijske sigurnosti državnog sektor za pravnu osobu koja sklapa klasificirani ugovor s državnim tijelom ili međunarodnom organizacijom;* |
| 39. | Klasificirani ugovor | *Ugovor između dvaju ili više ugovaratelja koji sadrži klasificirane podatke ili čija provedba zahtijeva pristup klasificiranim podatcima, pri čemu je naručitelj državno tijelo ili međunarodna organizacija koje je vlasnik klasificiranih podataka;* |
| 40. | Ranjivost | *Slabost ili nedostatak u nekom elementu ili sustavu u cjelini, koju može iskoristiti prijetnja; ranjivost može biti organizacijsko-proceduralna, fizička ili tehnička, a sustavska se odnosi na projektiranje, konfiguraciju ili ostvarenje;* |

| R.br. | POJAM | OPIS PRIDRUŽENOG KONCEPTA (opći domenski koncepti) |
|---|---|---|
| 41. | Prijetnja | *Potencijalni uzrok neželjenog incidenta koji može naštetiti sustavu ili organizaciji, koristi se sveobuhvatno viđenje prijetnji bilo da nastaju u okviru unutarnjih slabosti organizacije, zbog prirodnih nepogoda ili drugih vanjskih prijetnji, kao i uslijed namjernog ili nenamjernog postupanja ljudi, što obuhvaća generička podjela općih prijetnji na: otkaze (slučajne), nezgode (prirodne i okoliš) i napade (namjerne);* |
| 42. | Rizik | *Predstavlja vjerojatnost ostvarenja prijetnje koja iskorištava ranjivost i uzrokuje štetu organizaciji;* |
| 43. | Sigurnosne kontrole | *Sigurnosne zaštite za procijenjene sigurnosne rizike koje imaju obilježja kao što je način djelovanja i ostvarenja te osnovne ciljeve djelovanja na jedan ili više temeljnih sigurnosnih kriterija informacijske sigurnosti;* |
| 44. | Vrsta imovine | *Generička podjela štićenih vrijednosti (npr. objekti, sklopovlje, podatci i sl.) koja olakšava korištenje taksonomija ranjivosti i prijetnji te se povezuje sa stvarnom imovinom utvrđenom kao štićena vrijednost;* |
| 45. | Zaštita osobnih podataka | *Specifičnosti suvremenih zahtjeva zaštite osobnih podataka kao sigurnosnih zahtjeva politika informacijske sigurnosti (EU, zemlje članice i dr.);* |

**PRILOG B:** Hijerarhijska domenska taksonomija skupa dominantnih politika i normi informacijske sigurnosti

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| **PODSUSTAV PS1: DOMENA POLITIKE INFORMACIJSKE SIGURNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Domena politike informacijske sigurnosti | *Obuhvaća politiku informacijske sigurnosti kroz životni ciklus (planiranje, ostvarenje, provođenje i preispitivanje) te globalno i lokalno okruženje organizacije koja provodi politiku informacijske sigurnosti;* |
| 2. | • Organizacijski entitet | *Organizacija koja provodi politiku informacijske sigurnosti ili organizacija koja surađuje;* |
| 3. | • Organizacija provoditelj politike | *Organizacija koja provodi politiku informacijske sigurnosti;* |
| 4. | • Organizacija koja surađuje | *Organizacija koja surađuje u provedbi politike informacijske sigurnosti;* |
| 5. | • Vlasnik | *Vlasnik organizacijskog entiteta;* |
| 6. | • Rukovoditelj | *Rukovoditelj organizacijskog entiteta;* |
| 7. | • Ustrojstvena cjelina | *Ustrojstvena jedinica organizacijskog entiteta;* |
| **PODSUSTAV PS2: REGULATIVNA USKLAĐENOST** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Regulativni zahtjev | *Sastoji se od taksonomije koja osigurava strukturirani pristup analizi i primjeni regulativnih zahtjeva kroz proces planiranja koji obuhvaća zakonske, sektorske i ugovorne zahtjeve;* |
| 2. | • Zakonski zahtjev | *Planiranje i provedba informacijske sigurnosti obuhvaća niz zakonskih zahtjeva propisanih u različitim vrstama zakonskih i podzakonskih akata, odnosno međunarodnih ugovora;* |
| 3. | • Međunarodni ugovor | *Multilateralni i bilateralni sigurnosni međunarodni ugovori te međunarodni ugovori o resornoj suradnji koji su povezani s razmjenom klasificiranih podataka ili sa sigurnosnom suradnjom u različitim resorima;* |
| 4. | • Ekvivalentni stupnjevi tajnosti | *Međunarodni ugovor definira ekvivalentne nacionalne i međunarodne oznake tajnosti.* |
| 5. | • Regulativa odgovornosti | *Propisi ove vrste mogu biti unutarnji propisi organizacije (npr. dokumenti politike informacijske sigurnosti, politike prikladnog korištenja resursa i sl.) ili vanjski opći propisi poput zaštite na radu (Due Diligence - obveza kontinuiranog istraživanja i razumijevanja rizika s kojima se pravna osoba suočava, Due Care - obveza primjerene pažnje u provedbi sigurnosnih propisa);* |
| 6. | • Regulativa kibernetičke sigurnosti | *Obuhvaća: ekonomske aspekte, društvene aspekte, sigurnosne aspekte i obrambene aspekte.* |
| 7. | • Regulativa telekom sektora | *Sektor javnih elektroničkih usluga i infrastrukture, ekonomski aspekti upravljanja telekom sektorom, sektor telekoma kao sektor kritične infrastrukture, tajni nadzor i sl.;* |
| 8. | • Regulativa Internet sigurnosti | *Regulativa globalnog i lokalnog internetskog prostora, CERT hijerarhija i koordinacija i sl.* |
| 9. | • Regulativa privatnosti u kibernetičkom sektoru | *Privatnost u korištenju usluga raspoloživih u kibernetičkom prostoru, vezano za davatelje i korisnike usluga, zaštita komunikacija korisnika javnih usluga, zaštita osobnih podataka korisnika javnih usluga, zaštita mreža davatelja usluga;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 10. | • Regulativa kibernetičkog kriminala | *Kibernetički kriminal u smislu svih oblika računalnog kriminaliteta i druga područja poput terorizma ili korištenja kibernetičkog prostora za potrebe organiziranog kriminala;* |
| 11. | • Regulativa kritične infrastrukture | *Sektori kritične infrastrukture i podsektor kritične informacijske infrastrukture, nacionalni i EU propisi;* |
| 12. | • Regulativa posebnih podatkovnih domena | *Taksonomija regulative posebnih podatkovnih domena dominantnih s obzirom na zahtjeve informacijske sigurnosti prema [3];* |
| 13. | • Regulativa tajnosti podataka | *Zakonske definicije domena tajnih podataka;* |
| 14. | • Definicija i oznaka tajnosti | *Definicija i oznaka tajnosti zakonom i drugim aktima propisuje se za klasificirane podatke, osjetljive (službene) podatke i poslovnu tajnu;* |
| 15. | • Regulativa privatnosti | *Zakonske definicije domene osobnih podataka;* |
| 16. | • Regulativa osjetljivih podataka | *Zakonske definicije domene osjetljivih podataka (službeni podatci, privatnost pravnih osoba);* |
| 17. | • Regulativa intelektualnog vlasništva | *Zakonske definicije domene intelektualnog vlasništva (autorsko pravo, industrijsko vlasništvo, patent, žig, geografsko porijeklo, industrijski dizajn);* |
| 18. | • Sektorski zahtjev | *Sektorski regulativni zahtjevi propisani u različitim vrstama poslovne sektorske regulative, međunarodnih i nacionalnih normi;* |
| 19. | • Poslovna sektorska regulativa | *Regulativa primjenjiva, odnosno obvezujuća u nekom sektoru, npr. zaštitarstvo, financijske institucije i sl.;* |
| 20. | • Norme | *Koje se potiču ili su obavezne u nekom području poslovanja (npr. telekom sektor);* |
| 21. | • Ugovorni zahtjev | *Za potrebe politike informacijske sigurnosti razrađena je taksonomija ugovornih zahtjeva koja se sastoji od: klasificiranih ugovora, povjerljivih poslovnih ugovora (NDA), ugovora o razini usluge (SLA) te ostalih poslovnih ugovora.* |
| 22. | • Povjerljivi poslovni ugovor (NDA) | *Engl. Non-disclosure Agreement – NDA, bitni su za politike informacijske sigurnosti zbog povezanosti sa štićenim vrijednostima;* |
| 23. | • Ugovori o razini usluge (SLA) | *Engl. Service Level Agreements – SLA, bitni su za politike informacijske sigurnosti jer predstavljaju dio infrastrukture organizacije povezan sa štićenim vrijednostima i razdiobom podataka;* |
| 24- | • Ostali poslovni ugovori | *Mogu biti povezani s politikom informacijske sigurnosti (npr. ugovor s honorarnim zaposlenicima, ugovori o zaštiti objekta i slično);* |
| 25. | • Povreda sigurnosti | *Svaka aktivnost ili neprovođenje mjera sigurnosti, protivno propisima, a koje je uzrokovalo ili može uzrokovati štetu za utvrđene štićene vrijednosti;* |
| 26. | • Povreda sigurnosti bez štetnih posljedica | *Svaka aktivnost ili neprovođenje mjera sigurnosti, protivno propisima, a koje je moglo uzrokovati štetu za utvrđene štićene vrijednosti;* |
| 27. | • Stegovni postupak | *Za povredu sigurnosti bez štetnih posljedica provodi se stegovni postupak protiv odgovornih zaposlenika, a propisane kazne su vezane uz radno-pravni status;* |
| 28. | • Povreda sigurnosti sa štetnim posljedicama | *Svaka aktivnost ili neprovođenje mjera sigurnosti, protivno propisima, a koje je uzrokovalo štetu za utvrđene štićene vrijednosti;* |
| 29. | • Međunarodna povreda sigurnosti | *Moguća šteta po međunarodni klasificirani podatak ili prijetnja povjerljivosti, cjelovitosti i raspoloživosti međunarodnih klasificiranih podataka;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 30. | • Povreda nacionalne sigurnosti | *Moguća šteta po nacionalnu sigurnost ili prijetnja povjerljivosti, cjelovitosti i raspoloživosti klasificiranih podataka;* |
| 31. | • Poslovna povreda sigurnosti | *Moguća šteta poslovnim aktivnostima ili prijetnja povjerljivosti, cjelovitosti i raspoloživosti tajnih podataka pravne osobe;* |
| 32. | • Kazneni postupak | *Za povredu sigurnosti sa štetnim posljedicama provodi se kazneni postupak, a propisane kazne ovise o stupnju tajnosti i vrsti podataka te razini štete;* |
| **PODSUSTAV PS3: RAZDIOBA PODATAKA** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Razdioba podataka | *Poslovna razdioba podataka koja se provodi u sklopu redovnih poslovnih aktivnosti organizacijskog entiteta ili javna razdioba podataka;* |
| 2. | • Poslovna razdioba | *Razdioba podataka koja se provodi u sklopu redovnih poslovnih aktivnosti organizacijskog entiteta;* |
| 3. | • Interesna skupina | *Engl. Community of Interest – CoI, čine organizacijski entiteti upravitelja i članova interesne skupine (pravne osobe);* |
| 4. | • Domena razdiobe | *Domena podataka od interesa i razlog razdiobe, ograničeno je regulativnim zahtjevima i pravilima interoperabilnosti;* |
| 5. | • Pravila interoperabilnosti | *Obuhvaćaju obilježja interesne skupine, domene razdiobe i operativnih zahtjeva korištenja;* |
| 6. | • Organizacijska pravila | *Obuhvaćaju nadležna tijela (interesna skupina) i fizičke osobe- korisnike u tim tijelima, kao i obilježja domene razdiobe u smislu pristupa i korištenja;* |
| 7. | • Semantička pravila | *Obuhvaćaju značenje podataka za korisnike, kao i podatkovnih struktura za informacijske sustave;* |
| 8. | • Tehnička pravila | *Obuhvaćaju podatkovne protokole i tehnologije povezivanja;* |
| 9. | • Javna razdioba | *Javna objava podataka, zahtjevi za javni pristup podatcima ili podatci nastali u kibernetičkom prostoru aktivnošću organizacijskog entiteta ili drugih subjekata;* |
| 10. | • Javna objava | *Engl. Public Disclosure, u javnom informacijskom prostoru;* |
| 11. | • Vlastita objava | *Intencija vlasnika podataka vezana za podatke koji nisu klasificirani ili su prethodno deklasificirani;* |
| 12. | • Neovlaštena objava | *Kazneno djelo ili stegovni prijestup, ovisno o vrsti podataka.* |
| 13. | • Javni pristup | *Engl. Public Release, predstavlja uvid javnosti u podatak;* |
| 14. | • Pravo na pristup informacijama | *Engl. Freedom of Information – FOI, realizira se na temelju suglasnosti vlasnika podatka ili odluke povjerenika, uz prethodnu deklasifikaciju;* |
| 15. | • Sudski proces | *Oblik međusektorske suradnje različitih stupova vlasti, odnosno pravnih osoba – vlasnika podataka i fizičkih osoba – zaposlenika (sudski procesi, istražne radnje, svjedočenja i sl.)* |
| 16. | • Nastali podatci | *U javnoj domeni u sklopu aktivnosti organizacijskog entiteta ili aktivnosti drugih subjekata, predlaže se modifikacija taksonomije iz [97];* |
| 17. | • Povjereni podatci | *Engl. Entrusted Data, vlasnik nema kontrolu nad tim podatcima jer ih je povjerio drugim subjektima (korištenje usluga kroz SLA ugovore, društvene mreže i sl.);* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 18. | • Podatci o ponašanju | *Engl. Behavioral Data, prikupljeni na web mjestu ili kod davatelja usluge/infrastrukture (odnose se i na pravne osobe s SLA ugovorima s operatorima);* |
| 19. | • Slučajni podatci | *Engl. Incidental Data, slučajno nastali o nekomu/nečemu u okviru drugih podataka/tema;* |
| 20. | • Izvedeni podatci | *Engl. Derived Data, iz drugih javno dostupnih podataka analizom i zaključivanjem;* |
| **PODSUSTAV PS4: NADZOR INFORMACIJSKE SIGURNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Proces nadzora | *Opća obilježja procesa nadzora kao vrsta, metode i opseg nadzora;* |
| 2. | • Metoda | *Sustav praksi, tehnika, procedura i pravila,odnosno skup smjernica i principa, kao i specifičan pristup, predlošci i obrasci koji se koriste u procesu nadzora;* |
| 3. | • Procjena | *Engl. Assesment, obavlja se kao kvalificirana revizija u određenom funkcionalnom području za potrebe nekog organizacijskog entiteta (npr. procjena ranjivosti, procjena rizika i sl.);* |
| 4. | • Inspekcija | *Dio nadzora/revizije, a podrazumijeva neposredan uvid u proces, objekt, podatke ili opremu od interesa, i to u definiranom trenutku ili periodičnim intervalima;* |
| 5. | • Ispitivanje | *Metoda koja može biti primijenjena u sklopu procesa nadzora ili odvojeno (npr. penetracijsko ispitivanje), a najčešće je ograničeno na IS pri čemu nepronalaženje ranjivosti ne implicira sigurnost sustava;* |
| 6. | • Opseg | *Može biti organizacija ili jedan samostalno definirani dio organizacije, odnosno informacijski sustav ili jedan logički i organizacijski samostalni dio informacijskog sustava;* |
| 7. | • Vrsta | *S obzirom na status izvršitelja nadzora;* |
| 8. | • Unutarnji | *Ima izvršitelje koji su zaposlenici nadzirane organizacije;* |
| 9. | • Vanjski | *Ima izvršitelje koji su zaposlenici nezavisne pravne osobe;* |
| 10. | • Provedba nadzora | *Tipični procesi nadzora koji se koriste u različitim politikama i normama informacijske sigurnost;* |
| 11. | • Akreditacija | *Odobrenje rada u segmentu poslovanja organizacije, čime organizacija preuzima odgovornost za poslovanje u skladu sa određenom normom ili politikom te odgovornost za rizike u ovom segmentu poslovanja;* |
| 12. | • Certifikacija | *Sveobuhvatna procjena tehničkih, organizacijskih i administrativnih kontrola, kako bi se utvrdilo jesu li kontrole primijenjene sukladno normi kojom su propisane;* |
| 13. | • ISO 27001 certifikacija | *Formalni postupak certifikacije koji provodi akreditirana institucija sukladno zahtjevima norme;* |
| 14. | • Nadzor/revizija | *Engl. Audit, sastoji se od evaluacije sustava sigurnosnih procesa i kontrola, a provodi se u skladu s određenom normom ili definiranim skupom dokumentiranih procedura (kvalificirano procjenjivanje);* |
| 15. | • Unutarnji nadzor/revizija | *Provode zaposlenici same organizacije koja je predmet nadzora, kroz poseban odjel ili povjerenstvo sastavljeno od zaposlenika, u skladu s određenom normom ili skupom dokumentiranih procedura i s ciljem internog procjenjivanja stanja u organizaciji;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 16. | • ISO 27001 unutarnja revizija | *Postupak provjere provedbe zahtjeva norme u okviru pristupa kroz unutarnju reviziju;* |
| **PODSUSTAV PS5: ORGANIZACIJSKI OKVIR** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Nadležno sigurnosno tijelo | *Sastoji se od taksonomije koja obuhvaća nacionalna i međunarodna tijela, razradu potrebnih hijerarhija nacionalnih sigurnosnih tijela, kao i tijela s koordinacijskim i operativnim zadaćama povezanim s područjem informacijske sigurnosti;* |
| 2. | • Nadležno međunarodno sigurnosno tijelo | *Sigurnosno tijelo NATO-a i EU-a u multilateralnoj međunarodnoj suradnji, kao i NSA tijela drugih država u okviru bilateralne međudržavne suradnje (npr. gospodarska suradnja i klasificirani ugovori);* |
| 3. | • Nadležno nacionalno sigurnosno tijelo | *Nadležno nacionalno sigurnosno tijelo sastoji se od više hijerarhija i skupina tijela nadležnih u području informacijske sigurnosti ili povezanim sigurnosnim područjima;* |
| 4. | • NSA hijerarhija/tijelo | *NSA hijerarhiju tijela predstavlja središnje državno tijelo koje ima nadležnost za politiku informacijske sigurnosti (Engl. National Security Authority – NSA), prema [73, 75], nadležno za politiku informacijske sigurnosti i koordinaciju svih drugih tijela s nacionalnim nadležnostima u području informacijske sigurnosti državnog sektora.* |
| 5. | • DSA funkcionalnost | *Engl. Designated Security Authority - DSA, nadležnost za politiku sigurnosti poslovne suradnje;* |
| 6. | • Funkcionalnost sigurnosnih provjera | *Nadležnost za provedbu sigurnosnih provjera fizičkih i pravnih osoba;* |
| 7. | • Sustav registara | *Nacionalni sustav registara za distribuciju međunarodnih klasificiranih podataka;* |
| 8. | • Središnji registar | *Centralizirani prijem i distribucija svih međunarodnih klasificiranih podataka te koordinacija rada nacionalnog Sustava registara;* |
| 9. | • Sastavnice sustava registara | *Ustrojavaju se u državnim tijelima ili pravnim osobama s međunarodnim klasificiranim ugovorima, u svrhu unutarnje distribucije podataka;* |
| 10. | • NCSA/IAA funkcionalnost | *Engl. National Communications Security Authority / Information Assurance Authority, nadležnost za politikuinformacijske sigurnosti IS-ova;* |
| 11. | • SAA funkcionalnost | *Engl. Security Accreditation Authority – SAA, nadležnost za sigurnosnu akreditaciju klasificiranih IS-ova;* |
| 12. | • CDA/NDA funkcionalnost | *Engl. Crypto Distribution Authority – CDA/National Distribution Authority – NDA, nadležnost distribucije kriptografske opreme i materijala;* |
| 13. | • CAA funkcionalnost | *Engl. Crypto Approval Authority – CAA, nadležnost odobravanja kriptografske opreme;* |
| 14. | • TA funkcionalnost | *Engl. TEMPEST Authority –TA, nadležnost certifikacije IT opreme i fizičkog prostora od neželjenog elektromagnetskog zračenja;* |
| 15. | • Vojna teklićka služba | *Engl. Military Courier Service, u okviru Ministarstva obrane, uobičajeno se koristi za distribuciju kriptografskog materijala i veće međunarodne pošiljke klasificiranih podataka;* |
| 16. | • Akreditacijsko-certifikacijsko tijelo | *Nadležno za provedbu različitih postupaka akreditacije i/ili certifikacije (međunarodne ili nacionalne norme i/ili regulativa), ovlaštena zakonom ili putem nadležnog normizacijskog tijela;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 17. | • Funkcionalnost certifikacije e-potpisa | *Engl. Certificate Authority – CA, nadležnost usluge izdavanja/verificiranja e-potpisa;* |
| 18. | • Nacionalna CERT hijerarhija/tijelo | *Nacionalna CERT hijerarhija predstavlja nacionalno CERT tijelo koje koordinira rad tijela u CERT hijerarhiji i povezuje tu hijerarhiju s nadležnim međunarodnim CERT tijelima, odnosno NSA hijerarhijom i drugim sigurnosnim tijelima;* |
| 19. | • CERT funkcionalnost državnog tijela | *CERT funkcionalnost za državni sektor;* |
| 20. | • Vladin CERT | *Zadužen za zajedničku informacijsku i komunikacijsku infrastrukturu državnog sektora;* |
| 21. | • CERT državnog tijela | *CERT-ovi pojedinih državnih tijela zaduženi za vlastitu komunikacijsku i informacijsku infrastrukturu državnog tijela (npr. CERT Ministarstva obrane);* |
| 22. | • CERT funkcionalnost pravne osobe | *CERT funkcionalnost privatne tvrtke, obično se realizira kroz manje timove zaposlenika u tvrtkama koje imaju značajnije poslovanje u kibernetičkom prostoru (financijski sektor, sektor el. usluga i sl.);* |
| 23. | • Nacionalno koordinacijsko i operativno tijelo | *Tijela koja nisu direktno u NSA hijerarhiji, a imaju koordinacijsku ili operativnu ulogu u područjima povezanim s područjem informacijske sigurnosti;* |
| 24. | • Tijelo za zaštitu osobnih podataka | *Nadležno za nacionalne okvire i za EU okvire u zemljama članicama te za suradnju s međunarodnim nadležnim tijelima;* |
| 25. | • Tijelo za upravljanje krizama | *Na nacionalnoj razini koordinacijom različitih nadležnih tijela;* |
| 26. | • Tijelo koordinator kibernetičke sigurnosti | *Tijelo koordinator kibernetičke sigurnosti (ekonomski, društveni, sigurnosni ili obrambeni aspekti) prema nadležnim tijelima kao što su resorna ministarstva, sektorske regulatorne agencije ili sigurnosna tijela;* |
| 27. | • Tijelo koordinator kritične infrastrukture | *Uobičajeno se organizira u okviru sektorskog pristupa u određenom gospodarskom području (npr. financijski sektor ili promet), a koordinacijska tijela su resorna ministarstva, regulatorne agencije, odnosno druga sigurnosna i koordinacijska tijela, ovisno o specifičnostima pojedinog sektora;* |
| 28. | • Normizacijsko tijelo | *Nacionalno normizacijsko tijelo koje preuzima relevantne međunarodne i EU norme te provodi proces nacionalne normizacije;* |
| **PODSUSTAV PS6: DEFINICIJA PODATAKA I DRUGIH VRIJEDNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Štićena vrijednost | *Obuhvaća podatke i druge poslovne vrijednosti za koje se osigurava zaštita sigurnosnih kriterija povjerljivosti, cjelovitosti i raspoloživosti;* |
| 2. | • Nematerijalna imovina | *Engl. Intangible Assets, koristi atribut intelektualnog vlasništva;* |
| 3. | • Usluge | *Primarno komunikacijske i informacijske usluge te druge usluge od značaja za politiku informacijske sigurnosti;* |
| 4. | • Programska podrška | *Operativni sustavi, programske aplikacije te ostala programska podrška (razvojna, uslužna, ...);* |
| 5. | • Ostale nematerijalne vrijednosti | *Obuhvaćaju ugled i imidž organizacije te druge interno utvrđene vrijednosti organizacije;* |
| 6. | • Podatak | *Predlaže se taksonomija podataka prema kriterijima informacijske sigurnosti i kriteriju službenog postupanja;* |
| 7. | • Javno dostupan podatak | *Kao npr. web mjesto, propagandni materijali, s kriterijima: cjelovitost, raspoloživost;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 8. | • Osobni podatak | *Kao npr. podatci o zaposlenicima, klijentima, s kriterijima: cjelovitost, privatnost;* |
| 9. | • Osjetljivi podatak | *Podatci za interno i službeno korištenje (označeni neklasificirani podatci, interni podatci i sl.), s kriterijima: cjelovitost, raspoloživost, službeno postupanje (engl. Need-to-Know);* |
| 10. | • Povjerljivi podatak | *Kao npr. poslovno osjetljivi podatci, ili klasificirani podatci najnižeg stupnja tajnosti (OGR), s kriterijima: cjelovitost, raspoloživost, povjerljivost (tajnost) na užoj razini djelovanja i aktivnosti pravne osobe, službeno postupanje;* |
| 11. | • Vrlo povjerljivi podatak | *Kao npr. poslovna tajna, nacionalno relevantni klasificirani podatci razine POV, s kriterijima: cjelovitost, raspoloživost i povjerljivost (tajnost), službeno postupanje te sigurnosni certifikat za klasificirane podatke;* |
| 12. | • Klasificirani podatak posebne odgovornosti | *Za koji se postavljaju dodatne mjere kontrole osoba koje ih koriste ili imaju uvid u njih, uobičajeno dva najviša stupnja tajnosti klasificiranih podataka (VT, T), s kriterijima: cjelovitost, raspoloživost i povjerljivost (tajnost) na najvišoj nacionalnoj razini, službeno postupanje i sigurnosni certifikat te osobna odgovornost i sljedivost aktivnosti;* |
| 13. | • Materijalna imovina | *Obuhvaća pokretnu i nepokretnu imovinu važnu za politiku informacijske sigurnosti;* |
| 14. | • Objekti i prostori | *Predstavljaju nepokretnu imovinu (engl.Fixed Assets);* |
| 15. | • Fizička imovina | *Predstavlja pokretnu imovinu (engl. Current Assets),odnosno fizičku opremu u inventurnoj listi;* |
| 16. | • Doseg utjecaja povreda sigurnosti | *Povezuje štićene vrijednosti definirane na razini organizacije s dosegom utjecaja koje povrede sigurnosti mogu imati na te štićene vrijednosti, a sastoji se od taksonomije usklađene s kategorijama štićenih vrijednosti;* |
| 17. | • Međunarodni doseg | *Štićena vrijednost je definirana određenim međunarodnim ugovorom i povreda sigurnosti ima međunarodni doseg;* |
| 18. | • Nacionalni doseg | *Štićena vrijednost je definirana određenim nacionalnim zakonima i povreda sigurnosti ima nacionalni doseg (nacionalna sigurnost);* |
| 19. | • Kritična infrastruktura | *Štićena vrijednost je definirana određenim nacionalnim ili međunarodnim propisima kao kritična infrastruktura i povreda sigurnosti ima nacionalni ili međunarodni doseg;* |
| 20. | • Pravna osoba | *Štićena vrijednost je definirana određenim propisima i povreda sigurnosti ima doseg na razini pravne osobe (npr. osjetljivi podatak);* |
| 21. | • Fizička osoba | *Štićena vrijednost je osobni podatak;* |
| **PODSUSTAV PS7: KRITERIJI INFORMACIJSKE SIGURNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Kriteriji informacijske sigurnosti | *Predstavljaju svojstva štićenih vrijednosti koja se utvrđuju i štite sa stanovišta informacijske sigurnosti, a sastoje se od taksonomije koja se dijeli na sigurnosne, dodatne i ostale kriterije;* |
| 2. | • Temeljni sigurnosni kriteriji | *Povjerljivost, cjelovitost i raspoloživost;* |
| 3. | • Povjerljivost | *Svojstvo štićene vrijednosti koja nije učinjena raspoloživom ili nije otkrivena neovlaštenim pojedincima, entitetima, ili procesima;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 4. | • Privatnost | *Promatra se kao vrstu povjerljivosti u postupanju s podatcima za fizičke i pravne osobe, koja traži službeno postupanje i primjenu odgovarajućih mjera zaštite podataka (osobni podatci, osjetljivi podatci);* |
| 5. | • Cjelovitost | *Svojstvo točnosti i potpunosti štićene vrijednosti (podatak, sustav);* |
| 6. | • Autentičnost | *Kriterij povezan s cjelovitošću u slučaju elektroničkih usluga i identiteta (autentifikacija), kada i gdje može biti primjenjiv (potvrda vjerodostojnosti korisničkog identiteta);* |
| 7. | • Neporecivost | *Kriterij povezan s cjelovitošću u slučaju elektroničkih usluga i identiteta, kada i gdje može biti primjenjiv (potvrđuje da je određena transakcija napravljena u određeno vrijeme i na određenoj logičkoj lokaciji);* |
| 8. | • Raspoloživost | *Svojstvo štićene vrijednost koja je dohvatljiva i iskoristiva na zahtjev ovlaštenog entiteta (osoba, proces);* |
| 9. | • Dodatni kriteriji | *Povezani s korištenjem visokih razina povjerljivosti;* |
| 10. | • Odgovornost | *Vezana za aktivnosti i sukladna zahtjevima razine povjerljivosti podataka koji se koriste u toj aktivnosti, a primjenjuje se na osobe i uvodi zahtjeve posebnih sigurnosnih mjera ili kontrola za osobe koje pristupaju takvim podatcima (npr. najviši stupnjevi tajnosti ili posebne kategorije klasificiranih podataka);* |
| 11. | • Sljedivost | *Vezana za aktivnosti i sukladna zahtjevima razine povjerljivosti podataka koji se koriste u toj aktivnosti, a primarno se odnosi na poslovne proces;* |
| 12. | • Ostali kriteriji | *Ostali kriteriji sastoje se od grupa kriterija povjerenja i kvalitete koje ne proizlaze direktno iz informacijske sigurnosti, ali se koriste i u ovom području;* |
| 13. | • Kriteriji povjerenja | *Engl. Fiduciary Criteria, u određenom ostvarenju podrazumijevaju usklađenost i pouzdanost rješenja.* |
| 14. | • Sukladnost | *U odnosu na definiranu normu;* |
| 15. | • Pouzdanost | *U odnosu na postavljene zahtjeve;* |
| 16. | • Kriteriji kvalitete | *Engl. Quality Criteria, u određenom ostvarenju podrazumijevaju učinkovitost i uspješnost rješenja;* |
| 17. | • Učinkovitost | *Izvršenje zadanih zahtjeva;* |
| 18. | • Uspješnost | *Izvršenje zadanih zahtjeva uz kriterij optimalnosti;* |
| **PODSUSTAV PS8: DEFINICIJA OSOBA** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Sigurnosna uloga osoba | *Odnosi se na sve vrste osoba u vezi sa štićenim vrijednostima;* |
| 2. | • Osoblje | *Koje radi u nekoj organizaciji i ima status zaposlenika ili vanjskog suradnika (zaposlenik ugovaratelja ili ugovorna osoba - honorarac);* |
| 3. | • Obilježja osobe | *Osnovna obilježja osoba kao državljanstvo, kvalifikacije, vještine, radno iskustvo;* |
| 4. | • Status osobe | *U organizaciji može biti zaposlenik na radnom mjestu, osoba na ugovoru o djelu, zaposlenik ugovaratelja;* |
| 5. | • Zahtjevi povjerenja u osobe | *Poslovna potreba pristupa određenim podatcima (Need-to-Know), ovlaštenje za kategorije podataka s obzirom na povjerljivost, sigurnosni uvjeti (certifikat), drugi ugovorni zahtjevi;* |
| 6. | • Osoba | *Pripada organizacijskom entitetu kao zaposlenik tvrtke koja provodi politiku informacijske sigurnosti, ugovorni djelatnik ili zaposlenik ugovaratelja, a ima odgovarajuća obilježja i autorizacije;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 7. | • Unutarnja sigurnosna organizacija | *Skup sigurnosnih uloga koje organizacija koja provodi politiku informacijske sigurnosti treba utvrditi;* |
| 8. | • Vlasnik podataka i drugih vrijednosti | *Rukovoditelj organizacijskog entiteta koji može delegirati nadležnosti na niže razine;* |
| 9. | • Savjetnik za informacijsku sigurnost | *Općenito rukovoditelj sigurnosti, odnosno CISO, LISO, CIO, CSO i slično;* |
| 10. | • Delegirani upravitelj podataka/rizika | *Optimalno pozicioniran nositelj odgovornosti za pojedine poslovne segmente podataka po funkcionalnoj logici ili u smislu decentraliziranog upravljanja podružnicama ili operacijama (npr. službenik za zaštitu osobnih podataka u pravnim osobama;* |
| 11. | • Ostale sigurnosne uloge | *Specijalističke sigurnosne uloge kao vlasnik IS-a, administrator poslužitelja / mreže / sigurnosti, čuvari / zaštitari / portiri i sl.* |
| **PODSUSTAV PS9: DEFINICIJA INFORMACIJSKIH SUSTAVA (IS)** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Sigurnosna uloga IS-a | *Obuhvaća obilježja IS-a bitna za politiku informacijske sigurnosti kao što su organizacijski elementi, pristup korisnika, otvorenost sustava, razvoj sigurnosne svijesti, edukacija i obuka;* |
| 2. | • Organizacijski elementi IS-a | *Kroz pridruživanje sigurnosnih odgovornosti za IS te utvrđivanje potrebne razine povjerljivosti IS-a na temelju kategorija podataka koje se koriste na IS-u, a s obzirom na različite domene podataka prema PS6;* |
| 3. | • Sigurnosni kriteriji pristupa korisnika | *Obuhvaćaju zahtjeve povjerenja u korisnike, zahtjeve poslovnog procesa s obzirom na potrebe pristupa podatcima te autorizaciju korisnika;* |
| 4. | • Sigurnosni kriteriji otvorenosti sustava | *Obuhvaćaju razine povjerenja koje se definiraju ovisno o vlasništvu infrastrukture, usluga i profilu korisnika prema [100];* |
| 5. | • Razvoj sigurnosne svijesti, edukacija i obuka | *Provedba programa po organizacijskim i funkcionalnim razinama;* |
| 6. | • Informacijski sustav | *Skup elemenata koji povezan u sustav ima novu funkcionalnost i vrijednost te podliježe posebnim pravilima politike informacijske sigurnosti (akreditacija/certifikacija, sustav/komponente, kategorije podataka);* |
| 7. | • Klasificirani informacijski sustav | *IS na kojem se koriste klasificirani podatci;* |
| 8. | • Kibernetički prostor | *Suvremeno stanje informacijskog prostora koje uključuje široko korištenje informacijskih i komunikacijskih sustava te povezivanje različitih IS-ova i pohranjenih podataka u elektroničkom obliku putem Interneta;* |
| 9. | • Dimenzija kibernetičkog prostora | *Predlaže se korištenje četiri ključne dimenzije: društvena, ekonomska, sigurnosna i obrambena, kao i utvrđivanje nacionalnih organizacijskih nadležnosti u kibernetičkom prostoru;* |
| 10. | • Kibernetičke prijetnje | *Prijetnje povezane s kibernetičkim prostorom koje obuhvaćaju prijetnje korisnicima računala, prijetnje informacijskim sustavima i napredne metode kombiniranih prijetnji;* |
| 11. | • Prijetnje korisnicima računala | *Obuhvaćaju socijalni inženjering te elektroničke prijevare korisnika (Phishing, Spaming, Hoaxes - chain letters, scams, ... );* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 12. | • Napredne metode prijetnji | *Predstavljaju kombinaciju prijetnji korisnicima računala i prijetnji informacijskim sustavima (npr. Advanced Persisting Threats - APT);* |
| 13. | • Prijetnje informacijskim sustavima | *Koriste taksonomiju prema [13] koja obuhvaća sigurnosni: događaj, napad i incident;* |
| 14. | • Sigurnosni događaj | *Sadrži aktivnost i metu;* |
| 15. | • Sigurnosni napad | *Sadrži uz sigurnosni događaj i proširenje na alat i neovlašteni rezultat;* |
| 16. | • Sigurnosni incident | *Sadrži, uz sigurnosni napad i događaj, proširenje na napadača i motiv;* |
| 17. | • Taksonomija sigurnosnih incidenata | *Prema [13] obuhvaća: aktivnost, meta, alat za iskorištavanje ranjivosti, ranjivost sustava, neovlašteni rezultat, napadač, motiv;* |
| 18. | • Aktivnost | *Korak koji poduzima osoba ili proces s namjerom postizanja nekog rezultata kao što je npr. preplavljivanje (engl. Flood), lažiranje izvorišnih adresa (engl. Spoofing), skeniranje, ili autentifikacija;* |
| 19. | • Meta | *Računalo, mrežni logički (račun, proces, podatak) ili fizički entitet (komponenta, računalo, mreža);* |
| 20. | • Alat za iskorištavanje ranjivosti | *Sredstva za iskorištavanje računalne ili mrežne ranjivosti;* |
| 21. | • Ranjivost sustava | *Slabost ili nedostatak u nekom sustavu koji može iskoristiti prijetnja;* |
| 22. | • Neovlašteni rezultat | *Neovlaštena posljedica nekog događaja;* |
| 23. | • Napadač | *Osoba koja pokušava jedan ili više napada kako bi ostvario neki cilj;* |
| 24. | • Motiv | *Razlog ili konačni cilj nekog incidenta;* |
| **PODSUSTAV PS10: DEFINICIJA FIZIČKE SIGURNOSTI** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Sigurnosna uloga objekata i prostora | *Obuhvaća ciljeve fizičke sigurnosti, čimbenike rizika i pristup fizičkoj zaštiti po dubini (slojevima);* |
| 2. | • Ciljevi fizičke sigurnosti | *Predstavljaju obilježja slojeva fizičke sigurnosti i sigurnosnih mjera / kontrola u smislu odvraćanja, sprečavanje, detektiranja ili usporavanja neovlaštenog ulaska u štićene prostore i objekte;* |
| 3. | • Čimbenici rizika | *Razina povjerljivosti i kategorija podataka, količina i oblik podataka i drugih vrijednosti, okruženje objekta i prostora;* |
| 4. | • Fizička zaštita po dubini | *Engl. Defence in depth, obuhvaća perimetar, slojeve fizičke zaštite, sigurnosne prostore;* |
| 5. | • Perimetar | *Vanjski fizički perimetar* |
| 6. | • Slojevi fizičke zaštite | *Obuhvaćaju unutarnji perimetar, objekte i prostore unutar objekta;* |
| 7. | • Sigurnosni prostori | *Imaju poseban sigurnosni status povezan s razinom povjerljivosti i kategorijama podataka koji se u njima koriste;* |
| **PODSUSTAV PS11: ZAŠTITA KLASIFICIRANIH PODATAKA** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Zaštita klasificiranih podataka | *Specifičnosti politike informacijske sigurnosti državnog sektora prema područjima koja se koriste u dominantnim politikama informacijske sigurnosti državnih sektora (NATO, EU, zemlje članice), prema [39, 54, 73, 75, 83];* |
| 2. | • Nadzor zaštite klasificiranih podataka | *Provodi se u svim tijelima i pravnim osobama koje trajno ili povremeno u svom radu koriste klasificirane podatke;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 3. | • Unutarnji nadzor zaštite klasificiranih podataka | *Provode tijela i pravne osobe (savjetnik za informacijsku sigurnost) koje trajno ili povremeno u svom radu koriste klasificirane podatke;* |
| **PODSUSTAV PS12: SIGURNOST OSOBLJA** | | |
| 1. | • Zahtjevi sigurnosti osoblja | *Obuhvaćaju koncepte u odgovornosti poslodavca, odnosno tijela koje provodi politiku informacijske sigurnosti i koncepte u odgovornosti vanjskih tijela (proces certificiranja osoba);* |
| 2. | • Popis dužnosti i poslova za certificiranje | *Organizacijski entitet mora utvrditi i redovito održavati popis dužnosti i poslova za koje se zahtijeva certificiranje zaposlenika;* |
| 3. | • Upitnik za sigurnosnu provjeru | *Vlastoručno popunjava osoba koja se certificira, a upitnici se razlikuju u detaljima za svaki pojedini stupanj tajnosti (obrazac u referentnom propisu);* |
| 4. | • Vrsta certifikata | *Za uporabu u nacionalnom i međunarodnom okruženju, odnosno u okviru međunarodnih organizacija (NATO, EU);* |
| 5. | • Razina certifikata | *Usklađena s propisanim stupnjevima tajnosti prema vrsti certifikata;* |
| 6. | • Sigurnosno informiranje | *Provodi se prilikom prvog certificiranja, periodično i završno, a obuhvaća upoznavanje s pravima i obvezama korištenja klasificiranih podataka;* |
| 7. | • Proces certificiranja osoba | *Vrsta certificiranja kao obvezujući uvjet pristupa klasificiranim podatcima u politikama informacijske sigurnosti državnog sektora;* |
| **PODSUSTAV PS13: FIZIČKA SIGURNOST** | | |
| 1. | • Plan fizičke sigurnosti | *Obuhvaća obvezne mjere fizičke sigurnosti koje se provode te periodičku procjenu učinkovitosti mjera fizičke sigurnosti;* |
| 2. | • Periodička procjena učinkovitosti | *Realiziranog plana fizičke sigurnosti;* |
| 3. | • Matrična metoda upravljanja rizikom | *Ovisno o traženom stupnju tajnosti i procijenjenoj ukupnoj razini rizika metoda zadaje potrebni broj bodova koji se postiže kombiniranjem slojeva i opreme s ciljem postizanja tražene razine sigurnosti uz najmanja financijska ulaganja;* |
| 4. | • Mjere fizičke sigurnosti | *Obuhvaćaju obvezujuće minimalne sigurnosne mjere;* |
| 5. | • Namjena slojeva fizičke zaštite | *Obuhvaćaju koncept „Slojevi fizičke zaštite " iz PS10 i proširuju ga funkcionalnim povezivanjem u smislu namjene i opremanja;* |
| 6. | • Odobrena oprema za fizičku zaštitu | *Odabir opreme za fizičku zaštitu sukladno određenom propisu ili normi kao kriteriju za odabir komercijalno raspoložive opreme;* |
| 7. | • Sigurnosna razdioba prostora | *Na sigurnosne zone, administrativne zone, prostore za otvorenu pohranu podataka (trezor) i tehnički sigurne prostore;* |
| 8. | • Kontrola ključeva/pinova/lozinki | *Obuhvaća pravila korištenja, pohranu i stvaranje pričuvnih kopija, a uspostavlja se za prostore sa sigurnosnim statusom i tehničku opremu (vođenje evidencije korištenja, označavanja, pohrane);* |
| 9. | • Kontrola pristupa osoba/osoblja | *Obuhvaća pravila fizičkog pristupa osoba/posjetitelja i uspostavlja se za objekte i prostore sa sigurnosnim statusom;* |
| **PODSUSTAV PS14: SIGURNOST PODATAKA** | | |
| 1. | • Klasificiranje podatka | *Utvrđivanje stupnja tajnosti određenog podatka koji se koristi u radu državnog sektora ili međunarodne organizacije, sukladno zakonom propisanim kriterijima klasificiranja;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 2. | • Označavanje podatka | *Obuhvaća stupanj tajnosti i dodatne oznake (ograničavanje distribucije, označavanje preslika, trajanje stupnja tajnosti i sl.);* |
| 3. | • Ovlaštenik vlasnika podatka | *Koncept vlasnika podatka obuhvaća mogućnost prijenosa ovlasti za klasificiranje podataka na ovlaštenika;* |
| 4. | • Promjena stupnja tajnosti i deklasifikacija | *Procedura promjene koja se provodi u svim slučajevima promjene stupnja tajnosti i deklasifikacije (periodična procjena, javni pristup iz PS3);* |
| 5. | • Periodična procjena | *Procjena potrebe daljnjeg zadržavanja dodijeljenog stupnja tajnosti i mogućnost njegovog snižavanja ili deklasifikacije u propisanim vremenskim rokovima;* |
| 6. | • Korištenje klasificiranog podatka | *Zahtjevi korištenja ovise o stupnju tajnosti te o globalnoj kategoriji vlasništva (nacionalno, međunarodno);* |
| 7. | • Stupanj tajnosti i kategorija klasificiranih podataka | *Uobičajeno se koriste četiri stupnja tajnosti sukladno mogućoj šteti od neovlaštenog otkrivanja klasificiranog podatka. Globalne kategorije vlasništva su: nacionalni i međunarodni klasificirani podatci, a postoje i posebne kategorije klasificiranih podataka s obzirom na sadržaj (primjerice Crypto, Atomal);* |
| 8. | • Zahtjevi pristupa | *Obuhvaćaju poslovnu potrebu, ovlast ili autorizaciju pristupa određenom klasificiranom podatku (uključenost u projekt ili drugu vrstu ovlasti u poslovnoj organizaciji), sigurnosno informiranje, posjedovanje odgovarajućeg sigurnosnog certifikata;* |
| 9. | • Odgovornost korištenja klasificiranih podataka | *Ovisi o razinama povjerljivosti podatka: institucionalna odgovornost (pravna osoba) za osjetljive podatke, osobna odgovornost za tajne podatke (stupanj tajnosti POV, T), posebna osobna odgovornost (stupanj tajnosti VT, posebne kategorije klasificiranih podataka);* |
| 10. | • Ostali zahtjevi | *Adresati (korisnici/imatelji) su vezani ograničenjima daljnje distribucije podataka s obzirom na vlasništvo podatka, ograničenjem kopiranja/prevođenja i uništavanja za neke stupnjeve/kategorije;* |
| 11. | • Poslovi sustava registara | *Poslovi s međunarodnim klasificiranim podatcima (prijem, evidentiranje, unutarnja distribucija, pohrana, uništavanje, slanje);* |
| 12. | • Prijevoz klasificiranih podataka | *Razlikuje koncepte nacionalnog i međunarodnog;* |
| 13. | • Nacionalni prijevoz | *Reguliran zakonom;* |
| 14. | • Teklićka ili osobna dostava | *Provodi zaposlenik tijela ili pravne osobe, ograničena za međunarodnu primjenu na zemlje članice NATO-a, odnosno EU-a, osoba koristi teklićko pismo;* |
| 15. | • Komercijalna usluga dostave | *Obuhvaća poštansku uslugu nacionalne pošte ili koncesionara za zakonom definiran stupanj tajnosti, a može biti regulirano i međunarodnim ugovorom (NATO, EU), kao i certifikatom poslovne sigurnosti;* |
| 16. | • Međunarodni prijevoz | *Reguliran međunarodnim ugovorima;* |
| 17. | • Diplomatska pošta | *Međunarodna konvencija na razini UN-a za sve zemlje, osoba/diplomat koristi diplomatsko pismo;* |
| **PODSUSTAV PS15: SIGURNOST INFORMACIJSKIH SUSTAVA** | | |
| 1. | • Sigurnosna uloga klasificiranog IS-a | *U zaštiti klasificiranih podataka obuhvaća dodatne elemente povjerenja u IS, skup i taksonomiju minimalnih sigurnosnih mjera, kao i upravljanje rizikom za izbor dodatnih mjera te evaluaciju i odobravanje;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 2. | • Dodatni elementi povjerenja u IS | *Obuhvaćaju obilježja kao što su sigurnosni način rada, interkonekcija, životni ciklus, kriteriji povjerenja otvorenosti sustava;* |
| 3. | • Interkonekcija IS-ova | *Povezivanje IS-ova različitih vlasnika ili razina povjerljivosti, pri čemu se koriste zahtjevi interoperabilnosti i razdiobe podataka te evaluacija i odobravanje;* |
| 4. | • Životni ciklus IS-a | *Obuhvaća sigurnosne procedure razrađene i usklađene prema specifičnostima faza životnog ciklusa IS-a (planiranje, razvoj /nabava, ostvarenje, korištenje, povlačenje i uklanjanje);* |
| 5. | • Minimalne sigurnosne mjere | *Utvrđuje svaka pojedina politika informacijske sigurnosti u državnom sektoru ili međunarodnoj organizaciji, kao jedan ili više skupova obaveznih sigurnosnih mjera koji se propisuje zakonom ili međunarodnim ugovorom;* |
| 6. | • Taksonomija minimalnih sigurnosnih mjera | *Preuzeta je iz norme NIST SP 800-53 [85] koja sadrži preko 200 sigurnosnih mjera podijeljenih u 18 porodica i tri vrste mjera (upravljačke, operativne i tehničke), odnosno tri grupe mjera prema utjecaju povreda sigurnosti na IS;* |
| 7. | • Grupe osnovnih mjera prema utjecaju | *Procjena razine utjecaja provodi se preko tri temeljna kriterija informacijske sigurnosti za sve vrste podataka koje se koriste na IS-u (npr. osobni podatci, klasificirani podatci), a odabire se grupa kontrola prema najvišem od tri procijenjena kriterija.* |
| 8. | • Dodatne mjere za povećane zahtjeve | *Mogu uzeti u obzir dodatne mjere iz bilo kojeg od skupova osnovnih mjera, odnosno iz skupa sigurnosnih kontrola ISO27001 u PS17 (npr. slučajevi povećanih zahtjeva za kriterij povjerljivosti, specifična okolina IS-a, posebna obilježja korisnika);* |
| 9. | • Evaluacija i odobravanje | *Različiti procesi određivanja razine povjerenja prema ključnim čimbenicima politika informacijske sigurnosti (osobe, procesi, tehnologija), temeljeni na određenoj vrsti provedbe nadzora;* |
| 10. | • Akreditacija IS-a | *Odobravanje korištenja klasificiranih podataka određenog stupnja tajnosti na IS-u obuhvaća provjeru propisanih sigurnosnih mjera ;* |
| 11. | • Certifikacija TEMPEST-a | *Provjera neželjenog elektromagnetskog zračenja (TEMPEST) koja je obavezna za klasificirane IS-ove stupnja tajnosti POV i više;* |
| 12. | • Certifikacija kriptografskih proizvoda | *Provodi se u skladu s određenom međunarodnom normom, može se propisati i provoditi u ovlaštenim državnim ili međunarodnim tijelima, a koriste se i zakonom verificirane liste certificiranih kriptografskih proizvoda (NATO, EU);* |
| 13. | • Certifikacija sustava/uređaja/komponenata | *Sukladno određenoj međunarodnoj normi može se propisati i provoditi u ovlaštenim pravnim osobama, uobičajeno se koristi norma Common Criteria (ISO 15408) i popisi certificiranih proizvoda koje objavljuju akreditirani laboratoriji;* |
| **PODSUSTAV PS16: SIGURNOST POSLOVNE SURADNJE** | | |
| 1. | • Životni ciklus poslovne suradnje | *Životni ciklus poslovne suradnje obuhvaća temeljne procese certificiranja pravne osobe (ugovaratelj) i provedbe klasificiranog ugovora (naručitelj i vlasnik klasificiranih podataka);* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 2. | • Certificiranje pravne osobe | *Vrsta certificiranja kao obvezujući uvjet pristupa klasificiranim podatcima u politikama informacijske sigurnosti državnog sektor za pravnu osobu koja sklapa klasificirani ugovor s državnim tijelom ili međunarodnom organizacijom;* |
| 3. | • Certifikat pravne osobe | *Usklađuje se s potrebama pojedinog klasificiranog ugovora i obuhvaća sigurnosnu provjeru pravne osobe i fizičkih osoba koje rade na ugovoru te po potrebi akreditaciju za korištenje klasificiranih podataka u prostoru pravne osobe i na IS-u;* |
| 4. | • Klasificirani ugovor | *Ugovor između dvaju ili više ugovaratelja koji sadrži klasificirane podatke ili čija provedba zahtijeva pristup klasificiranim podatcima, pri čemu je naručitelj državno tijelo ili međunarodna organizacija koje je vlasnik klasificiranih podataka;* |
| **PODSUSTAV PS17: SIGURNOSNE KONTROLE** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Proces odabira sigurnosnih kontrola | *Temeljen je na procjeni rizika i na dodatnim zahtjevima norme ili politike informacijske sigurnosti;* |
| 2. | • Taksonomija vrsta imovine | *Predstavlja generičku podjelu štićenih vrijednosti te informacijskih sustava prema preporukama za ISO 27001 normu [91] (objekti i prostori, sklopovlje koje uključuje i komunikacijsku opremu, podatci i programska podrška), na koju se povezuju generičke vrijednosti tipičnih ranjivosti i generičke vrijednosti prijetnji koje te ranjivosti mogu iskoristiti;* |
| 3. | • Taksonomija ranjivosti | *Razrađena je za generičke tipove vrste imovine prema [91] kao opća podjela ranjivosti koja može biti organizacijsko-proceduralna, fizička ili tehnička;* |
| 4. | • Taksonomija prijetnji | *Razrađena je prema [91]tako da su prijetnje povezane s generičkim tipovima ranjivosti koje mogu iskoristiti, a obuhvaćaju opću podjelu prijetnji na: otkaze (slučajne), nezgode (prirodne i okoliš) i napade (namjerne);* |
| 5. | • Vrsta identificirane imovine koja se štiti | *Predstavlja povezivanje stvarnih štićenih vrijednosti s generičkom podjela vrsta imovine koje olakšava korištenje taksonomija ranjivosti i prijetnji;* |
| 6. | • Primjenjive sigurnosne kontrole | *Odabiru se na temelju procjene rizika, odnosno prijetnji i ranjivosti te dodatnih zahtjeva norme/politike informacijske sigurnosti, iz taksonomije sigurnosnih kontrola;* |
| 7. | • Taksonomija sigurnosnih kontrola | *Preuzeta je iz široko korištene norme ISO 27001 prema [27], koja sadrži 133 sigurnosne kontrole podijeljene u 11 područja, a koristi obilježja načina djelovanja kontrola te osnovne ciljeve djelovanja na temeljne sigurnosne kriterije informacijske sigurnosti;* |
| 8. | • Dodatni zahtjevi norme/politike | *Mogu biti povezani s legislativnim, ugovornim ili poslovnim zahtjevima, za koje treba provjeriti pokrivenost u drugim podsustavima ovog modela ili koristiti dodatne sigurnosne kontrole u PS17;* |
| 9. | • Metoda procjene rizika | *Čiji se rezultati koriste kao način utvrđivanja potrebnih sigurnosnih kontrola za određenu primjenu, provodi se za štićene vrijednosti, a u slučaju politike informacijske sigurnosti državnog sektora provodi se na ovakav način u okviru područja sigurnosti klasificiranih informacijskih sustava. U najvećem broju slučajeva koriste se kvalitativne metode;* |

| R.br. | KATEGORIJE I HIJERARHIJE POJMOVA | OPIS PRIDRUŽENOG KONCEPTA |
|---|---|---|
| 10. | • Analiza utjecaja na imovinu | *Koje može imati gubitak povjerljivosti, cjelovitosti i raspoloživosti, pri čemu se definira skala utjecaja na imovinu i procjenjuje utjecaj za svaku konkretnu imovinu prepoznatu kao štićena vrijednost;* |
| 11. | • Procjena vjerojatnosti utjecaja | *Vjerojatnost da će se analizirani utjecaji na imovinu dogoditi vrši se s obzirom na procijenjene razine prijetnji i ranjivosti (mogući vektor napada) kao umnožak s prethodno dobivenim utjecajem gubitka temeljnih sigurnosnih kriterija za neku imovinu i procjenom učestalosti rizika;* |
| 12. | • Procjena razine rizika | *Sadrži utvrđene razine rizika prema skali poslovnog utjecaja rizika, kao i prihvatljivu razinu rizika i ostale razine rizika od značaja za poslovanje (npr. razina za određivanje prioriteta u rješavanju);* |
| **PODSUSTAV PS18: ZAŠTITA OSOBNIH PODATAKA** | | |
| | *Vrh hijerarhije* | *Vršni koncept metamodela (:THING; root)* |
| 1. | • Zaštita osobnih podataka | *Specifičnosti suvremenih zahtjeva zaštite osobnih podataka [93, 94, 95, 96] kao sigurnosnih zahtjeva za politike informacijske sigurnosti (EU, zemlje članice);* |
| 2. | • Odgovornosti pravne osobe | *Za korištenje osobnih podataka sastoje se od skupa prava i obveza koje pravna osoba kao voditelj zbirke osobnih podataka mora osigurati;* |
| 3. | • Svrha i poslovna potreba prikupljanja | *Jasna definicija svrhe prikupljanja osobnih podataka i načina korištenja podataka u poslovnom procesu;* |
| 4. | • Definicija zbirke osobnih podataka | *Interno propisana u pravnoj osobi i povezana s odgovarajućim skupom sigurnosnih mjera;* |
| 5. | • Minimalizacija količine i roka čuvanja | *Minimalizacija količine i roka čuvanja osobnih podataka s obzirom na svrhu za koju su prikupljeni;* |
| 6. | • Uvjeti korištenja | *U organizaciji voditelju zbirke moraju biti jasno definirani i javno objavljeni te redovito ažurirani s obzirom na promjene koje mogu nastati;* |
| 7. | • Izvješćivanje nadležnih tijela | *O zbirkama osobnih podataka koje se vode, prijavama povreda sigurnosti osobnih podataka nadležnom tijelu i fizičkoj osobi o čijim se podatcima radi, koordinacija preko nacionalnog tijela za nadzor provedbe mjera zaštite, a za pravne osobe koje rade na području više zemalja članica EU-a mogućnost izbora;* |
| 8. | • Prava i obveze fizičke osobe | *Čiji se osobni podatci prikupljaju i koje pravna osoba koja je voditelj zbirke osobnih podataka mora osigurati;* |
| 9. | • Suglasnost za korištenje | *Suglasnost osobe za korištenje svojih osobnih podataka mora biti jasna i uočljiva te mora biti korištena za sve vrste korištenja osobnih podataka fizičke osobe.* |
| 10. | • Uvid, ispravke i brisanje | *Omogućavanje uvida u svoje osobne podatke, ispravljanja i brisanja mora biti jasno propisano internom procedurom, uključeno u politiku privatnosti te raspoloživo u obliku instrukcija fizičkim osobama čiji se osobni podatci koriste;* |
| 11. | • Nadzor nad obradom osobnih podataka | *Provodi nadležno nacionalno tijelo u suradnji s imenovanim službenikom za zaštitu osobnih podataka u tijelu koje vodi zbirku osobnih podataka.* |
| **Ukupno:**<br>**260 pojmova razvrstanih u 18 kategorija (podsustava), složenih u unutarnje hijerarhije pojmova** | | |

**PRILOG C:** Relacije između klasa definiranih u konceptualnom UML metamodelu kao daljnja razrada hijerarhijske domenske taksonomije skupa dominantnih politika i normi informacijske sigurnosti

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| **PODSUSTAV PS1: DOMENA POLITIKE INFORMACIJSKE SIGURNOSTI** | | | |
| 1. | Organizacijski entitet – PS2/Regulativni zahtjev | *koristi* | *Obvezujući regulativni zahtjevi u okviru politike informacijske sigurnosti;* |
| 2. | Organizacijski entitet – Vlasnik | *koristi* | *Pridružuje organizacijskom entitetu klasu vlasnika;* |
| 3. | Organizacijski entitet – Ustrojstvena cjelina | *koristi* | *Pridružuje organizacijskom entitetu klasu ustrojstvene cjeline;* |
| 4. | Organizacijski entitet – Rukovoditelj | *koristi* | *Pridružuje organizacijskom entitetu klasu rukovoditelja;* |
| 5. | Organizacija koja surađuje – PS8/Osoba | *koristi* | *Pridružuje vanjske zaposlenike organizacije koja surađuje kada su bitni za politike informacijske sigurnosti organizacije provoditelja;* |
| 6. | Ustrojstvena cjelina – PS8/Osoba | *koristi* | *Pridružuje zaposlenike organizacije koja provodi politiku informacijske sigurnosti pripadnoj ustrojstvenoj cjelini;* |
| 7. | Ustrojstvena cjelina – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Pridružuje ustrojstvenoj cjelini klasu uloge u unutarnjoj sigurnosnoj organizaciji;* |
| 8. | Rukovoditelj – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Pridružuje rukovoditelju klasu uloge u unutarnjoj sigurnosnoj organizaciji;* |
| **PODSUSTAV PS2: REGULATIVNA USKLAĐENOST** | | | |
| 1. | Regulativa odgovornosti – PS1/Organizacijski entitet | *koristi* | *Regulativa odgovornosti koja se odnosi na organizacijski entitet;* |
| 2. | Regulativa odgovornosti – PS6/Štićena vrijednost | *koristi* | *Regulativa odgovornosti koja se odnosi na štićenu vrijednost;* |
| 3. | Regulativa odgovornosti – PS9/Informacijski sustav | *koristi* | *Regulativa odgovornosti koja se odnosi na informacijski sustav (IS);* |
| 4. | Regulativa kibernetičke sigurnosti – PS5/Nadležno nacionalno sigurnosno tijelo | *koristi* | *Regulativa kibernetičke sigurnosti koja utvrđuje nadležno nacionalno sigurnosno tijelo;* |
| 5. | Regulativa kibernetičke sigurnosti – PS6/Podatak | *koristi* | *Regulativa kibernetičke sigurnosti koja se odnosi na određene kategorije podataka;* |
| 6. | Regulativa kibernetičke sigurnosti – PS9/Inf. sustav | *koristi* | *Regulativa kibernetičke sigurnosti koja se odnosi na određene IS-ove;* |
| 7. | Regulativa posebnih podatkovnih domena – PS6/Podatak | *koristi* | *Regulativa posebnih podatkovnih domena koja se odnosi na određene kategorije podataka;* |
| 8. | Definicija i oznaka tajnosti - PS6/Podatak | *koristi* | *Definicija i oznaka tajnosti koja se odnosi na određene kategorije podataka;* |
| 9. | Ekvivalentni stupnjevi tajnosti - PS6/Podatak | *koristi* | *Ekvivalentni stupnjevi tajnosti koji se odnose na određene kategorije podataka;* |
| 10. | Sektorski zahtjev – PS1/ Organizacijski entitet | *koristi* | *Sektorska regulativa koja se odnosi na organizacijski entitet;* |
| 11. | Sektorski zahtjev – PS6/Štićena vrijednost | *koristi* | *Sektorska regulativa koja se odnosi na štićenu vrijednost;* |
| 12. | Sektorski zahtjev – PS9/Informacijski sustav | *koristi* | *Sektorska regulativa koja se odnosi na informacijski sustav;* |
| 13. | Ugovorni zahtjev - PS1/Organizacijski entitet | *koristi* | *Ugovorni zahtjev koji se odnosi na organizacijski entitet;* |
| 14. | Ugovorni zahtjev - PS8/Osoba | *koristi* | *Ugovorni zahtjev koji se odnosi na osobu;* |
| 15. | Ugovorni zahtjev – PS6/Štićena vrijednost | *koristi* | *Ugovorni zahtjev koji se odnosi na štićenu vrijednost;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 16. | Ugovorni zahtjev – PS9/Informacijski sustav | *koristi* | *Ugovorni zahtjev koji se odnosi na IS;* |
| 17. | Ugovorni zahtjev – PS16/Klasificirani ugovor | *(višestruka specijali-zacija)* | *Klasificirani ugovor definira se u PS16 kao specijalizacija klase „Životni ciklus poslovne suradnje“ i klase „Ugovorni zahtjev“ (višestruko nasljeđivanje);* |
| 18. | Ugovor o razini usluge – PS3/Nastali podatci | *koristi* | *Ugovor o razini usluge (Service Level Agreement - SLA) treba obuhvatiti koncept nastalih podataka;* |
| 19. | Povreda sigurnosti – PS17/Taksonomija prijetnji | *koristi* | *Povreda sigurnosti povezuje se s prijetnjom iz taksonomije u PS17;* |
| 20. | Povreda sigurnosti – PS9/Kibernetičke prijetnje | *koristi* | *Povreda sigurnosti povezuje se s kibernetičkim prijetnjama iz taksonomije u PS9;* |
| 21. | Stegovni postupak - PS8/Osoba | *koristi* | *Stegovni postupak povezuje se s osobom;* |
| 22. | Povreda sigurnosti sa štetnim posljedicama – PS6/Podatak | *koristi* | *Povreda sigurnosti sa štetnim posljedicama povezuje se kategorijom podataka o kojima se radi;* |
| 23. | Kazneni postupak - PS8/Osoba | *koristi* | *Kazneni postupak povezuje se s osobom;* |
| 24. | Kazneni postupak – PS6/Štićena vrijednost | *koristi* | *Kazneni postupak povezuje se sa štićenom vrijednosti na kojoj je nastupila šteta ;* |
| 25. | Kazneni postupak – Međunarodna povreda sigurnosti | *koristi* | *Kazneni postupak povezuje se s međunarodnom povredom sigurnosti;* |
| 26. | Kazneni postupak – Povreda nacionalne sigurnosti | *koristi* | *Kazneni postupak povezuje se s povredom nacionalne sigurnosti;* |
| 27. | Kazneni postupak – Poslovna povreda sigurnosti | *koristi* | *Kazneni postupak povezuje se s poslovnom povredom sigurnosti;* |
| 28. | Međunarodna povreda sigurnosti – Ekvivalentni stupnjevi tajnosti | *koristi* | *Međunarodna povreda sigurnosti za utvrđeni ekvivalent nacionalnog stupnja tajnosti klasificiranog podatka;* |
| 29. | Povreda nacionalne sigurnosti – Definicija i oznaka tajnosti | *koristi* | *Povreda nacionalne sigurnosti prema utvrđenoj definiciji i oznaci tajnosti;* |
| 30. | Poslovna povreda sigurnosti – Definicija i oznaka tajnosti | *koristi* | *Poslovna povreda sigurnosti prema utvrđenoj definiciji i oznaci tajnosti;* |
| **PODSUSTAV PS3: RAZDIOBA PODATAKA** | | | |
| 1. | Poslovna razdioba – PS6/Podatak | *koristi* | *Poslovna razdioba povezuje se s kategorijom podataka na koju se odnosi;* |
| 2. | Poslovna razdioba – PS1/Organizacijski entitet | *koristi upravitelja* | *Poslovna razdioba povezuje se s organizacijskim entitetom koji je upravitelj poslovne razdiobe;* |
| 3. | Interesna skupina – PS1/Organizacijski entitet | *koristi članove* | *Interesna skupina za poslovnu razdiobu povezuje se s organizacijskim entitetima koji su članovi skupine;* |
| 4. | Domena razdiobe – PS2/Regulativni zahtjev | *koristi* | *Pridruživanje regulativnog zahtjeva kojim se definira domena razdiobe;* |
| 5. | Domena razdiobe – Organizacijska pravila | *ograničava* | *Pridruživanje organizacijskih pravila domeni razdiobe;* |
| 6. | Domena razdiobe – Semantička pravila | *ograničava* | *Pridruživanje semantičkih pravila domeni razdiobe;* |
| 7. | Domena razdiobe – Tehnička pravila | *ograničava* | *Pridruživanje tehničkih pravila domeni razdiobe;* |
| 8. | Tehnička pravila – PS15/Evaluacija i odobravanje | *koristi* | *Pridruživanje odgovarajućih zahtjeva za evaluaciju i odobravanje tehničkim pravilima domene razdiobe;* |
| 9. | Javna razdioba – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Svakoj javnoj razdiobi pridružuje se vlasnik podataka;* |
| 10. | Javna objava – PS6/Podatak | *koristi* | *Svakoj javnoj razdiobi pridružuje se definirani podatak;* |
| 11. | Neovlaštena objava – PS2/Povreda sigurnosti | *koristi* | *Neovlaštena objava povezuje se s konceptom povrede sigurnosti;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 12. | Javni pristup – PS6/Podatak | *koristi* | *Svakom javnom pristupu pridružuje se definirani podatak;* |
| 13. | Javni pristup – PS14/Promjena stupnja tajnosti i deklasifikacija | *koristi* | *Svaki javni pristup klasificiranim podatcima prolazi prethodnu deklasifikaciju;* |
| 14. | Povjereni podatci – PS6/Podatak | *koristi* | *Definira se skup povjerenih podataka s obzirom na kategorizaciju u politici informacijske sigurnosti;* |
| 15. | Povjereni podatci – PS2/Ugovorni zahtjev | *koristi* | *Skup povjerenih podataka definira se kao ugovorni zahtjev;* |
| 16. | Podatci o ponašanju – PS2/Ugovorni zahtjev | *koristi* | *Prikupljanje i korištenje podataka o ponašanju definira se kao ugovorni zahtjev;* |
| **PODSUSTAV PS4: NADZOR INFORMACIJSKE SIGURNOSTI** | | | |
| 1. | Provedba nadzora – PS6/Štićena vrijednost | *koristi* | *Provedba nadzora koristi uvid u štićene vrijednosti;* |
| 2. | Provedba nadzora – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Provedba nadzora koordinira se s vlasnikom podataka i drugih vrijednosti;* |
| 3. | Provedba nadzora – Metoda | *koristi* | *Provedba nadzora koristi metodu nadzora;* |
| 4. | Opseg – PS1/Organizacijski entitet | *koristi* | *Opseg nadzora je organizacijski entitet;* |
| 5. | Opseg – PS1/Ustrojstvena cjelina | *koristi* | *Opseg nadzora je ustrojstvena cjelina;* |
| 6. | Opseg – PS1/Informacijski sustav | *koristi* | *Opseg nadzora je IS;* |
| 7. | Unutarnji – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Proces unutarnjeg nadzora koristi unutarnju sigurnosnu organizaciju;* |
| 8. | Vanjski – PS8/Nadležno nacionalno sigurnosno tijelo | *koristi* | *Proces vanjskog nadzora koristi nadležno nacionalno sigurnosno tijelo;* |
| 9. | Vanjski – Akreditacija | *ograničava* | *Koncept vanjskog nadzora obavezan je za akreditaciju;* |
| 10. | Vanjski – Certifikacija | *ograničava* | *Koncept vanjskog nadzora obavezan je za certifikaciju;* |
| 11. | Vanjski – Nadzor/revizija | *ograničava* | *Koncept vanjskog nadzora obavezan je za nadzor/reviziju;* |
| 12. | Unutarnji – Unutarnji nadzor/revizija | *ograničava* | *Unutarnji nadzor/revizija temelji se na konceptu unutarnjeg nadzora;* |
| 13. | Akreditacija – PS15/Akreditacija informacijskog sustava | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 14. | Akreditacija – PS5/Akreditacija registara | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 15. | Certifikacija – PS15/Certifikacija TEMPEST-a | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 16. | Certifikacija – PS15/Certifikacija kriptografskih proizvoda | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 17. | Certifikacija – PS15/Certifikacija sustava/uređaja/komponenata | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 18. | Certifikacija – PS15/Proces certifikacije osoba | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 19. | Certifikacija – PS15/Certifikacija pravne osobe | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 20. | Nadzor/revizija – PS18/Nadzor nad obradom osobnih podataka | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 21. | Nadzor/revizija – PS11/Nadzor zaštite klasificiranih podataka | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 22. | Unutarnji nadzor/revizija – PS13/Periodička procjena učinkovitosti | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| 23. | Unutarnji nadzor/revizija – PS11/ Unutarnji nadzor zaštite klasificiranih podataka | *(višestruka specijali-zacija)* | *Specijalizacija opće klase za korištenje u drugom podsustavu gdje se dodatno specijalizira višestrukim nasljeđivanjem;* |
| **PODSUSTAV PS5: ORGANIZACIJSKI OKVIR** | | | |
| 1. | Nadležno međunarodno sigurnosno tijelo – PS2/Regulativni zahtjev | *koristi* | *Regulativni zahtjev koji definira nadležno međunarodno sigurnosno tijelo;* |
| 2. | Nadležno nacionalno sigurnosno tijelo – PS2/Regulativni zahtjev | *koristi* | *Regulativni zahtjev koji definira nadležno nacionalno sigurnosno tijelo;* |
| 3. | Sustav registara – PS1/Organizacijski entitet | *koristi* | *Sustav registara za međunarodne klasificirane podatke uspostavlja se u državnim tijelima i pravnim osobama;* |
| 4. | NSA hijerarhija/tijelo – Akreditacija registara | *ostvaruje* | *NSA hijerarhija/tijelo ima nadležnost akreditacije registara;* |
| 5. | Akreditacija registara – Sustav registara | *ograničava* | *Akreditacija predstavlja odobrenje za rad svake sastavnice Sustava registara;* |
| **PODSUSTAV PS6: DEFINICIJA PODATAKA I DRUGIH VRIJEDNOSTI** | | | |
| 1. | Štićena vrijednost – PS2/Regulativni zahtjev | *koristi* | *Regulativni zahtjev koji utvrđuje potrebu zaštite podataka i drugih poslovnih vrijednosti;* |
| 2. | Štićena vrijednost – PS7/Kriteriji informacijske sigurnosti | *koristi* | *Štićena vrijednost za koju se osigurava zaštita kriterija informacijske sigurnosti;* |
| 3. | Podatak – PS9/Informacijski sustav | *koristi* | *Utvrđuje se mogućnost korištenja definiranih grupa podataka na određenom IS-u;* |
| 4. | Osobni podatak – PS18/Zaštita osobnih podataka | *koristi* | *Za sve grupe osobnih podataka u korištenju koristi se provedba zaštite osobnih podataka u PS18;* |
| 5. | Povjerljivi podatak – PS11/Zaštita klasificiranih podataka | *koristi* | *Za sve grupe klasificiranih podataka definiranih preko koncepta povjerljivi podatak koristi se provedba zaštite klasificiranih podataka u PS11;* |
| 6. | Vrlo povjerljivi podatak – PS11/Zaštita klasificiranih podataka | *koristi* | *Za sve grupe klasificiranih podataka definiranih preko koncepta vrlo povjerljivi podatak koristi se provedba zaštite klasificiranih podataka u PS11;* |
| 7. | Klasificirani podatak posebne odgovornosti – PS11/Zaštita klasificiranih podataka | *koristi* | *Za sve grupe klasificiranih podataka definiranih preko koncepta klasificirani podatak posebne odgovornosti koristi se provedba zaštite klasificiranih podataka u PS11;* |
| 8. | Objekti i prostori – PS10/ Čimbenici rizika | *(višestruka specijali-zacija)* | *Specijalizacija preko klase iz drugog podsustava višestrukim nasljeđivanjem;* |
| 9. | Objekti i prostori – PS10/ Ciljevi fizičke sigurnosti | *(višestruka specijali-zacija)* | *Specijalizacija preko klase iz drugog podsustava višestrukim nasljeđivanjem;* |
| 10. | Doseg utjecaja povreda sigurnosti – PS2/Regulativni zahtjev | *koristi* | *Regulativni zahtjev koji utvrđuje doseg utjecaja povreda sigurnosti;* |
| 11. | Kritična infrastruktura – Nacionalni doseg | *koristi* | *Nacionalna kritična infrastruktura;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 12. | Kritična infrastruktura – Međunarodni doseg | *koristi* | *EU kritična infrastruktura;* |
| **PODSUSTAV PS8: DEFINICIJA OSOBA** | | | |
| 1. | Osoblje – PS12/Zahtjevi sigurnosti osoblja | *koristi* | *Definiranje zahtjeva sigurnosti osoblja vezanih za potrebu korištenja klasificiranih podataka;* |
| 2. | Osoblje – PS2/Povreda sigurnosti | *koristi* | *Evidentiranje povreda sigurnosti povezanih s osobljem;* |
| 3. | Zahtjevi povjerenja u osobe – PS2/Ugovorni zahtjev | *koristi* | *Ugovorni zahtjev koji utvrđuje zahtjeve povjerenja u osobe;* |
| 4. | Osoba – PS1/Organizacijski entitet | *koristi* | *Povezuje osobu sa organizacijom poslodavcem;* |
| 5. | Osoba – PS9/Informacijski sustav | *koristi* | *Povezuje osobu s ovlaštenjem za pristup informacijskom sustavu;* |
| 6. | Osoba – Unutarnja sigurnosna organizacija | *koristi* | *Povezuje osobu i sigurnosne uloge koje su joj dodijeljene obostrano;* |
| 7. | Vlasnik podataka i drugih vrijednosti – PS1/Rukovoditelj | *koristi* | *Dodjeljuje ulogu vlasnika podataka i drugih vrijednosti rukovoditelju organizacije;* |
| **PODSUSTAV PS9: DEFINICIJA INFORMACIJSKIH SUSTAVA** | | | |
| 1. | Informacijski sustav – PS2/Regulativni zahtjev | *koristi* | *Regulativni zahtjev za IS;* |
| 2. | Informacijski sustav – PS7/Temeljni sigurnosni kriteriji | *koristi* | *Definiranje temeljnih sigurnosnih kriterija za IS;* |
| 3. | Informacijski sustav – PS6/Doseg utjecaja povreda sigurnosti | *koristi* | *Definiranje dosega utjecaja povreda sigurnosti za IS;* |
| 4. | Informacijski sustav – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Definiranje sigurnosne odgovornosti za IS;* |
| 5. | Informacijski sustav – PS8/Osoba | *koristi* | *Definiranje korisnika IS-a;* |
| 6. | Informacijski sustav – PS17/Vrsta identificirane imovine koja se štiti | *koristi* | *Definiranje informacijskog sustava kao generičkog tipa vrste imovine radi korištenja taksonomija prijetnji, ranjivosti i odabira sigurnosnih kontrola;* |
| 7. | Klasificirani informacijski sustav – PS15/Minimalne sigurnosne mjere | *koristi* | *Definiranje korištenja skupa minimalnih sigurnosnih mjera za klasificirani IS;* |
| 8. | Klasificirani informacijski sustav – PS15/Životni ciklus razvoja sustava | *koristi* | *Definiranje korištenja faza životnog ciklusa razvoja sustava za klasificirani IS;* |
| 9. | Klasificirani informacijski sustav – PS15/Evaluacija i odobravanje | *koristi* | *Definiranje potrebnih postupaka evaluacije i odobravanja (akreditacija, certifikacija) za klasificirani IS;* |
| 10. | Klasificirani informacijski sustav – PS15/Interkonekcija IS-ova | *koristi* | *Definiranje uvjeta interkonekcije za klasificirani IS;* |
| 11. | Klasificirani informacijski sustav – PS15/Dodatni elementi povjerenja u IS | *(višestruka specijali-zacija)* | *Specijalizacija preko klase iz drugog podsustava višestrukim nasljeđivanjem;* |
| 12. | Organizacijski elementi IS-a – PS1/Ustrojstvena cjelina | *koristi upravitelja* | *Definiranje ustrojstvene cjeline kao odgovornog upravitelja IS-a;* |
| 13. | Organizacijski elementi IS-a – PS8/Unutarnja sigurnosna organizacija | *koristi administra-tora* | *Definiranje administratorskog osoblja IS-a;* |
| 14. | Organizacijski elementi IS-a – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje se koriste na IS-u;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 15. | Organizacijski elementi IS-a – PS5/Nadležno nacionalno sigurnosno tijelo | *koristi* | *Definiranje vanjskog nadležnog sigurnosnog tijela za IS;* |
| 16. | Dimenzija kibernetičkog prostora – PS5/ Nadležno nacionalno sigurnosno tijelo | *koristi* | *Definiranje nacionalnog koordinacijskog tijela za četiri ključne dimenzije: društvena, ekonomska, sigurnosna i obrambena;* |
| 17. | Kibernetičke prijetnje – PS2/Povreda sigurnosti | *koristi* | *Definiranje mogućnosti povreda sigurnosti temeljenih na kibernetičkim prijetnjama;* |
| 18. | Kibernetičke prijetnje – PS9/Informacijski sustav | *koristi* | *Definiranje utjecaja kibernetičkih prijetnji na informacijski sustav;* |
| 19. | Napredne metode kombiniranih prijetnji – Prijetnje korisnicima računala | *koristi* | *Definiranje naprednih kombiniranih prijetnji;* |
| 20. | Napredne metode kombiniranih prijetnji – Prijetnje informacijskim sustavima | *koristi* | *Definiranje naprednih kombiniranih prijetnji;* |
| 21. | Sigurnosni događaj – Aktivnost | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 22. | Sigurnosni događaj – Meta | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 23. | Sigurnosni napad – Alat za iskorištavanje ranjivosti | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 24. | Sigurnosni napad – Ranjivost sustava | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 25. | Sigurnosni napad – Neovlašteni rezultat | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 26. | Sigurnosni incident – Napadač | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 27. | Sigurnosni incident – Motiv | *koristi* | *Ostvarenje taksonomije računalnih sigurnosnih incidenata prema [13];* |
| 28. | Alat za iskorištavanje ranjivosti – PS17/Taksonomija prijetnji | *koristi* | *Definiranje veze između taksonomije općih prijetnji u PS17 i računalnih prijetnji u PS9;* |
| 29. | Ranjivost sustava – PS17/Taksonomija ranjivosti | *koristi* | *Definiranje veze između opće taksonomije ranjivosti u PS17 i ranjivosti sustava u PS9;* |
| **PODSUSTAV PS10: DEFINICIJA FIZIČKE SIGURNOSTI** | | | |
| 1. | Čimbenici rizika – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje predstavljaju čimbenike rizika fizičke sigurnosti;* |
| **PODSUSTAV PS11: ZAŠTITA KLASIFICIRANIH PODATAKA** | | | |
| 1. | Nadzor zaštite klasificiranih podataka – PS5/NSA hijerarhija/tijelo | *koristi* | *Definira nadležno sigurnosno tijelo za provedbu vanjskog nadzora;* |
| 2. | Unutarnji nadzor zaštite klasificiranih podataka – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Definira unutarnju sigurnosnu organizaciju (savjetnik za informacijsku sigurnost) nadležnu za provedbu unutarnjeg nadzora;* |
| **PODSUSTAV PS12: SIGURNOST OSOBLJA** | | | |
| 1. | Zahtjevi sigurnosti osoblja – PS8/Osoba | *koristi* | *Primjena zahtjeva sigurnosti na definiranu osobu;* |
| 2. | Zahtjevi sigurnosti osoblja – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Definira unutarnju sigurnosnu organizaciju nadležnu za zahtjeve sigurnosti osoblja;* |
| 3. | Vrsta certifikata – PS2/Zakonski zahtjev | *koristi* | *Zakonski zahtjev koji definira vrstu certifikata;* |
| 4. | Razina certifikata - PS2/Zakonski zahtjev | *koristi* | *Zakonski zahtjev koji definira razinu certifikata;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| **PODSUSTAV PS13: FIZIČKA SIGURNOST** | | | |
| 1. | Plan fizičke sigurnosti – PS6/Štićena vrijednost | *koristi* | *Primjena plana fizičke sigurnosti na štićene vrijednosti;* |
| 2. | Plan fizičke sigurnosti – PS6/Unutarnja sigurnosna organizacija | *koristi* | *Definira unutarnju sigurnosnu organizaciju nadležnu za planiranje fizičke sigurnosti;* |
| 3. | Namjena slojeva fizičke zaštite – PS10/Fizička zaštita po dubini | *koristi* | *Definiranje slojeva fizičke zaštite po dubini;* |
| 4. | Namjena slojeva fizičke zaštite – PS10/Sigurnosna razdioba prostora | *koristi* | *Definiranje funkcionalnosti slojeva fizičke zaštite po dubini;* |
| 5. | Namjena slojeva fizičke zaštite – PS10/Odobrena oprema za fizičku zaštitu | *koristi* | *Definiranje opremanja slojeva fizičke zaštite po dubini;* |
| **PODSUSTAV PS14: SIGURNOST PODATAKA** | | | |
| 1. | Klasificiranje podatka – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje se klasificiraju;* |
| 2. | Klasificiranje podatka – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Definiranje vlasnika podataka koji se klasificiraju;* |
| 3. | Ovlaštenik vlasnika podataka – PS8/Osoba | *koristi* | *Pridruživanje uloge ovlaštenika vlasnika podataka osobi;* |
| 4. | Korištenje klasificiranog podatka – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje se koriste;* |
| 5. | Korištenje klasificiranog podatka – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Definiranje vlasnika podataka koji se koriste;* |
| 6. | Zahtjevi pristupa – PS12/Popis dužnosti i poslova za certificiranje | *koristi* | *Poslovnu potrebu kao zahtjev pristupa klasificiranim podatcima formalizira donošenje popisa dužnosti i poslova za sigurnosno certificiranje;* |
| 7. | Zahtjevi pristupa – PS12/Vrsta certifikata | *koristi* | *Vrsta certifikata kao zahtjev pristupa usklađena je sa stupnjem tajnosti;* |
| 8. | Zahtjevi pristupa – PS12/Sigurnosno informiranje | *koristi* | *Sigurnosno informiranje provodi se prilikom izdavanja certifikata, periodično tijekom važenja certifikata te završetkom potrebe pristupa;* |
| 9. | Poslovi sustava registara – PS5/Sustav registara | *koristi* | *Povezuje aktivnosti s nadležnom sastavnicom Sustava registara;* |
| 10. | Prijevoz klasificiranih podataka – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje se prevoze;* |
| 11. | Prijevoz klasificiranih podataka – PS8/Vlasnik podataka i drugih vrijednosti | *koristi* | *Definiranje vlasnika podataka čiji se podatci prevoze;* |
| 12. | Međunarodni prijevoz – PS5/NSA hijerarhija/tijelo | *koristi* | *Definiranje NSA hijerarhije/tijela nadležnog za međunarodni prijevoz;* |
| **PODSUSTAV PS15: SIGURNOST INFORMACIJSKIH SUSTAVA** | | | |
| 1. | Sigurnosna uloga klasificiranog IS-a – PS9/Klasificirani informacijski sustav | *koristi* | *Pridruživanje sigurnosne uloge IS-a, odnosno skupa mjera zaštite IS-a, definiranom klasificiranom IS-u;* |
| 2. | Sigurnosna uloga klasificiranog IS-a – PS8/Unutarnja sigurnosna organizacija | *koristi* | *Pridruživanje odgovorne sigurnosne uloge za klasificirani IS-a;* |
| 3. | Interkonekcija IS-ova – PS3/Domena razdiobe | *koristi* | *Interkonekcija IS-ova preko domene razdiobe iz PS3 povezuje se s pravilima interoperabilnosti;* |
| 4. | Minimalne sigurnosne mjere – PS17/Taksonomija sigurnosnih kontrola | *koristi dodatne mjere* | *Korištenje dodatnih sigurnosnih kontrola (npr. temeljeno na upravljanju rizikom) uz obavezne minimalne sigurnosne mjere;* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 5. | Minimalne sigurnosne mjere – Taksonomija minimalnih sigurnosnih mjera | *koristi* | *Korištenje obaveznih minimalnih sigurnosnih mjera;* |
| 6. | Taksonomija minimalnih sigurnosnih mjera – PS7/Temeljni sigurnosni kriteriji | *koristi* | *Sigurnosne mjere imaju djelovanje na jedan ili više temeljnih sigurnosnih kriterija povjerljivosti, cjelovitosti i raspoloživosti;* |
| 7. | Taksonomija minimalnih sigurnosnih mjera – PS17/Taksonomija sigurnosnih kontrola | *koristi mapiranje* | *Sigurnosne mjere iz taksonomije sigurnosnih mjera mapiraju se sa sukladnim sigurnosnim kontrolama iz Taksonomije sigurnosnih kontrola u PS17prema [27, 85];* |
| **PODSUSTAV PS16: SIGURNOST POSLOVNE SURADNJE** | | | |
| 1. | Životni ciklus poslovne suradnje – PS6/Podatak | *koristi* | *Definiranje grupa podataka koje se koriste u okviru poslovne suradnje;* |
| 2. | Životni ciklus poslovne suradnje – PS8/ Unutarnja sigurnosna organizacija | *koristi* | *Definiranje odgovornih unutarnjih sigurnosnih uloga koje se koriste u okviru poslovne suradnje;* |
| 3. | Klasificirani ugovor – PS1/Organizacijski entitet | *koristi naručitelja* | *Organizacijski entitet naručitelj klasificiranog ugovora;* |
| 4. | Klasificirani ugovor – PS1/Organizacijski entitet | *koristi ugovaratelja* | *Organizacijski entitet ugovaratelj klasificiranog ugovora;* |
| 5. | Klasificirani ugovor – PS5/NSA hijerarhija/tijelo | *koristi ugovaratelja* | *Nadležno sigurnosno tijelo za provođenje klasificiranog ugovora;* |
| **PODSUSTAV PS17: SIGURNOSNE KONTROLE** | | | |
| 1. | Vrsta identificirane imovine koja se štiti – PS6/Štićena vrijednost | *koristi* | *Definiranje štićene vrijednosti kao vrste identificirane imovine koja se štiti sigurnosnim kontrolama;* |
| 2. | Vrsta identificirane imovine koja se štiti – PS9/Informacijski sustav | *koristi* | *Definiranje informacijskog sustava kao vrste identificirane imovine koja se štiti sigurnosnim kontrolama;* |
| 3. | Vrsta identificirane imovine koja se štiti – Taksonomija vrsta imovine | *koristi* | *Definiranje vrste identificirane imovine prema generičkim vrstama imovine u taksonomiji prema [91];* |
| 4. | Vrsta identificirane imovine koja se štiti – Taksonomija ranjivosti | *koristi* | *Definiranje ranjivosti određene vrste identificirane imovine prema taksonomiji ranjivosti povezanoj s taksonomijom generičkih vrsta imovine prema[91];* |
| 5. | Taksonomija vrsta imovine - Taksonomija ranjivosti | *koristi* | *Definiranje ranjivosti za generičke tipove vrste imovine, povezivanjem dvaju taksonomija prema [91];* |
| 6. | Taksonomija ranjivosti – Taksonomija prijetnji | *koristi* | *Definiranje prijetnji koje mogu iskoristiti pojedinu ranjivost, povezivanjem dvaju taksonomija prema [91];* |
| 7. | Vrsta identificirane imovine koja se štiti – Primjenjive sigurnosne kontrole | *koristi* | *Definiranje skupa primjenjivih sigurnosnih kontrola za određenu vrstu identificirane imovine;* |
| 8. | Taksonomija prijetnji – PS7/Temeljni sigurnosni kriteriji | *koristi* | *Djelovanje prijetnji definira se utjecajem na temeljne sigurnosne kriterije povjerljivosti, cjelovitosti i raspoloživosti;* |
| 9. | Taksonomija prijetnji – PS9/Alat za iskorištavanje ranjivosti | *koristi* | *Opće prijetnje iz Taksonomije prijetnji mogu se povezati sa specijaliziranom taksonomijom alata za iskorištavanje ranjivosti u PS9;* |
| 10. | Taksonomija prijetnji – PS2/Povreda sigurnosti | *koristi* | *Opće prijetnje iz Taksonomije prijetnji mogu se povezati s definiranim povredama sigurnosti u PS2;* |
| 11. | Primjenjive sigurnosne kontrole – Taksonomija sigurnosnih kontrola | *koristi* | *Odabir primjenjivih sigurnosnih kontrola vrši se iz taksonomije sigurnosnih kontrola prema [27];* |

| R.br. | KLASE KOJE SE POVEZUJU | OZNAKA RELACIJE | OPIS ZNAČENJA RELACIJE |
|---|---|---|---|
| 12. | Taksonomija sigurnosnih kontrola – PS7/Temeljni sigurnosni kriteriji | *koristi* | *Sigurnosne kontrole imaju djelovanje na jedan ili više temeljnih sigurnosnih kriterija povjerljivosti, cjelovitosti i raspoloživosti;* |
| 13. | Taksonomija sigurnosnih kontrola – PS15/ Taksonomija minimalnih sigurnosnih mjera | *koristi mapiranje* | *Sigurnosne kontrole iz Taksonomije sigurnosnih kontrola mapiraju se sa sukladnim sigurnosnim mjerama iz taksonomije sigurnosnih mjera u PS15 prema [27, 85];* |
| 14. | Metoda procjene rizika – PS2/Regulativa odgovornosti | *koristi* | *Regulativa odgovornosti koja se odnosi na procjenu rizika;* |
| 15. | Primjenjive sigurnosne kontrole – Metoda procjene rizika | *koristi* | *Odabir primjenjivih sigurnosnih kontrola vrši se na temelju rezultata procjene rizika;* |
| 16. | Primjenjive sigurnosne kontrole – Dodatni zahtjevi norme/smjernice | *koristi* | *Odabir primjenjivih sigurnosnih kontrola vrši se na temelju dodatnih zahtjeva norme/smjernice;* |
| **PODSUSTAV PS18: ZAŠTITA OSOBNIH PODATAKA** | | | |
| 1. | Zaštita osobnih podataka – PS6/Osobni podatak | *koristi* | *Povezivanje mjera zaštite s definiranom kategorijom osobnih podataka;* |
| 2. | Odgovornosti pravne osobe – PS8/Unutarnja sigurnosna organizacija | *koristi službenika za zaštitu* | *Definiranje odgovornih unutarnjih sigurnosnih uloga koje se koriste u okviru zaštite osobnih podataka;* |
| 3. | Uvjeti korištenja – PS6/Javno dostupan podatak | *koristi politiku privatnosti* | *Definira obvezu objave politike privatnosti;* |
| 4. | Izvješćivanje nadležnih tijela – PS5/Tijelo za zaštitu osobnih podataka | *koristi* | *Definira nadležno tijelo za izvješćivanje;* |
| 5. | Nadzor nad obradom osobnih podataka – PS5/Tijelo za zaštitu osobnih podataka | *koristi* | *Definira nadležno tijelo za nadzor nad obradom osobnih podataka;* |
| **Ukupno:**<br>**187 relacija između klasa definiranih u konceptualnom UML metamodelu kao daljnja razrada hijerarhijske domenske taksonomije skupa dominantnih politika i normi informacijske sigurnosti** | | | |

## POPIS SLIKA:

## POPIS TABLICA:

# ŽIVOTOPIS

Aleksandar Klaić rođen je 1964. godine u Vinkovcima. Diplomirao je 1990. godine na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu, na smjeru automatike i računalnog inženjerstva. Magistrirao je 1997. godine, također na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu, iz područja tehničkih znanosti, polje elektrotehnika, smjer automatika.

Profesionalnu karijeru započeo je u Brodarskom institutu u Zagrebu kao istraživač, a potom i voditelj projekata u području upravljanja procesima i primjeni ugrađenih računalnih sustava za vojne i civilne namjene. Radio je u više institucija hrvatskog sigurnosnog sustava na stručnim i rukovodnim radnim mjestima, u okviru problematike planiranja, upravljanja i održavanja komunikacijskih i informacijskih sustava. Posljednjih desetak godina bavi se područjem informacijske sigurnosti, a zaposlen je u Uredu Vijeća za nacionalnu sigurnost na poslovima vezanim za nadležnosti Ureda kao središnjeg državnog tijela za informacijsku sigurnost u nacionalnom, NATO i EU kontekstu (National Security Authority – NSA).

Njegovi istraživački interesi obuhvaćaju područja informacijske sigurnosti, teorije sustava, automatskog upravljanja sustavima i ugrađenih računalnih sustava. Član je i utemeljitelj Hrvatskog društva za robotiku te član međunarodne organizacije IEEE. Autor je više znanstvenih i stručnih radova.

## POPIS OBJAVLJENIH RADOVA:


[1] Klaić, A., Golub, M., „Conceptual Modelling of Information Systems within the Information Security Policies", International Conference on Computing and Business Management, ICCBM 2013, Paris, June 2013, published in Journal of Economics, Business, and Management, JOEBM 2013 Vol.1(4), November 2013, ISSN: 2301-3567, str. 371-376, dostupno na: http://www.joebm.com/index.php?m=content&c=index&a=show&catid=33&id=349 (4. studenog 2013.).

[2] Klaić, A., Golub, M., "Conceptual Information Modelling within the Contemporary Information Security Policies", International Convention on Information and

Communication Technology, Electronics and Microelectronics, MIPRO 2013/ISS, Opatija, 2013, str. 1386-1391.

[3] Klaić, A., Perešin, A., „The Impact of the National Information Security Regulation Framework on Cyber Security in Global Environment“, International Scientific Conference on Corporate Security in Dynamic Global Environment - Challenges and Risks, Institute for Corporative Security Studies, Ljubljana, Slovenia, 2012, str. 85-96.

[4] Klaić, A., Hadjina, N., „Methods and Tools for the Development of Information Security Policy – A Comparative Literature Overview”, Proceedings of the International Convention MIPRO 2011, Opatija, Croatia, 2011, str. 190-195.

[5] Klaić, A., Perešin, A., „Koncept regulativnog okvira informacijske sigurnosti“, Zbornik radova međunarodne znanstvene konferencije „Dani kriznog upravljanja“, Velika Gorica, Hrvatska, 2011., str. 678-707.

[6] Klaić, A., „Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies”, Proceedings of the International Convention MIPRO 2010, Opatija, Croatia, 2010, str. 136-141.

[7] Perešin, A., Klaić, A., „Povezanost koncepata kritične nacionalne infrastrukture i zaštite podataka“, Zbornik radova međunarodne znanstvene konferencije „Dani kriznog upravljanja“, Velika Gorica, Hrvatska, 2010., str. 13-29.

[8] Klaić, A., „Information Security Requirements in the Information Systems Planning Process”, Proceedings of the International Conference on Information and Intelligent Systems (IIS), Varaždin, Croatia, 2006, str. 265-269.

[9] Klaić, A., „Information Security in Business and Government Sectors”, Proceedings of the International Convention MIPRO 2005, Opatija, Croatia, 2005, str. 193-198.

[10] Klaić, A., Turek, F., „Nacionalna sigurnost i telekomunikacije“, Međunarodne studije, časopis za međunarodne odnose, vanjsku politiku i diplomaciju, II (2002), 4, Zagreb 2002., str. 97-112.

[11] Klaić, A., „Koordinatno upravljanje malim podvodnim vozilom, magistarski rad, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 1997.

[12] Klaić, A., Koroman, V., Kuljača, Lj., „Modular Approach to Designing Simulation System of Unmanned Underwater Vehicle“, Proceedings of the 39th International Symposium Electronics in Marine, ELMAR 97, Zadar, Croatia, 1997, str. 216-219.

[13] Klaić, A., Koroman, V., Kuljača, Lj., „Actual State and Trends in the Development of Unmanned Underwater Vehicles“, Proceedings of the 38th Congress of International Symposium Electronics in Marine, ELMAR 96, Zadar, Croatia, 1996, str. 211-214.

[14] Klaić, A., Koroman, V., Kuljača, Lj., „CAN - Računalna mreža u vozilima“, Zbornik radova Automatizacija u prometu 1995, Zagreb, KoREMA, 1995, str. 146-150.

[15] Klaić, A., „Odabir ugrađenih računalnih sustava i integracija procesne mreže distribuiranog sustava nadzora baterije“, Proceedings of the 18th International Convention MIPRO 1995, Rijeka, MIPRO, 1995, str. 56-61.

[16] Klaić, A., „Comparable Characteristics of Some Fieldbusses“, Proceedings of the VII Congress of the International Maritime Association of the Mediterranean, IMAM 95, Dubrovnik, 1995, str. 701-708.

[17] Klaić, A., „Sustav nadzora baterije podvodnog vozila“, Proceedings of the 36th ELMAR International Symposium, Božava, ELMAR, 1994, str. 45-48.

## BIOGRAPHY

Aleksandar Klaić was born on 1964 in Vinkovci, Croatia. He received his B.Sc. degree in Electrical Engineering and Computing from the University of Zagreb, Faculty of Electrical Engineering and Computing in 1990, and M.Sc. degree in Control Engineering from the same university in 1997.

He has started his professional carrier in the Croatian Institute of Advanced Technologies (Brodarski institute) working as the researcher and later on as the project manager in the field of process control and embedded systems technology, both for military and civilian purposes. He has worked in several different institutions of the Croatian national security system, where he was involved with the development and operational issues of communication and information systems, working on different expert and management positions. Last ten years he has been mainly involved in the field of information security. He is currently employed in the Office of the National Security Council where he is responsible for the Croatian National Security Authority (NSA) role of the Office in the national, NATO and EU context.

His research interests include information security, systems theory, control theory, and embedded systems. He is the founding member of the Croatian Association for the Robotics (HDR) and the member of international organization IEEE. He is the author of several scientific and professional papers.