RAZVOJ ZNANOSTI IN STROKE INFORMACIJSKE VARNOSTI

ANŽE MIHELIČ, KAJA PRISLAN MIHELIČ
Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
anze.mihelic@um.si, kaja.prislan@um.si

Povzetek Prispevek predstavlja vpogled v zgodovinski razvoj informacijske varnosti, ki jo v literaturi pogosto zasledimo tudi kot sinonim za računalniško varnost, v zadnjem času pa vse pogosteje tudi kibernetsko varnost. Razvoj znanosti in stroke je predstavljen v dveh ključnih delih. V prvem delu predstavljamo strokovni razvoj informacijske varnosti skozi štiri ključna obdobja: obdobje do šestedesetih let dvajsetega stoletja, obdobje med šestdesetimi in osemdesetimi leti, obdobje osemdesetih in devetdesetih let in obdobje enaindvajsetega stoletja. V drugem delu pa skozi kvantitativne analize prispevkov, objavljenih v virih, ki so indeksirani v bibliografski zbirki *Web of Science*, zarišemo razvoj raziskovalne dejavnosti s področja informacijske varnosti tako v svetu kot v Sloveniji in na Fakulteti za varnostne vede Univerze v Mariboru. Ugotovitve kažejo, da Slovenija glede na svojo majhnost objavi razmeroma veliko število prispevkov s tega področja, za kar so v pretežnem delu zaslužni raziskovalci Katedre za informacijsko varnost Fakultete za varnostne vede Univerze v Mariboru.

Ključne besede:
informacijska varnost,
kibernetska varnost,
računalniška varnost,
bibliometrija,
zgodovina informacijske varnosti

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/um.fvv.3.2023.8
ISBN 978-961-286-731-7

DEVELOPMENT OF THE SCIENCE AND PROFESSION OF INFORMATION SECURITY

ANŽE MIHELIČ, KAJA PRISLAN MIHELIČ
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
anze.mihelic@um.si, kaja.prislan@um.si

Abstract The paper presents an insight into the historical development of information security, a term frequently interchangeably used in the literature as computer security and, more recently, cybersecurity. The historical development of information security is presented in two parts. First, the paper presents the professional development of information security through four critical periods: the period up to 1960, between 1960 and 1980, between 1980 and 1990, and the twenty-first century. Second, through quantitative analysis of documents published in sources indexed in the bibliographic collection Web of Science, we outline the academic development of information security: in the world, Slovenia, and the Faculty of Criminal Justice and Security, University of Maribor. The findings indicate that relative to Slovenia's small size, researchers publish a significant number of documents, most of which are published by researchers from the Department of Information Security at the Faculty of Criminal Justice and Security University of Maribor.

Keywords: information security, cybersecurity, computer security, bibliometrics, information security history

https://doi.org/10.18690/um.fvv.3.2023.8 DOI
978-961-286-731-7 ISBN
University of Maribor Press

1 Uvod

Informacijska varnost je danes nepogrešljiv gradnik zagotavljanja varnosti na vseh ravneh. Ima številne operativne, taktične in strateške prednosti za organizacije, je ključnega pomena za celostno zagotavljanje nacionalne varnosti in varnosti kritične infrastrukture, obenem pa je sestavni del zagotavljanja mednarodne varnosti in stabilnosti. Čeprav zaradi potencialnih posledic kibernetskih napadov na stabilnost držav, gospodarstva in javno varnost pomembnost tovrstnega področja in discipline pretežno odmeva na višjih ravneh, informacijska varnost skozi zaščito raznoterih interesov, pravic in potreb pomembno prispeva tudi k osebni varnosti vsakega posameznika. Vloga informacijske varnosti v našem vsakdanjem življenju je predvsem zavarovati našo temeljno pravico, tj. varstvo osebnih podatkov. To vključuje zaščito finančnih podatkov, osebnih identifikatorjev, zdravstvenih podatkov, poslovnih in drugih zaupnih podatkov. Skozi onemogočanje pridobivanja in uporabljanja naših podatkov za nedovoljene namene pa prav tako pomaga ohranjati spoštovanje naše zasebnosti na pričakovani ravni. Je ključna tudi za preprečevanje različnih groženj, ki lahko resno poškodujejo naše naprave, sisteme in omrežja ali pa vodijo do zlorabe naših podatkov. Na splošno pa ima informacijska varnost ključno vlogo pri ohranjanju zaupanja v digitalni svet, zmanjševanju odpora do adopcije tehnologije in s tem spodbujanju kakovostnega življenja.

Skladno z raznoterimi cilji, vlogami in področji, ki jih pokriva informacijska varnost, gre za multidimenzionalni sistem oz. domeno, ki vključuje številna podpodročja. Razprave o informacijski varnosti se najpogosteje navezujejo na koncepte, kot so računalniška varnost, kibernetska varnost in varnost omrežij. Kot krovni koncept se informacijska varnost nanaša na zaščito podatkov in informacij, tako v digitalni kot fizični obliki. Računalniška varnost zaobsega zaščito računalniških sistemov (torej strojne, programske opreme in digitalnih podatkov) pred fizičnimi in kibernetskimi grožnjami. Kibernetska varnost se specifično ukvarja z zaščito sistemov (vključno s strojno opremo, programsko opremo, podatki), povezanih z internetom, pred kibernetskimi grožnjami. Omrežna varnost pa pomeni zaščito računalniških omrežij pred nepooblaščenimi dostopi ali napadi, kar vključuje zaščito vseh komponent omrežne infrastrukture, vključno s podatki, ki se prenašajo po omrežju. Gre torej za področja, ki se prepletajo, dopolnjujejo in prekrivajo ter skupaj delujejo pod okriljem celostnega sistema informacijske varnosti, da bi podatke, naprave, informacijske sisteme in omrežja zaščitila pred nepooblaščenim dostopom, uporabo,

spreminjanjem, razkritjem, motenjem, poškodovanjem ali uničenjem. V literaturi opredelitve neizogibno spremlja t. i. triada CIA, ki zaupnost, celovitost in dostopnost opisuje kot ključne atribute oz. ciljna stanja informacijske varnosti.

Čeprav je terminološka konceptualizacija informacijske varnosti danes razmeroma uveljavljena, gre za relativno mlado in stalno razvijajočo se stroko in disciplino, kar vpliva tudi na razvoj zmogljivosti in standardizacijo v praksi. Razvoj področja je bil (in še vedno ostaja) tesno povezan z (zgodovinskim) razvojem informacijske tehnologije (IT) in s tem povezanih izvornih disciplin ter strok. Čeprav je zametke informacijske varnosti oz. s tem povezanih ukrepov mogoče opaziti že pred razvojem in preboji na področju digitalnih računalnikov, telekomunikacij in interneta, se je intenzivnejši razvoj znanosti in posledično stroke dogajal sočasno z razvojem omenjenih inovacij in omogočitvenih tehnologij, ki so soustvarjale nova varnostna tveganja.

Zgodovina informacijske varnosti sega v petdeseta in šestdeseta leta prejšnjega stoletja oz. zgodnje dni računalništva, ko so se računalniki začeli širše uveljavljati v vojaškem, industrijskem in vladnem sektorju. V začetnih fazah se je informacijska varnost razvijala kot računalniška varnost – skladno z naravo delovanja računalnikov in shranjevanja podatkov je bil poudarek predvsem na ukrepih fizične zaščite računalniške opreme in prostorov pred fizičnimi grožnjami, kot so nepooblaščen dostop, kraja, poškodbe, nesreče ipd. S pojavom večnamenskih računalnikov in omrežij pa so računalniki postajali vse bolj razširjeni, povezani, podatki pa decentralizirani, s čimer je rasla potreba po bolj sofisticiranih metodah, intenzivneje pa sta se začela razvijati podpodročje omrežne varnosti in raziskovalna dejavnost. Ko so se pojavili prvi računalniški virusi in vdori, informacijska varnost postane uveljavljena tematika strokovnih razprav, začnejo pa se pojavljati tudi prve regulacije. S prebojem osebnih računalnikov in interneta v vsakdanje življenje ljudi in razvojem elektronskega poslovanja je nato prihajalo do širjenja virusov, vse več hekerskih napadov in spletnih prevar, zaradi česar je informacijska varnost doživela pravi razmah. V ospredje so se začela postavljati vprašanja, povezana z zasebnostjo, varnostjo osebnih podatkov, zaščito finančnih podatkov, intenzivneje so se razvijale tehnologije šifriranja, varni spletni protokoli in podpodročje kibernetske varnosti. Ob prehodu v novo tisočletje so države in organizacije začele informacijsko varnost obravnavati resneje in intenzivneje razvijati ter regulirati tovrstno področje. S tem je informacijska varnost prerasla svojo izvorno (tehnično) naravo in uveljavila status

samostojne (multidimenzionalne in interdisciplinarne) vede. Novo tisočletje je zaznamovala eksponentna rast, lahko bi rekli celo evolucija, kibernetskih groženj. Napadi so postajali vse bolj intenzivni, organizirani in skozi posledice pridobivali vse večjo razsežnost. Mega vdori, izsiljevalski in hektivistični napadi, napredne tehnike socialnega inženiringa, informacijsko bojevanje, informacijske propagande in širjenje lažnih novic, organizirani hekerski napadi ter širjenje kibernetske kriminalitete, kot storitve, so zgolj nekatere variacije in značilnosti sodobne kibernetske kriminalitete. Razvoj novih tehnologij (kot so računalništvo v oblaku, internet stvari, nosljive naprave, avtonomne naprave), uvajanje pametnih tehnologij in umetne inteligence v vse pore družbenega delovanja je privedel do obdobja velikih podatkov, vsesplošne digitalizacije in odvisnosti od IT, s čimer pa se neizogibno povečujejo tudi tveganja. Skladno s tovrstnimi trendi informacijska varnost ni postala prioriteta zgolj nacionalnih, temveč tudi mednarodnih varnostnih in razvojnih strategij, ki med drugim vključujejo tudi razvoj ofenzivnih, defenzivnih in skupnih odzivnih zmogljivosti, standardizacijo ter profesionalizacijo. Med tistimi, ki razvijajo tehnologije in varnostne ukrepe, ter tistimi, ki razvijajo nove tehnike odkrivanja in izkoriščanja njihovih ranljivosti, poteka stalna tekma. Zato je danes informacijska varnost pomembna disciplina in ena izmed najvrednejših industrij, v okviru katere potekajo intenzivna prizadevanja za razvoj naprednejših (inteligentnih in avtomatiziranih) zmogljivosti, tudi na območju kvantnega računalništva.

Z razvojem čez čas in ob boku drugih razvojnih trendov in družbenih izzivov je informacijska varnost torej pridobila več statusov; uveljavila se je kot stroka, poslovna funkcija, industrija, vzporedno pa tudi kot ena pomembnejših znanstvenih disciplin sodobnega časa. V tem poglavju je orisan zgodovinski pregled razvoja informacijske varnosti kot stroke ter znanstvenoraziskovalne dejavnosti po svetu in v Sloveniji, s poudarkom na raziskovalni dejavnosti Fakultete za varnostne vede Univerze v Mariboru. Namen je predstaviti, kako sta se sočasno razvijali stroka in znanost informacijske varnosti, izpostaviti ključne razvojne mejnike ter analizirati rezultate in dosežke v slovenski raziskovalni sferi.

2 Zgodovinski razvoj informacijske varnosti kot stroke

Natančno določiti začetke informacijske varnosti je zelo težko, saj obstajajo deljena mnenja o izvornih kontekstih. Vidnejši razvoj informacijske varnosti se večinoma povezuje s pojavom informacijske dobe, kjer so prav tako različna stališča glede

glavnih mejnikov – je to npr. razvoj telekomunikacij v devetnajstem stoletju; računalništva, omrežij in interneta v dvajsetem stoletju; ali družbenih medijev, neposrednega komuniciranja in vsesplošne digitalizacije v enaindvajsetem stoletju (Kessler, 2012)? Ne glede na to, pa je seveda splošne zametke informacijskih groženj in s tem povezane varnosti moč opaziti že bistveno prej v zgodovini razvoja človeške družbe. Konceptualno gledano pa se je informacijska varnost začela razvijati s pojavom potrebe po ohranitvi skrivnostnosti in monopola nad informacijami, kar sega v daljno zgodovino človeštva. Informacije so namreč vedno predstavljale moč in določeno prednost tistim, ki so jih posedovali. Ko so se informacije začele shranjevati z zapisi ali posredovati med ljudmi in se je želelo preprečiti njihovo uničenje, krajo ali pa ohraniti njihovo tajnost, takrat so se začeli izvajati tudi ukrepi, povezani z informacijsko varnostjo (Ibrahimova, 2020).

Dejavnosti, povezane z informacijsko varnostjo, segajo tudi v čas antike oz. razvoja hierarhičnega upravljanja in nadziranja družbenih struktur ter vojne umetnosti. V teh razmerah so se pojavljale grožnje varnosti podatkom in komunikacij, zametki razvoja kriptografije in zaščite zaupnosti komunikacij in pošiljk ter skrb za zagotavljanje zaupnosti, celovitosti in dostopnosti v upravljavskih ter birokratskih procesih (de Leeuw, 2007). Prav tako sta pomembna tudi čas industrijske revolucije in razvoj elektrike ter telekomunikacij. Ob pojavu radijskih sprejemnikov in oddajnikov se je zgodil tudi prvi (hekerski) napad, ko je prišlo do vdora v naprave in posredovanja neželenih sporočil (Ibrahimova, 2020). Devetnajsto stoletje je pomembno tudi zaradi zametkov na področju računalniške discipline, ki se je začela vidneje razvijati z začetki modernih računalnikov oz. mehanskih strojev za računanje. Kljub takšnim daljnim koreninam pa so se sodobni pogledi na informacijsko varnost, ki jo obravnavajo kot multidisciplinarno znanost in stroko, ki zahteva veliko več kot zgolj tehnične rešitve, uveljavili šele v zadnjih dveh desetletjih (Anderson in Moore, 2009).

Četudi je literatura, ki bi predstavljala sistematične preglede zgodovinskega razvoja informacijske varnosti zelo skopa, celostnih povzetkov oz. posnetkov praktično ni, v nadaljevanju skozi prizmo razvoja informacijske dobe povzemamo ključne časovne mejnike in njihove značilnosti. Je pa pri tem treba omeniti, da so izpostavljeni zgolj nekateri, za razvoj informacijske varnosti, pomembni dogodki in okoliščine, saj vseh razmer ni mogoče popisati, obenem pa je do nekaterih idej in s tem zametkov razvoja tehnologij, storitev ter s tem povezanih groženj prišlo že prej. Prav tako je ob prebiranju nujno upoštevati, da razvoj ni potekal v tako strogo

definiranih in ločenih obdobjih, saj je šlo za kontinuiran napredek. V nadaljevanju so torej postavljeni časovni mejniki, ki so zaznamovani z določenimi preboji oz. inovacijami in v katerih so postali aktualni določeni vidiki, pomembni za razvoj področja informacijske varnosti. Obdobja in njihove značilnosti so povzeta po Chadd (2020), Ibrahimova (2020), Kesslerju (2012), von Solmsu (2010), Whitmanu in Mattordu (2012) ter poznavanju področja avtorjev prispevka.

2.1 Obdobje do šestdesetih let (< 1960)

Vidnejši razvoj informacijske varnosti se je začel v vladni, vojaški in diplomatski sferi, kjer je vedno obstajala visoka težnja po zasebnosti in skrivnostnosti. Z razvojem prvih digitalnih računalnikov v vojaške namene, se je razvila potreba po računalniški varnosti – tj. potreba po zaščiti fizičnih lokacij oz. centrov, kjer so bili nameščeni računalniki, ter varnosti strojne in programske opreme. Ta se je okrepila predvsem med drugo svetovno vojno. Takrat so bili razviti prvi veliki (večtonski) elektronski računalniki za pomoč pri »razbijanju« šifriranih komunikacij, kar je prav tako vplivalo na razvoj tehnik dešifriranja. Pri teh računalnikih so se podatki shranjevali na luknjanih karticah in drugih fizičnih pomnilnikih. V obdobju do šestdesetih je potekal nasploh intenziven razvoj pomnilnikov (od luknjanih kartic, luknjanjih trakov in magnetnih trakov ter magnetnih bobnov do trdih oz. magnetnih diskov) in funkcij operacijskih sistemov.

V teh zgodnjih letih je bila informacijska varnost preprost proces, sestavljen pretežno iz ukrepov fizične varnosti, nadzora dostopa in enostavnih shem klasifikacije dokumentov. Primarne grožnje varnosti računalnikom in podatkom so bile povezane s fizičnim dostopom, zato so glavni problem predstavljale fizične kraje, vohunjenje, sabotaže in naravne ter druge nesreče. Za zaščito teh velikih računalnikov in ohranjanje celovitosti njihovih podatkov se je začelo uvajati več stopenj varnosti, kar zaznamuje pojav večnivojske varnosti. Dostop do vojaških lokacij in vstope v prostore so denimo nadzorovali z značkami, ključi in identifikacijo pooblaščenega osebja, ki so ga opravljali varnostniki. Šifriranje komunikacij, kot eden izmed ključnih vojaških taktik, pa je sicer eden prvih in še danes najpomembnejših ukrepov zagotavljanja zaupnosti komunikacij in podatkov. V tem času je bila informacijska varnost zgolj sestavni del discipline računalništva in področja razvoja informacijskih tehnologij. Omeniti velja, da je to obdobje zaznamovano tudi s koreninami tehnološkega hekanja. Konec petdesetih let so se

namreč začeli pojavljati vdori v telefonske sisteme za opravljanje brezplačnih klicev (ang. *phone phreaking*), ki pa so bili bolj aktualni v naslednjih desetletjih.

2.2 Obdobje med šestdesetimi in osemdesetimi leti (1960–1980)

Na začetku tovrstnega časovnega obdobja so bili računalniki še vedno pretežno centralizirani in so delovali na temeljih osnovnih terminalov, se pa je povečevala zapletenost in sofisticiranost nalog, ki so jih opravljali. Med hladno vojno je bilo v uporabi veliko več velikih računalnikov, ki jim je bilo treba omogočiti lažjo komunikacijo – poenostaviti je bilo treba okorne postopke pošiljanja magnetnih trakov med računalniškimi centri. Kot odgovor na to potrebo je agencija za napredne raziskovalne projekte ameriškega ministrstva za obrambo (*Advanced Research Projects Agency – ARPA*) začela proučevati izvedljivost redundantnega omrežnega komunikacijskega sistema, ki bi podprl izmenjavo vojaških informacij. Na tej osnovi je bil nato v šestdesetih letih razvit ARPANET (ang. *Advanced Research Projects Agency Network*), ki danes velja za predhodnika interneta. Konec šestdesetih let je bilo preko omenjenega omrežja poslano prvo elektronsko sporočilo, njegov razvoj pa se je intenzivneje nadaljeval v sedemdesetih letih, do osemdesetih pa je bilo nanj povezanih že več sto računalnikov.

Sedemdeseta leta je zaznamoval tudi razvoj mikroprocesorjev, kar je omogočilo krepitev zmogljivosti računalnikov in njihovega gospodarnejšega delovanja. V tem času se je nadaljeval razvoj pomnilnikov (disket, optičnih, bliskovnih in polprevodniških pomnilnikov), mikroračunalnikov, večopravilnih in večuporabniških operacijskih sistemov ter grafičnih uporabniških vmesnikov. To je predstavljalo temelje za razvoj in ugodne pogoje za komercializacijo osebnih računalnikov v naslednjem obdobju. S tem se je začela tudi nova doba v računalništvu, ki je bila zaznamovana s selitvijo računalnikov v različna okolja izven podatkovnih centrov.

V tem razvojnem obdobju je bila večina groženj še vedno pretežno vezana na dogajanje v fizičnem okolju, so se pa začele pojavljati tudi druge grožnje, kot npr. prve večje napake sistemskih administratorjev pri upravljanju sistemov, ki so ogrozile varnost podatkov in gesel. V raziskovalne namene je bil v sedemdesetih letih razvit tudi prvi eksperimentalni samorazmnoževalni program oz. računalniški črv *Creeper*. Sočasno je bil z namenom odstranjevanja tega črva razvit tudi prvi

antivirusni program *Reaper*. Čeprav prvi računalniški črv ni bil škodljive narave, so bili s tem postavljeni temelji za razmah zlonamerne programske opreme v naslednjih obdobjih. V okviru eksperimentiranja z zmogljivostmi sistemov so se v šestdesetih letih začele izvajati tudi različne oblike testiranja njihovega delovanja, kar je ustvarjalo močnejše zametke hekerske skupnosti.

Informacijska varnost je bila sprva tako še vedno pretežno osredotočena oz. omejena na fizične in logične kontrole (nadzor dostopa), razvijati pa so se začeli tudi tehnični ukrepi, kot so preproste oblike identifikacije, avtentikacije za prijave v sisteme in zelo grobe oblike avtorizacije. Večina teh funkcij je bila skoncentrirana v operacijskih sistemih, z njimi pa so upravljali tehnični kadri oz. administratorji. S širjenjem ARPANET so namreč naraščala tudi tveganja za zlorabe, zato so se začele intenzivnejše razprave o nevarnostih nepooblaščenega oddaljenega dostopa, ranljivosti gesel, neustreznih postopkih identifikacije in avtorizacije v sistemu. Konec šestdesetih in začetek sedemdesetih let se je, zaradi interesov vojaške in obrambne skupnosti, začelo razvijati bolj zapleteno in tehnološko bolj izpopolnjeno računalniško zaščito. Vidnejše gibanje k informacijski varnosti, ki presega zgolj fizično zaščito, se je začelo z raziskavami v sedemdesetih letih. V tem času je pod okriljem ARPA nastalo raziskovalno poročilo »*Protection analysis – final report*« (Bisbey in Hollingworth, 1978), v katerem so se raziskovale ranljivosti operacijskih sistemov ter dokument »*Security Controls for Computer Systems*« (Ware, 1979), v katerem so bila podana opozorila, da povečevanje omrežnih komponent v informacijskih sistemih povečuje tveganja, ki jih z varnostnimi mehanizmi, ki so bili do takrat v uporabi, ni mogoče ustrezno nasloviti. V tem poročilu so opredelili različne mehanizme in kontrole, potrebne za zaščito večnivojskih računalniških sistemov, ter izpostavili vlogo managementa in politike v sistemu varnosti. Poudarilo se je pomembnost varnosti podatkov, upravljanja s kontrolo dostopa in vključevanje različnih ljudi v sistem varnosti. Med znanimi dokumenti tega desetletja je tudi Andersonovo poročilo »*Computer Security Technology Planning Study«,* izdano v dveh serijah (Anderson, 1972a; 1972b) in izdelano za potrebe računalniške varnosti ameriškega vojnega letalstva.

Strokovne razprave in objave na temo informacijske varnosti v sedemdesetih in v začetku osemdesetih so se torej pretežno nanašale na fizično varnost, varnost računalnikov, varnost gesel, ranljivosti operacijskih sistemov in njihovo zaznavanje ter zaščito uporabniških podatkov. Obdobje do osemdesetih let dvajsetega stoletja

se zato v literaturi imenuje tudi kot t. i. tehnični val informacijske varnosti. Vidiki, kot so politike informacijske varnosti ali ozaveščenost uporabnikov računalnikov, v tem času še niso bili visoka prioriteta, se je pa vse bolj poudarjala tudi vloga uporabniškega oz. človeškega vidika in upravljavskih procesov.

2.3 Obdobje osemdesetih in devetdesetih let (1980–2000)

Pojav porazdeljenega računalništva in osebnega računalnika sta glavna trenda, ki zaznamujeta obdobje pred novim tisočletjem. Decentralizacija, ki ima začetke v osemdesetih letih, je spodbudila razmah omrežij in s tem povezovanje računalniških zmogljivosti. V začetku osemdesetih so se razvijali novi standardi in protokoli za lokalna omrežja, kot je npr. nova verzija Etherneta. Omrežja in računalniki v različnih okoljih so postajali vse pogostejši kakor tudi potreba po njihovem povezovanju, kar je, skupaj s protokolom TCP/IP, privedlo do razvoja interneta oz. prvega globalnega omrežja omrežij. Tudi internet se je, tako kot računalniki, postopno komercializiral in prešel iz vladne, akademske in industrijske sfere v domeno splošne javnosti, kar je ustvarilo podlago za hiter razvoj, inovacije in preboje na področju računalniške tehnologije. Skladno s tem informacije niso bile več shranjene na enem osrednjem dobro zaščitenem računalniku, kot v preteklosti, ampak so bile porazdeljene med veliko namiznih računalnikov, povezanih z omrežji, kar je ustvarjalo nova resna varnostna tveganja. Konec osemdesetih zaznamuje tudi pojav komercialnih antivirusnih programov in varnostnih podjetij, devetdeseta leta pa je med drugim zaznamoval razvoj brezžičnih omrežij.

Začetki uvajanja interneta so temeljili na osnovnih standardih, ki so varnost obravnavali kot nizko prioriteto. Pravzaprav je veliko težav, ki danes ogrožajo podatke, komunikacijo in varnost na internetu, rezultat tega zgodnjega pomanjkanja varnosti. Takrat, ko je bila uporaba interneta in elektronske pošte omejena na relativno manjše število verodostojnih uporabnikov, preverjanje pristnosti na ravni strežnikov in šifriranje e-pošte npr. nista bila potrebna. Ko pa so omreženi in decentralizirani računalniki postali prevladujoč slog računalništva, zgolj fizično varovanje omrežja ni več zadostovalo. V zgodnjih osemdesetih letih prejšnjega stoletja so se še naprej pojavljala opozorila, da skrb za informacijsko varnost ni ustrezna, zato so se začeli organizirati prvi strokovni odbori za informacijsko varnost in centri za odzivanje ter prve mednarodne konference. Čeprav države in vlade na začetku internetne dobe niso posvečale večje pozornosti računalniškim grožnjam, se

je mentaliteta kmalu spremenila. Z razvojem kazenske zakonodaje se je okrepilo nadzorstvo in kaznovalna politika na področju kibernetske kriminalitete. Konec osemdesetih let se denimo začnejo oblikovati prvi predpisi oz. zakonodaja s področja računalniške in kibernetske kriminalitete (npr. *Computer Fraud and Abuse Act* iz leta 1986). Države so sicer sprva delovale bolj reaktivno in raje kaznovale storilce, kot pa vlagale v razvoj varnostnih sistemov, vendar ta potreba ni bila spregledana na mednarodni ravni. V mednarodnih organizacijah, kot so Organizacija za gospodarsko sodelovanje in razvoj (OECD), Organizacija združeni narodov (OZN), Evropska unija (EU) in zveza NATO, so začeli zaposlovati vse več raziskovalcev in strokovnjakov za informacijsko in kibernetsko varnost. Na začetku devetdesetih let je OECD pripravila ene izmed prvih smernic za varnost informacijskih sistemov in omrežij z mednarodnim statusom (*OECD Guidelines for the Security of Information Systems and Networks* iz leta 1992), nekaj let kasneje pa sledi razvoj varnostnih protokolov in dobrih praks v obliki standardov (eden izmed prvih znanih standardov s področja upravljanja informacijske varnosti je npr. BS 7799 iz leta 1995). Do konca devetdesetih let se uveljavi tudi koncept triade CIA kot temelj informacijske varnosti.

Z razmahom interneta se je začel tudi intenzivnejši razvoj kibernetskih groženj. Fizična prisotnost storilcev oz. fizičen dostop do sistemov je namreč postal nepomemben dejavnik v izvedbi napadov, saj so sedaj lahko storilci napadali uporabnike z drugega konca sveta. V devetdesetih letih se je spam razširil iz klasične pošte in faksov na elektronsko pošto, kar je utrlo pot širjenju zlonamerne programske opreme in raznovrstnim prevaram. Resnejši in zlonamerni hekerski napadi so se sicer začeli dogajati že konec sedemdesetih, močneje pa nadaljevali v osemdesetih letih dvajsetega stoletja, ko so se oblikovale tudi hekerske skupnosti. Ta čas so zaznamovali predvsem računalniški črvi, spremljali pa so jih tudi razvoj trojanskih konjev, zametki izsiljevalskega programja in pojav hekerskih vdorov večjega profila (v vladne oz. državne organizacije). Do sredine devetdesetih let je opaziti pravo eksplozijo v širjenju kibernetske kriminalitete. Številni virusi so uporabljali nove tehnike in inovativne metode, vključno z zmožnostjo prikrivanja, polimorfizmom in »makro virusi«, kar je ustvarilo nove izzive za razvijalce antivirusnih programov, ki so morali razviti nove zmožnosti zaznavanja in odstranjevanja.

Informacijska varnost je skladno z opisanimi trendi v devetdesetih letih doživela ogromen preboj. Postala je tematika, ki je pridobivala vse več pozornosti, ne le raziskovalcev, temveč tudi pri vodstvu organizacij. Vse bolj se je uveljavljalo razumevanje, da ima informacijska varnost več razsežnosti kot le tehnično in da je ključnega pomena za odpornost ter strateško prihodnost organizacij. Organizacije so začenjale imenovati vodje informacijske varnosti, razvijati varnostne politike in postopke ter postopno v organizacijske strukture vpeljevati oddelke za informacijsko varnost. Krepilo se je tudi zavedanje, da lahko zaposleni predstavljajo veliko ranljivost in tveganje za informacijsko varnost. Zaposleni kot končni uporabniki so prihajali v ospredje razprav, s čimer se je krepil pomen človeške dimenzije in multidimenzionalen pogled na informacijsko varnost. S tem se je začelo krepiti tudi ozaveščanje zaposlenih, razvijati so se začeli tečaji za zaposlene za krepitev osebne in organizacijske varnostne kulture.

Organizacije so začele proučevati najboljše prakse in možnosti standardizacije, ukvarjale so se z izzivi, kako se primerjati s konkurenco, kaj naj vsebuje politika informacijske varnosti, kako urediti sistem merjenja in poročanja ter kako pridobiti uradna potrdila oz. certifikate, ki dokazujejo status zrelosti informacijske varnosti. Organizacije so tako začele razvijati procese merjenja zrelosti in razvitosti, ocenjevanja skladnosti in poročanja vodstvu. Redne tematike vodstvenih srečanj so tako postala tudi vprašanja glede zasebnosti in varnosti podatkov. Organizacije so se pričele bolje zavedati tudi pomanjkljivosti enega omrežnega požarnega zidu. Za ustrezno zaščito svojih sredstev so potrebovale različne požarne pregrade, sisteme za odkrivanje in preprečevanje vdorov, pregledovalnike ranljivosti in druge zmogljivosti, kar je postopno rezultiralo v razvijanju t. i. globinske zaščite. Ob prehodu v novo tisočletje se v stroki ustali stališče, da je informacijska varnost odgovornost celotne organizacije in mora postati del organizacijske kulture in razmišljanja. Glede na omenjene značilnosti se tovrstno obdobje lahko poimenuje tudi kot managerski val informacijske varnosti, ki je potekal vzporedno s t. i. institucionalnim valom.

2.4 Enaindvajseto stoletje (> 2000)

Napredek v razvoju informacijske tehnologije se je najbolj intenzivno dogajal zadnjih štirideset let. Konec dvajsetega stoletja so se zgodili ključni preboji v zmogljivostih računalniške tehnologije in omrežij, medtem ko novo tisočletje

zaznamujejo številne inovacije in razrast informacijskih ter kibernetskih tveganj. Varnostnim sistemom, zaradi želje po hitrem napredku v razvoju tehnologije, prioritizaciji funkcionalnosti in ciljev po čim hitrejšem preboju, ni uspelo slediti inovacijam. Danes je praktično vsaka novost in inovacija povezana s kakšno ranljivostjo, ki jo je mogoče izkoristiti z obstoječimi ali novimi vektorji napadov.

V novem tisočletju je internet omogočil neprekinjeno povezovanje milijonov različnih omrežij po celotnem svetu, kar je skupaj z razvojem novih rešitev pospešilo proces digitalizacije. Osebni in finančni podatki organizacij in posameznikov so se vse bolj shranjevali in obdelovali na računalnikih, varnost podatkov, shranjenih na računalniških in elektronskih napravah, pa je postala odvisna od varnosti vseh povezanih naprav. Organizacije so odkrile komercialno stran interneta in se vključile v tekmovanje za prevzem prednosti na področju spletnega in elektronskega poslovanja. Stranski učinek tega so bile hitre inovacije na področju informacijskih sistemov in aplikacij, ki temeljijo na internetu in spletu in so postale na voljo milijonom strank in uporabnikom po celotnem svetu.

To je predstavljalo vstop v kibernetsko dobo. Med pomembne mejnike v razvoju IT v novem tisočletju, ki so imeli pomemben vpliv tudi na informacijsko varnost (tako z vidika ranljivosti kot zmogljivosti) sodi razmah družbenih omrežij, elektronskega bančništva, spletnega nakupovanja, mobilnih, pametnih, nosljivih in drugih omreženih (IoT) naprav, računalništvo v oblaku, strojno učenje in umetna inteligenca oz. vsesplošna digitalizacija in informatizacija vseh vidikov našega življenja, dela, učenja, razvoja ter družbenega upravljanja. Z razmahom kompleksnosti omrežij in napredne tehnologije se je povečevalo zavedanje pomembnosti informacijske varnosti za nacionalno varnost, politično stabilnost, varnost kritične infrastrukture in stabilnost gospodarstva. Na začetku novega tisočletja se na mednarodni ravni potrdi tudi prvi sporazum – Konvencija o kibernetski kriminaliteti (Svet Evrope, 2001) (imenovana tudi kot Budimpeška konvencija) o poenotenju inkriminacije in odzivanja na kibernetsko kriminaliteto.

Na področju informacijske varnosti je bil razvoj usmerjen v nadgradnjo zmogljivosti, ki so se gradile že v prejšnjem stoletju, cilj pa je bil preseči ozke usmeritve in segregacijo s povezovanjem področij, odgovornosti in vidikov. Do začetka enaindvajsetega stoletja so bile namreč razvojne iniciative usmerjene predvsem navznoter; v zaščito organizacij in njihovih meja, varnost njihovih informacij in

podatkov oz. zagotavljanje zaupnosti in celovitosti podatkov, v preprečevanje neavtorizirane uporabe, prevar in zlorab. Razlog je v tem, da je bila odgovornost za zagotavljanje informacijske varnosti osredotočena predvsem na organizacije in podjetja, ki so upravljala s podatki in uporabnikom zagotavljala storitve. Organizacije so uvajale močne varnostne ukrepe, ki so onemogočali dostop kriminalcem, in tako je v mnogih primerih IT infrastruktura organizacij postala dobro zaščitena utrdba. Po letu 2000 so se intenzivneje razvijali tudi novi standardi, v katerih se je poudarjal pomen sistematičnega upravljanja informacijske varnosti. Upravljanje informacijske varnosti je tako postalo pomemben del strateškega upravljanja organizacij, kar imenujemo upravljavski val informacijske varnosti. Neposredna posledica tega pa je bila, da so kriminalci začeli preusmerjati njihovo pozornost v končne uporabnike. Internet, kot splošno dostopen medij z milijoni končnih uporabnikov, in nizka raven ozaveščenosti oz. znanja o informacijski varnosti med uporabniki sta spodbudila storilce k razvijanju in uporabi širokega nabora napadalnih mehanizmov, usmerjenih proti končnim uporabnikom. Napadi, povezani s socialnim inženiringom, kot sta phishing in spoofing, in usmerjeni v končne uporabnike, so postali bistveno bolj napredni in intenzivni. Okužbe z zlonamerno programsko opremo niso več povezane z nalaganjem datotek, ampak potekajo samodejno preko vstavljanja ali ponarejanja legitimnih spletnih mest, novost v tem obdobju pa so tudi napadi preko kanalov direktnega sporočanja. Obenem je značilen pojav napadov ničelnega dne, ki izkoriščajo varnostne ranljivosti v novih rešitvah in zanje še ne obstajajo varnostni popravki, kar predstavlja velik izziv za varnostno skupnost in uporabnike. S širjenjem socialnega življenja v družbena omrežja in raznovrstna spletna okolja pa zasebnost ljudi ni bila nikoli tako ogrožena, kot je danes. Novo tisočletje so zaznamovali tudi veliki oz. mega vdori, DDoS napadi ogromnih razsežnosti, napadi z izsiljevalsko programsko opremo in razmah kompleksnejših, organiziranih ter hibridnih kibernetskih groženj, med drugim tudi informacijskega bojevanja.

Zadnjih dvajset let je informacijska varnost tudi v obdobju t. i. kibernetskega vala, ko se strokovnjaki ukvarjajo z izzivi preprečevanja, odkrivanja in preiskovanja kibernetske kriminalitete. Širjenju kibernetskih groženj in vse večjim ranljivostim sledi razvoj naprednejših oblik avtentikacije, omrežne analitike in spletnih požarnih pregrad, testnih in navideznih okolij, inteligentnega zaznavanja in avtomatskega odzivanja na incidente, odkrivanja ranljivosti, nadzorstva in zaščite v realnem času, podvajanja zmogljivosti in virov. Obenem so se pojavljala opozorila, da na področju informacijske varnosti primanjkuje ustreznih sistemov profesionalizacije,

izobraževanja, kodeksov etik, natančno definiranih vlog in odgovornosti ter nasploh upravljavskih teles, ki bi spodbujale razvoj teh poklicev. V zadnjem desetletju se je zato začelo intenzivneje razvijati mednarodne in nacionalne strategije kibernetske varnosti, ustanavljati centre in delovna telesa za pomoč pri regulaciji, odzivanju na napade in standardizaciji ukrepov, usklajevati stališča glede ključnih digitalnih kompetenc, kadrovskih profilov, urejati poenotene sisteme izobraževanja za različne strokovnjake in formalizirati njihov status ter vloge. Veliko pozornosti je usmerjene tudi v urejanje kazenskopravnih sistemov in mednarodnega sodelovanja pri preiskovanju in pregonu kibernetske kriminalitete. Danes je prisotnih veliko iniciativ in strokovnih združenj, ki razvijajo to področje, opozarjajo na ranljivosti in nevarnosti ter sodelujejo v sistemih razvoja obrambnih zmogljivosti, kljub močnemu napredku pa med ključne aktualne izzive še vedno sodi akutno pomanjkanje kadrov oz. strokovnjakov s področja informacijske in kibernetske varnosti.

3 Razvoj raziskovalne dejavnosti na področju informacijske varnosti

3.1 Razvoj v svetu

Da bi znanstveno literaturo pregledali karseda celovito, smo naše iskanje relevantne literature izvedli v bibliografski zbirki *Web of Science* (WoS). Ker je v literaturi mogoče zaslediti informacijsko, kibernetsko in računalniško varnost kot sinonime (čeprav temu vsekakor ni tako), je naš iskalni niz zajemal prav te tri pojme: »*information security«, »computer security«* in *»cybersecurity«*. Med pojme je bil umeščen logični operator »OR«, pojem kibernetska varnost pa je bil zapisan na vse tri načine, kot je pogosto najden v literaturi: »*cybersecurity*«, »*cyber security*« in »*cyber-security*«. Iskanja nismo omejevali drugače kakor s tipom dokumenta. Iskali smo zgolj med znanstvenimi članki in konferenčnimi prispevki, iskanje pa izvedli v *WoS Core Collection*.

Iskalni niz je na 4. januarja 2023 vrnil 65.844 zadetkov med letoma 1970 ter 2023. Članki in konferenčni prispevki so bili objavljeni v 13.189 različnih virih. Vse zadetke smo izvozili v obliki *»Plain text«* z vsemi postavkami, ki jih WoS hrani za vsak posamezni vnos ter jih analizirali v razvojnem okolju *Rstudio* ter s paketom *Bibliometrix* in *Microsoft Excel*. Osnovne lastnosti podatkovne zbirke analiziranih člankov so razvidne v tabeli 1.

Tabela 1: Osnovni podatki podatkovne zbirke

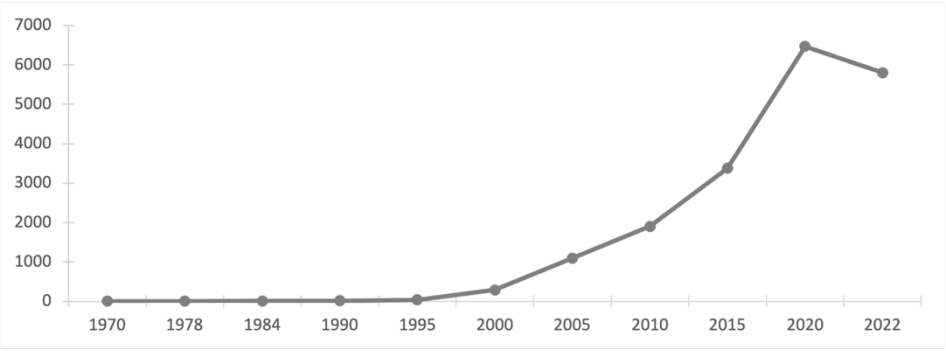
Postavka	Vrednost
Podatki o dokumentih	
Število virov (revije, knjige, zborniki), iz katerih izhajajo analizirani dokumenti	13.189
Število dokumentov	65.844
Povprečno število citatov za posamezni dokument	8,28
Povprečno število citatov za posamezni dokument na leto	1,12
Število člankov (revije, poglavja knjig)	27.895
Število konferenčnih prispevkov	37.949
Podatki o avtorjih	
Število avtorjev (unikatnih)	83.503
Število avtorjev (pojavnost)	218.920
Število avtorjev dokumentov z enim avtorjem	5.128
Število avtorjev dokumentov z več avtorji	78.375
Število dokumentov z enim avtorjem	8.157
Povprečno število dokumentov na avtorja	0,789
Povprečno število soavtorjev na dokument	3,32

Vsebinsko so se prvi avtorji s področja informacijske, kibernetske in računalniške varnosti osredotočali na družbene in pravne vidike informacijske varnosti. Gre za približno desetletno obdobje, ko so raziskovalci z družboslovnih področij (prava, državnih oblasti, ekonomije, sociologije) opozarjali predvsem na izzive in probleme povezane z varnostjo računalnikov (List, 1973; Scheidermayer, 1970). Šele kasneje so se začeli pretežno pojavljati prispevki s tehnično vsebino.

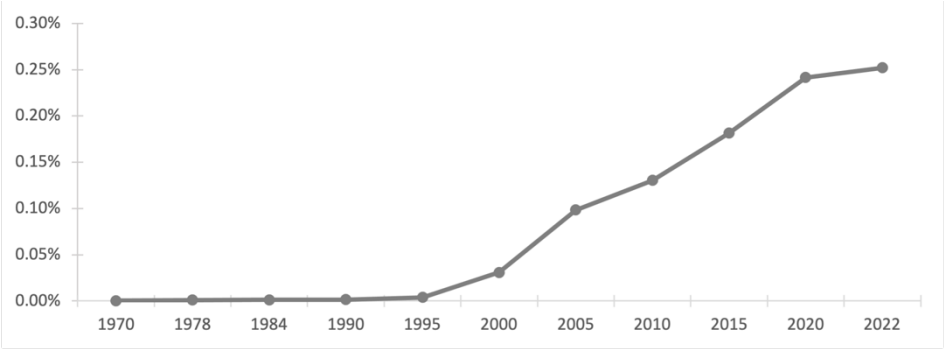
3.1.1 Zgodovinska rast področja

Rast števila objav področja informacijske in kibernetske varnosti smo analizirali skozi število indeksiranih objavljenih dokumentov za vsako leto posebej. Slika 1 prikazuje rast števila objavljenih dokumentov skozi zgodovino. Informacijska varnost (na začetku pogosteje imenovana računalniška varnost, saj sta se praksa in znanost osredotočali predvem na varnost računalnikov) se je kot znanost pojavila s pojavom računalnikov. Tako spada med mlajše znanosti, predvsem ko jo primerjamo z ostalimi naravoslovnimi področji, kot so denimo matematika, fizika, biologija, kemija, in družboslovno-humanističnimi področji, kot so denimo sociologija, filozofija in pravo. Tako večjega števila znanstvenih dokumentov pred pojavom računalnikov v industriji in domači rabi ni mogoče pričakovati. Prvi vzpon se je zgodil sredi devetdesetih let, močnejši vzpon pa je zaznati po letu 2000, ko se je število objavljenih dokumentov v letu 2005 v primerjavi z letom 2000 več kot potrojilo. V letu 2022 je bilo objavljeno skoraj 600 % več prispevkov kot leta 2005.

Skupna povprečna letna rast števila dokumentov s področja informacijske, kibernetske in računalniške varnosti znaša 10,27 %.



Slika 1: Število objavljenih dokumentov skozi zgodovino.
Vir: lasten.



Slika 2: Delež objavljenih dokumentov s področja informacijske, kibernetske in računalniške varnosti skozi leta v primerjavi z vso indeksirano literaturo v WoS.
Vir: lasten.

Ker gre v tem primeru za absolutno število objavljenih prispevkov in gre za relativno mlado znanost, slika 2 prikazuje delež prispevkov s področja informacijske, kibernetske in računalniške varnosti glede na vso indeksirano literaturo v bibliografski zbirki WoS. Prvi vzpon v deležu je zaznati podobno kot na sliki 1 sredi devetdesetih let, kar lahko povezujemo z razmahom in popularizacijo interneta in močnemu porastu uporabe osebnih računalnikov. Razlika med absolutnim (slika 1) in relativnim številom (slika 2) objavljenih prispevkov je ta, da je vzpon relativnega števila mogoče zaznati že prej (pri prvem vzponu leta 1995), raste pa tudi v letu 2022, medtem ko je absolutno število vseh v WoS indeksiranih dokumentov padlo. Tako

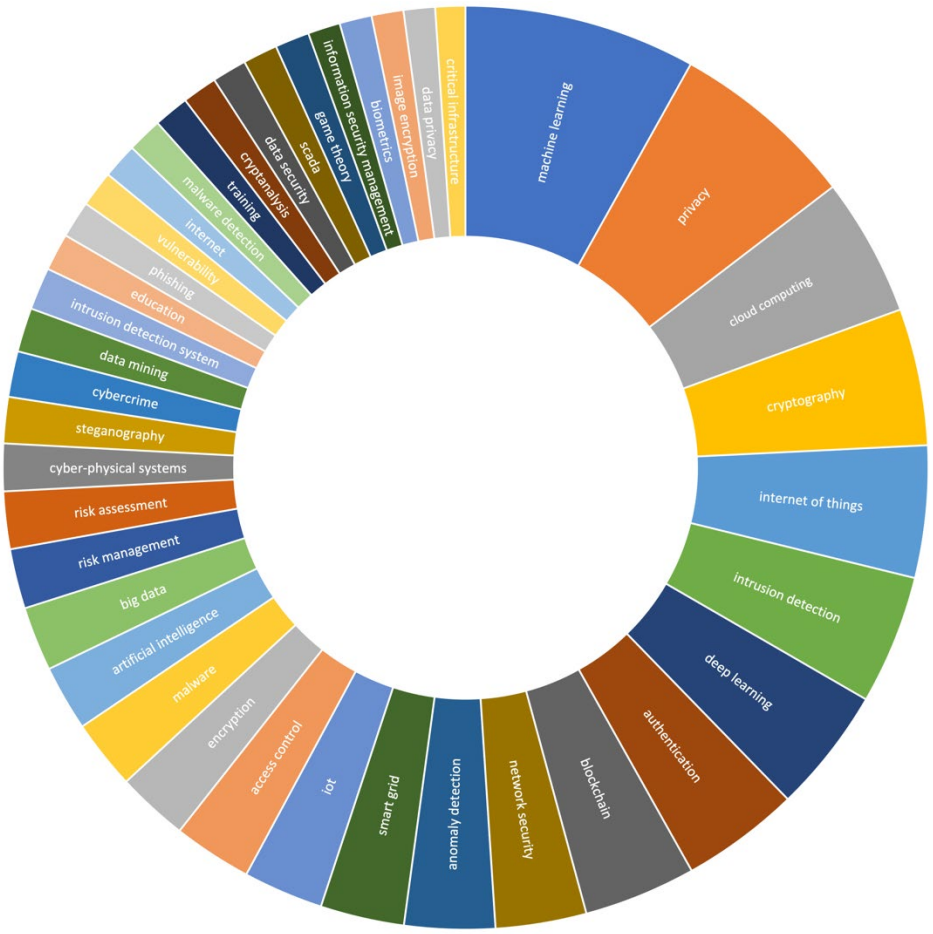
gre pričakovati, da bo tudi v prihodnje raziskovalno področje s področja informacijske in kibernetske varnosti naraščalo, kar gre vsekakor pripisovati vse intenzivnejši digitalizaciji vseh vidikov družbe.

3.1.2 Teme informacijske varnosti v literaturi

Ključne teme informacijske varnosti v literaturi smo analizirali skozi analizo frekvenc ključnih besed avtorjev. Iz nabora smo izključili iskalne pojme *information security*, *cybersecurity*, *cyber-security* in *computer security*. Rezultati so prikazani na sončnem diagramu (slika 3). Sledijo vzorcu števila objav po letih, ki smo jih prikazali v podpoglavju 3.1.1. Tako lahko med najpogostejšimi ključnimi besedami zasledimo teme, ki so se pogosteje začele pojavljati v zadnjih letih, kot npr. strojno in globoko učenje, ki je v kontekstu informacijske in kibernetske varnosti najpogosteje uporabljeno za prepoznave anomalij in s tem odkrivanju zlonamerne programske opreme ali prepoznavanju potencialnih napadov na informacijske sisteme. Ob navedenih pa se pojavljajo tudi teme o zasebnosti, kar odraža skrb za dobrobit informacijske družbe ter novejše teme, kot so internet stvari, oblačno računalništvo in tehnologija blockchain. S tem ugotavljamo, da v literaturi prevladujejo tehnične teme, saj poleg omenjenih zasledimo tudi teme, povezane z avtentikacijo, kriptografijo, enkripcijo, pametnimi mrežami. Skupaj tehnične teme zavzemajo več kot polovico vseh raziskovalnih tem, ki so povezane z informacijsko in kibernetsko varnostjo. Med najpogostejšimi netehničnimi temami pa zasledimo predvsem analizo in obvladovanje tveganj, upravljanje informacijske varnosti, zvabljanje, informacijskovarnostno izobraževanje in usposabljanje, kibernetsko kriminaliteto in teme, povezane s spletom. Čeprav je druga napogostejša ključna beseda zasebnost, ki bi jo tradicionalno umestili med netehnične teme, ne moremo mimo dejstva, da je v literaturi pogosto zaslediti tehnične rešitve, ki (kar najbolje) zagotavljajo zasebnost. Tako je nedvoumno ni mogoče umestiti niti med tehnične niti med netehnične raziskovalne teme.

Skozi rast ključnih besed lahko identificiramo najnovejše trende, ki so se razvili skozi leta. Slika 4 prikazuje raporeditev frekvenc najpogostejših besed skozi posamezna leta. Prikazana je rast posamezne ključne besede, pri čemer so najpogostejše besede izpuščene (*information security, security, cybersecurity, cyber security* in *cyber-security*). S slike je razvidno, da je daleč najpogostejša beseda *machine learning* (strojno učenje), ki je začela najmočnejšo rast leta 2012, še močnejšo pa leta 2015. Od tedaj do leta 2022 je število

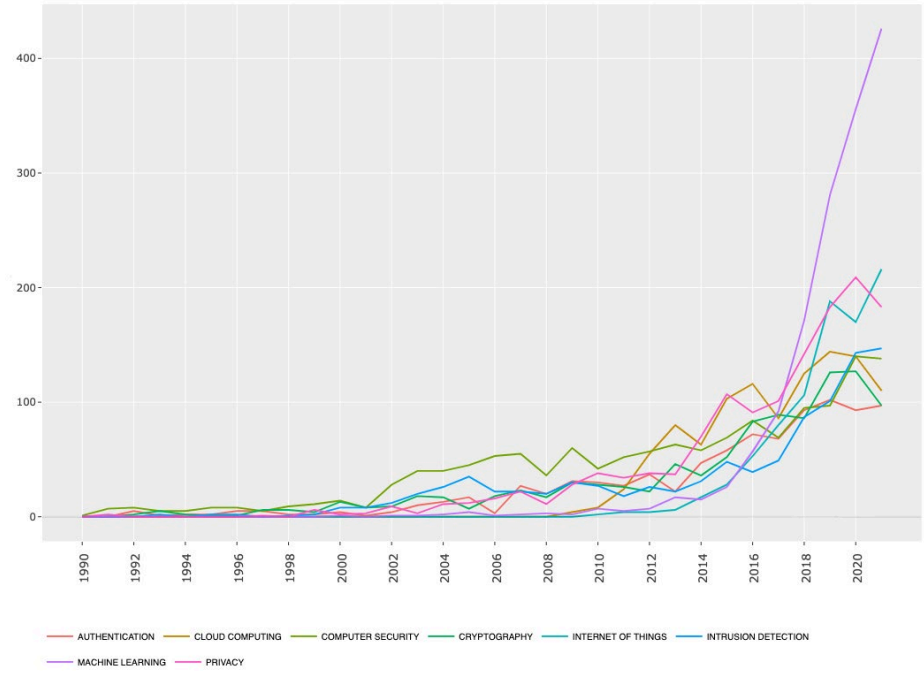
člankov na temo strojnega učenja zraslo za več kot 400 %. Podobno je z zaznavo vdorov, ki je pogost dvojček strojnega učenja, le da se je rast te teme začela že pred letom 2000. Nekoliko drugače je z raziskovanjem zasebnosti. Ta postopoma raste že od 2004, nekoliko več pozornosti pa je prejela med letoma 2013 in 2015, največji skok pa doživela med letoma 2017 in 2020. Med temami, ki so hitro začele rasti (pred tem pa bile skorajda neobravnavane) po letu 2010 sodita kriptografija in oblačno računalništvo. Najhitrejšo rast glede na svojo zgodovino pa je doživela tema interneta stvari, ki je bila do leta 2013 povsem neopazna, od leta 2014 pa je doživela več kot 200-% rast.



Slika 3: Sončni diagram pogostosti ključnih besed avtorjev.
Vir: lasten.

3.1.3 Razvoj tematskih področij

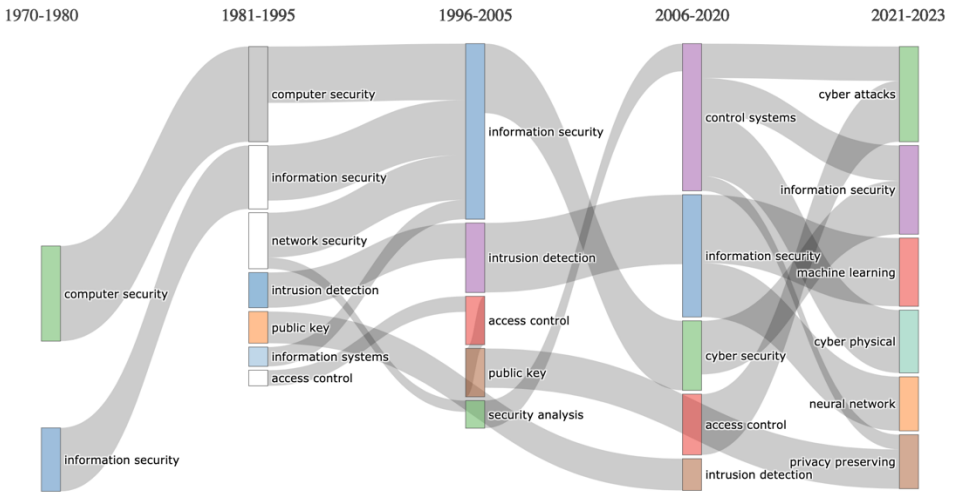
Tematska področja so se z leti razvijala skladno z razvojem tehnologije in pojavom problemov, ki so jih raziskovalci opazili v praksi. Slika 5 prikazuje Sankeyev diagram z razvojem tematskih področij skozi več kot 52-letno obdobje. Analiza temelji na gručenju besednih bigramov (besedne zveze dveh besed) skozi čas iz naslova dokumentov. Posamezna gruča sestoji iz najmanj petih bigramov, obteževanje je bilo opravljeno s Simpsonovim koeficientom (w_{min} = 0.1), število besed v mrežni analizi je n = 250. Vozlišče (posamezni blok) predstavlja temo, višina vozlišča predstavlja velikost gruče (število ključnih besed, ki jih vsebuje gruča), medtem ko višina tokovnega polja predstavlja število ključnih besed, ki povezujejo dve vozlišči (širši pas pomeni višjo relevantnost in boljšo povezavo med dvema gručama (temama)).



Slika 4: Rast števila ključnih besed skozi leta.
Vir: lasten.

Kot je mogoče razbrati z diagrama (slika 5), sta bili v literaturi na začetku pretežno omenjani osnovni temi: informacijska in računalniška varnost. Slednja tema je bila pogostejša in ostaja med najštevilčnejšimi tudi v drugem obdobju med letoma 1981

in 1995, ko se začnejo pojavljati kompleksnejše teme, ki so omogočale obravnavati računalniško in informacijsko varnost podrobneje, najpogosteje z vidika varnosti omrežij, skozi zaznavo vdorov, pogosto pa se pojavljajo tudi asimetrična kriptografija (ang. *public key criptography*) in kontrola dostopa. Prvič se pojavijo tudi informacijski sistemi, ki pa se v naslednjem obdobju (med letoma 1996 in 2005) povežejo z informacijsko varnostjo – največjo gručo v tem obdobju. To gre, skupaj z dejstvom, da je zaznava vdorov bistveno večja od prejšnjega obdobja, pripisati predvsem popularizaciji in dostopnosti interneta. Prav tako se v tem obdobju pogosteje začne raziskovanje kontrole dostopa in asimetrične kriptografije. Prvič se kot svoja tema pojavijo tudi analize varnosti. Informacijska varnost se v naslednjem obdobju (med letoma 2006 in 2020) prelevi v kibernetsko varnost (sicer nekoliko manjšo gručo). V tem obdobju največjo gručo skupaj z informacijsko varnostjo predstavljajo nadzorni sistemi. V zadnjih letih (po 2020) pa se znanost predvsem osredotoča na strojno in globoko učenje, povezano s kibernetskimi napadi in zagotavljanjem zasebnosti. Teme iz gruč v zadnjem obdobju gre pričakovati tudi v prihodnjih nekaj letih.



Slika 5: Sankeyev diagram razvoja tem informacijske varnosti skozi desetletja.
Vir: lasten.

3.1.4 Raziskovalna moč po državah

Pričakovano imajo največjo raziskovalno moč države, ki imajo tudi največ prebivalcev. Tabela 2 prikazuje število objavljenih dokumentov po državah (Število dokumentov), število dokumentov, ki je nastalo z znotrajdržavnim sodelovanjem soavtorjev (SCP), število dokumentov, ki je nastalo z mednarodnim sodelovanjem soavtorjev (MCP), in razmerje med številom objavljenih dokumentov in številom prebivalcev v posamezni državi – relativno število dokumentov (RND). Države so za vsak članek določene glede na državo korespondenčnega avtorja. Tako prednjačijo Kitajska, ZDA in Indija. Med evropskimi državami med prvih deset najbolj plodnih sodijo Združeno kraljestvo, Nemčija in Italija.

Tabela 2: Deset najproduktivnejših držav na področju informacijske, kibernetske in računalniške varnosti.

Država	Število dokumentov	SCP	MCP	RND
Kitajska	13875	11510	2365	9.8e-06
ZDA	12504	10708	1796	3.8e-05
Indija	3327	2919	408	2.4e-06
Združeno Kraljestvo	3044	2146	898	4.5e-05
Japonska	2106	1835	271	1.7e-05
Nemčija	2007	1471	536	2.4e-05
Rusija	1883	1783	100	1.3e-05
Koreja	1854	1499	355	3.6e-05
Avstralija	1780	1242	538	6.9e-05
Italija	1221	900	321	2.1e-05

Tabela 3 prikazuje najbolj produktivne države EU na področju informacijske, kibernetske in računalniške varnosti. Tabela 3 vključuje deset najproduktivnejših in Slovenijo, ki je po absolutnem številu na 19. mestu. Pomembno pa je izpostaviti relativno število dokumentov (RND), tj. razmerje števila objavljenih dokumentov glede na število prebivalcev v posamezni državi. V tem primeru lahko vidimo, da je Slovenija na tretjem mestu v Evropi (za Finsko in Estonijo), razmerje pa ima višje od velike večine vodilnih držav v svetu in se umesti takoj za Avstralijo na drugo mesto. Slovenija ima denimo od Nemčije več kot 250 % višje relativno število objavljenih dokumentov s tega področja.

Tabela 3: Deset najproduktivnejših držav na področju informacijske, kibernetske in računalniške varnosti in Slovenija.

Država	Število dokumentov	SCP	MCP	RND
Nemčija	2007	1471	536	2.4e-05
Italija	1221	900	321	2.1e-05
Francija	1148	845	303	1.7e-05
Španija	992	684	308	2.1e-05
Poljska	564	467	97	1.5e-05
Grčija	552	400	152	5.2e-05
Švedska	506	386	120	4.9e-05
Finska	494	384	110	8.9e-05
Nizozemska	478	334	144	2.7e-05
Belgija	461	295	166	4.0e-05
Slovenija	130	106	24	6.2e-05

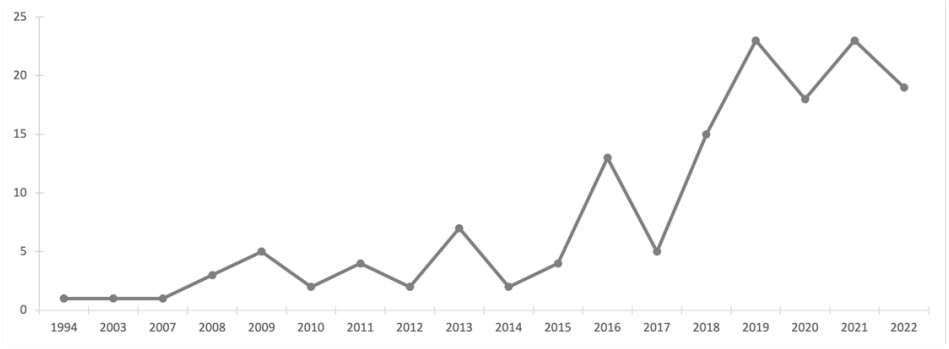
3.2 Razvoj v Sloveniji

Da bi analizirali razvoj informacijske, kibernetske in računalniške varnosti v Sloveniji, smo opravili dodatne analize na dokumentih, ki so bili objavljeni v (so)avtorstvu vsaj enega avtorja, ki je pripadal slovenski (raziskovalni) instituciji. Poizvedba je sledila metodi, ki je bila opisana na začetku poglavja 3. Edina razlika je bila vključevanje zgolj zadetkov iz Slovenije (nastavitev: *Country/Region*). Iskalni niz je na 9. januarja 2023 vrnil 150 zadetkov med letoma 1994 ter 2020, čeprav iskanje časovno ni bilo omejeno. Članki in konferenčni prispevki so bili objavljeni v 116 različnih virih. Tako kot metoda poizvedovanja je bil postopek izvoza in analize enak kot pri poizvedbi, ki ni imela lokacijsko omejenega iskanja. Omeniti velja, da je število iz tega iskalnega niza za 20 dokumentov višje od števila, ki smo ga poročali v podpoglavju *Raziskovalna moč po državah*. Razlika je nastala zaradi drugačnega štetja dokumentov. Pri 150 dokumentih vsaj eden izmed soavtorjev pripada slovenski (raziskovalni) instituciji, medtem ko je izmed 130 dokumentov avtor s slovensko afiliacijo naveden kot korespondenčni avtor.

3.2.1 Rast področja

Rast števila objav področja informacijske, kibernetske in računalniške varnosti smo analizirali skozi število indeksiranih objavljenih dokumentov za vsako leto posebej. Kot prikazuje slika 6, so se vidnejše objave (tj. objave, indeksirane v WoS) začele leta 1994 z raziskavo na področju varnosti računalniških sistemov v podjetjih. Naslednja objava je sledila šele devet let kasneje (2003), tretja pa še štiri leta kasneje, leta 2007.

Višje število objav se je začelo leta 2008 (manj tehnični vidiki informacijske varnosti) in leta 2009 (bolj tehnični vidiki informacijske varnosti), medtem ko se je prvi večji porast zgodil leta 2016, ko je število objav zraslo za 260 % glede na leto 2009, kasneje pa še leta 2019, ko se je število objav povečalo za dodatnih 175 %. Od leta 2019 je število objav relativno stabilno kljub manjšim padcem v letih 2020 in 2022. Padec v letu 2020 gre pripisati predvsem pandemičnim okoliščinam, padec v letu 2022 pa sledi trendu vseh objav, indeksiranih v WoS (slika 1).

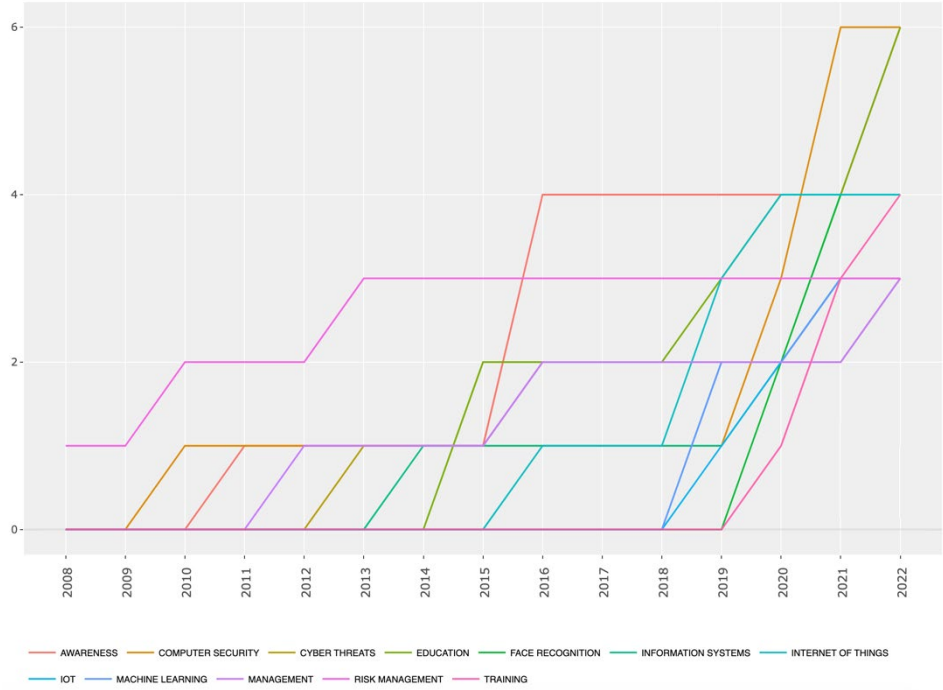


Slika 6: Število objavljenih dokumentov s slovenskimi (so)avtorji skozi leta.
Vir: lasten.

3.2.2 Teme informacijske varnosti v Sloveniji

Slovenija je zaznamovana z nizkim številom prebivalstva, posledično pa tudi absolutnega števila raziskovalcev ter objavljenih dokumentov na področju informacijske varnosti. Tako tudi analiza razvoja ključnih besed skozi časovno obdobje ne vrne informacij o podrobnejših temah, pač pa nudi zgolj splošen oris dinamike tem objavljenih dokumentov. Iz analize so bile izvzete najpogostejše generične ključne besede, ki so bile del iskalnega niza (informacijska varnost in varnost). Slika 7 prikazuje rezultate. Razbrati je mogoče, da so slovenski raziskovalci sledili trendu tujine, saj med najpogostejšimi ključnimi besedami zasledimo strojno učenje, internet stvari (tako v obliki celotne besedne zveze kot tudi akronimu). Med najdlje aktualnimi temami sta management in upravljanje s tveganji, ki sta med pomembnejšimi že od leta 2008 oz. leta 2011. Podobno velja tudi za informacijskovarnostno ozaveščenost, ki se je pogosteje začela pojavljati po letu 2010. Zadnji najbolj aktualni temi na tem področju, ki sta svojo rast začeli po letu

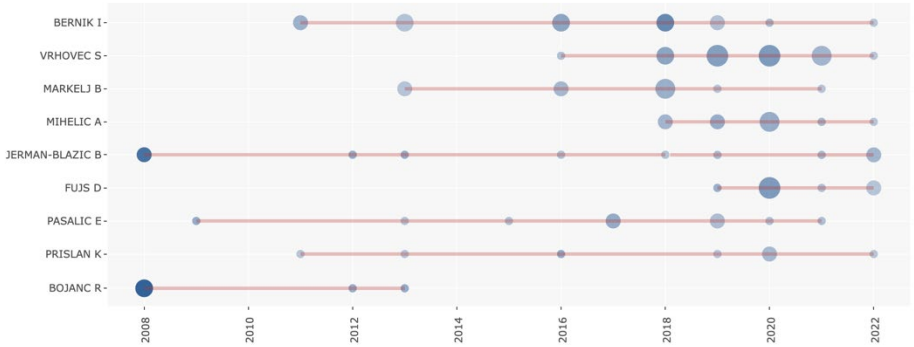
2018, sta prepoznava obrazov in informacijskovarnostno izobraževanje in usposabljanje.



Slika 7: Rast števila ključnih besed skozi leta.
Vir: lasten.

3.2.3 Vpliv avtorjev in institucij

Da bi ugotovili, katere institucije in njim pripadajoči avtorji so najbolj zaznamovali slovensko raziskovalno dejavnost s področja informacijske, kibernetske in računalniške varnosti, smo analizirali število prispevkov, ki so jih posamezni avtorji objavili skozi leta in katerim institucijam so pripadali. Slika 8 prikazuje rezultate, kjer so avtorji razvrščeni po številu objavljenih dokumentov padajoče. Slika prikazuje najproduktivnejše izmed 427 (so)avtorjev. Najdlje je v slovenskem prostoru dejavna *Borka Jerman-Blažič* (2008–2022), medtem ko ji sledita *Igor Bernik* in *Kaja Prislan* (2011–2022) kot druga dva najdlje dejavna slovenska avtorja z obravnavanega področja.



Slika 8: Časovnica dejavnosti najbolj produktivnih avtorjev v Sloveniji (avtorji so razvrščeni padajoče po številu objavljenih dokumentov).
Vir: lasten.

Izmed 129 sodelujočih institucij med najproduktivnejših pet umeščamo *Fakulteto za varnostne vede* (Univerza v Mariboru), ki je s skupno 45 dokumenti najvišje uvrščena institucija. Sledijo ji *Institut »Jožef Štefan«* s 35 dokumenti, *Fakulteta za računalništvo in informatiko* (Univerza v Ljubljani) s 14 dokumenti, *Fakulteta za elektrotehniko, računalništvo in informatiko* (Univerza v Mariboru) s 13 objavljenimi dokumenti ter *Fakulteta za elektrotehniko* (Univerza v Ljubljani) z 8 objavljenimi dokumenti.

3.3 Razvoj na Fakulteti za varnostne vede Univerze v Mariboru

Kot je pokazal pregled znanstvenoraziskovalne dejavnosti s področja informacijske varnosti v Sloveniji, Fakulteta za varnostne vede Univerze v Mariboru (UM FVV) predstavlja vodilno raziskovalno institucijo z najobsežnejšim opusom pomembnejših znanstvenih publikacij, za kar je zaslužna predvsem Katedra za informacijo varnost (KIV). Razvoj raziskovalne dejavnosti na UM FVV je potekal ob boku razvoja organizacijske strukture in študijskih programov. Šele leta 2003 je namreč postala polnopravna članica Univerze v Mariboru (UM) in se takrat tudi preimenovala iz Visoke policijsko-varnostne šole v Fakulteto za policijsko-varnostne vede, ki se je leta 2006 preimenovala v Fakulteto za varnostne vede. V prvem desetletju enaindvajsetega stoletja so se sicer že poučevale določene vsebine in predmeti o informacijski varnosti v okviru univerzitetnega programa in specializacije, intenzivnejši razvoj predmetnika, povezanega z informacijsko varnostjo, pa se je začel po letu 2007 z bolonjsko reformo.

V drugem desetletju sledi akreditacija novega visokošolskega študijskega programa Informacijska varnost (2010) in uvedba modula informacijska varnost na magistrskem študijskem programu (2017). Od leta 2010 katedra beleži tudi postopno povečevanje števila raziskovalcev, z novimi zaposlitvami v letih 2011, 2014 in 2019. Vidnejša znanstvenoraziskovalna dejavnost članov in sodelavcev KIV (raziskovalne šifre: 16312; 33190; 34047; 38302; 52374) se začne z letom 2010 po ustanovitvi katedre in ob zagonu študijskega programa. Raziskovanje se je sprva pretežno osredotočalo na splošnejše tematike, kot so kibernetske grožnje, kibernetska kriminaliteta, naprednejše grožnje (kibernetski terorizem, informacijsko bojevanje), upravljanje s tveganji, mednarodni standardi in informacijska varnost v povezavi z mobilnimi napravami. V prvih letih je prevladovalo predvsem publiciranje konferenčnih znanstvenih prispevkov, v drugem desetletju pa se zgodi vidnejši porast publiciranja v znanstvenih revijah in večja osredotočenost oz. specifikacija raziskovalnih tematik.

KIV je od leta 2010 do januarja 2023 skupaj objavila 58 izvirnih znanstvenih prispevkov (od tega 9 izjemnih (A") in 8 pomembnih znanstvenih del (A' in A1/2), 10 preglednih znanstvenih prispevkov (tip 1.02), tri kratke znanstvene prispevke, 46 znanstvenih prispevkov na konferencah in 18 poglavij v znanstvenih monografijah. Z zaposlovanjem novih raziskovalcev se je število objav po letih smiselno povečevalo. Če sta se v obdobju od leta 2010 do leta 2014 v povprečju objavila dva izvirna znanstvena prispevka letno, je povprečje v obdobju od leta 2015 do leta 2018 naraslo na šest in v tretjem obdobju od leta 2019 do leta 2022 na osem izvirnih znanstvenih prispevkov letno. Pomembnejše objave (A", A' in A1/2) člani in sodelavci katedre KIV beležijo predvsem v drugih dveh navedenih obdobjih. V letu 2022 so izmed vseh izvirnih znanstvenih člankov, objavljenih pod afiliacijo UM FVV, raziskovalci KIV objavili 29,4 % prispevkov. V svojih objavah so se osredotočali na proučevanje naslednjih tem: varnostni izzivi in vidiki razvoja programske opreme (Mihelič idr., 2023; Vrhovec idr., 2015a; Vrhovec idr., 2015b; Vrhovec in Markelj, 2021); varnost mobilnih naprav v organizacijskem okolju (Markelj in Završnik, 2016); merjenje in ocenjevanje kakovosti informacijske varnosti (Bernik in Prislan, 2016; Prislan idr., 2020); zaznave kibernetskih groženj med uporabniki in viktimizacija s kibernetsko kriminaliteto (Bernik idr., 2022; Markelj in Zgaga, 2016); notranje grožnje v informacijski varnosti (Choi idr., 2018); motivacija in namera za zaščito ter iskanje informacij (Vrhovec idr., 2023; Vrhovec in Mihelič, 2021); uporaba storitev spletnih omrežij in konferenčnih okolij za

izobraževanje na daljavo (Fujs idr., 2022; Fujs in Vrhovec, 2020); kategorizacija uporabnikov na podlagi dejavnikov informacijske varnosti (Fujs idr., 2021); uporaba zunanjega izvajanja storitev v informacijski varnosti (Jelovčan idr., 2022); uporaba pametnih naprav in informacijska varnost med starejšimi uporabniki (Mihelič in Žvanut, 2022).

V ostalih izvirnih znanstvenih prispevkih pa so raziskovalci KIV obravnavali in raziskovali tudi druge teme, povezane z informacijsko in kibernetsko varnostjo, denimo: upravljanje informacijskovarnostnih tveganj; informacijskovarnostni standardi, ozaveščenost in strah pred kibernetsko kriminaliteto; usposabljanja in treningi uporabnikov; socioekonomski vidiki informacijske varnosti in kibernetske kriminalitete; kazenskopravni pogledi na kršitve pravil informacijske varnosti; informacijska varnost v zdravstvenem sistemu in kritični infrastrukturi; kibernetska varnost in kriminaliteta, povezana s pametnimi napravami, pametnimi avtomobili in pametnimi mesti; varstvo osebnih podatkov in zasebnost; adopcija tehnologije in s tem povezani motivacijski in zaviralni dejavniki.

Iz predstavljenih tem je razvidno, da se raziskave pogosto nanašajo na kompleksne tematike, ki zahtevajo multidisciplinarno obravnavo, kar se odraža v značilnostih skupin avtorjev. KIV v objavah beleži sodelovanje ne le z obema preostalima univerzama v Sloveniji in tehničnimi ter zdravstvenimi fakultetami, temveč tudi z bogato mrežo tujih raziskovalnih institucij (iz Nemčije, Avstrije, Velike Britanije in Italije). Omeniti velja še, da so se raziskave neredko izvajale v realnih okoljih, posledično pa so kot soavtorji prispevkov pogosto vključeni strokovnjaki iz prakse (npr. s področja varnostnega svetovanja, revizije informacijskih sistemov, korporativne varnosti, kritične infrastrukture, analitike).

Svoja znanja, izkušnje in izsledke raziskovalne dejavnosti so s ciljem celostne predstavitve obravnavanih problematik raziskovalci KIV publicirali tudi v zaokroženih znanstvenih monografijah, izdanih pri nacionalnih in mednarodnih založbah. V zadnjem desetletju je bilo objavljenih pet samostojnih znanstvenih monografij, ki v kontekstu informacijske varnosti predstavljajo vidike, povezane z etičnim hekanjem (Tomše in Markelj, 2020), upravljanjem v organizacijah (Prislan in Bernik, 2019); mobilnimi napravami (Markelj in Bernik, 2020); kibernetsko kriminaliteto, informacijskim bojevanjem in kibernetskim terorizmom (Bernik, 2014; Bernik in Prislan, 2012).

4 Zaključek

Pričujoči prispevek predstavlja vpogled v zgodovinski razvoj informacijske, računalniške in kibernetske varnosti skozi stroko in raziskovalno dejavnost. Zametki informacijske varnosti imajo korenine že v daljni zgodovini človeške družbe, močnejše zametke razvoja področja kot discipline pa je opaziti v devetnajstem stoletju z razvojem računalniške discipline, bolj poglobljeno in intenzivno pa v dvajsetem stoletju z zasnovami modernih računalnikov in pojavom telekomunikacij. Na začetku se je informacijska varnost razvijala v okvirih računalništva, z razvojem omrežij, predvsem interneta in osebnih računalnikov pa v ospredje pride tudi potreba po varnosti omrežij in informacijskih sistemov. Informacijska varnost doživi razmah konec devetdesetih let in z novim tisočletjem začne razvijati svojo sodobno podobo, kot jo poznamo danes. V zadnjih desetletjih je poudarek predvsem na uporabniški in kibernetski varnosti ter izzivih, povezanih z razvojem profesionalizacije, razvojem inteligentnih rešitev in preprečevanjem oz. odzivanjem na kibernetske grožnje, pomembne za nacionalno in mednarodno varnost.

V Sloveniji se je vidnejša raziskovalna dejavnost na področju informacijske varnosti začela sredi devetdesetih let dvajsetega stoletja, medtem ko je svoj nagli vzpon doživela po letu 2005. S povečanjem števila raziskovalcev na tem področju se je pričakovano povečalo tudi število raziskav, tudi tistih, ki so objavljene v najvišje uvrščenih revijah. UM FVV je kot prva znanstvenoizobraževalna institucija vzpostavila akreditiran program s področja informacijske varnosti. Zaradi manka kadra, krepitve ustreznih kompetenc in potreb razvoja profesionalizacije na tem področju se vsebine vse pogosteje uvajajo tudi v druge visokošolske izobraževalne programe ter izobraževanja na drugih stopnjah.

Bralec mora biti pri interpretaciji predstavljenih rezultatov pozoren na naslednje omejitve raziskave. Prvič, ugotovitve izhajajo zgolj iz zbirke WoS in ne upoštevajo dokumentov, ki niso indeksirani v tej bibliografski zbirki. Tako obstaja verjetnost, da nekateri dokumenti (predvsem poglavje 3.2) niso vključeni v analizo. Kljub temu avtorja verjameva, da analiza najodmevnejših objavljenih raziskav (tj. raziskav, objavljenih v virih, ki so indeksirani v WoS) predstavlja zanesljiv in kakovosten vpogled v razvoj področja. Drugič, analiza dokumentov (rezultati v podpoglavjih 3.1 in 3.2) je bila opravljena zgolj kvantitativno. Kvalitativna analiza bi omogočila

podrobnejši vpogled v vsebine, ki so se obravnavale skozi čas in s tem natančnejši pregled razvoja posameznih tem znotraj področja.

Literatura

Anderson, J. P. (1972a). *Computer security technology planning study, ESD-TR-73-51, Vol. I.* Electronic System Division. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf

Anderson, J. P. (1972b). *Computer security technology planning study, ESD-TR-73-51, Vol. II.* Electronic System Division. https://csrc.nist.rip/publications/history/ande72.pdf

Anderson, R. in Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *367*(1898), 2717–2727. https://doi.org/10.1098/rsta.2009.0027

Bernik, I. (2014). *Cybercrime and cyberwarfare*. Wiley.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Fakulteta za varnostne vede.

Bernik, I. in Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE*, *11*(9), 1–33. https://doi.org/10.1371/journal.pone.0163050

Bernik, I., Prislan, K. in Mihelič, A. (2022). Country life in the digital era: Comparison of technology use and cybercrime victimization between residents of rural and urban environments in Slovenia. *Sustainability*, *14*(21). https://doi.org/10.3390/su142114487

Bisbey, R. in Hollingworth, R. (1978). *Protection analysis: Final report. ARPA order NO. 2223.* Information Sciences Institute, University of Southern Carolina. https://csrc.nist.rip/publications/history/bisb78.pdf

Chadd, K. (2020). The history of cybercrime and cybersecurity, 1940-2020. *Cybercrime Magazine.* https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

Choi, S., Martins, J. T. in Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752–767. https://doi.org/10.1177/0165551517748288

de Leeuw, K. (2007). Introduction. V K. de Leeuw in J. Bergstra (ur.), *The history of information security: A comprehensive handbook* (str. 1–25). Elsevier B.V.

Fujs, D. in Vrhovec, S. (2020). Use of social networking services among Slovenes around the world. *Dve domovini*, 52. https://doi.org/10.3986/dd.2020.2.04

Fujs, D., Vrhovec, S. in Vavpotič, D. (2021). Know your enemy: User segmentation based on human aspects of information security. *IEEE Access*, *9*, 157306–157315. https://doi.org/10.1109/ACCESS.2021.3130013

Fujs, D., Vrhovec, S., Žvanut, B. in Vavpotič, D. (2022). Improving the efficiency of remote conference tool use for distance learning in higher education: A kano based approach. *Computers & Education*, *181*, 104448. https://doi.org/10.1016/j.compedu.2022.104448

Ibrahimova, A. N. (2020). The defintions of information and security; history of information security development. *Vilnius University Open Series*, *6*, 48–57. https://doi.org/10.15388/os.law.2020.5

Jelovčan, L., Mihelič, A. in Prislan, K. (2022). Outsource or not? An AHP based decision model for information security management. *Organizacija*, *55*(2). https://doi.org/10.2478/orga-2022-0010

Kessler, G. C. (2012). Information security: New threats or familiar problems? *Computer*, *45*(2), 59–65. https://doi.org/10.1109/mc.2011.262

Svet Evrope. (2001). *Konvencija o kibernetski kriminaliteti.* http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/185/

List, W. (1973). Too many loopholes in computer security. *Cost and Management*, *47*.
Markelj, B. in Bernik, I. (2020). *Varnost mobilnih naprav*. Univerzitetna založba Univerze v Mariboru. https://press.um.si/index.php/ump/catalog/book/315
Markelj, B. in Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: Zavedanje uporabnikov v Sloveniji. *Revija za kriminalistiko in kriminologijo*, *67*(1), 44–60.
Markelj, B. in Zgaga, S. (2016). Comprehension of cyber threats and their consequences in Slovenia. *Computer Law & Security Review*, *32*(3), 513–525. https://doi.org/10.1016/j.clsr.2016.01.006
Mihelič, A., Vrhovec, S. in Hovelja, T. (2023). Agile Development of secure software for small and medium-sized enterprises. *Sustainability*, *15*(1). https://doi.org/10.3390/su15010801
Mihelič, A. in Žvanut, B. (2022). (In)secure Smart device use among senior citizens. *IEEE Security & Privacy*, *20*(1), 62–71. https://doi.org/10.1109/MSEC.2021.3113726
Prislan, K. in Bernik, I. (2019). *Informacijska varnost in organizacije*. Univerzitetna založba Univerze v Mariboru.
Prislan, K., Mihelič, A. in Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, *15*(9 September), 1–28. https://doi.org/10.1371/journal.pone.0238739
Scheidermayer, P. (1970). Many aspects of computer security. *Police Chief*, *37*(7), 64–67.
Tomše, S. in Markelj, B. (2020). *Informacijska varnost: Etično hekanje* (1. natis). GV Založba.
von Solms, B. (2010). The 5 Waves of information security – from Kristian Beckman to the present. V K. Rannenberg, V. Varadharajan in C. Weber (ur.), *Security and Privacy – silver linings in the cloud* (str. 1–8). Springer.
Vrhovec, S., Bernik, I. in Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*, 103038. https://doi.org/10.1016/j.cose.2022.103038
Vrhovec, S. L. R., Hovelja, T., Vavpotič, D. in Krisper, M. (2015a). Diagnosing organizational risks in software projects: Stakeholder resistance. *International Journal of Project Management*, *33*(6), 1262–1273. https://doi.org/10.1016/j.ijproman.2015.03.007
Vrhovec, S. L. R., Trkman, M., Kumer, A., Krisper, M. in Vavpotič, D. (2015b). Outsourcing as an Economic development tool in transition economies: Scattered global software development. *Information Technology for Development*, *21*(3), 445–459. https://doi.org/10.1080/02681102.2013.874316
Vrhovec, S. in Markelj, B. (2021). The relation between project team conflict and user resistance in software projects. *PLOS ONE*, *16*(11), e0260059. https://doi.org/10.1371/journal.pone.0260059
Vrhovec, S. in Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309. https://doi.org/10.1016/j.cose.2021.102309
Ware, W. H. (1979). *Security controls for computer systems. Report of defense science board Task force on computer security. R-609-1*. RAND. https://www.rand.org/pubs/reports/R609-1.html
Whitman, M. E. in Mattord, H. J. (2012). *Principles of information security* (4th ed). Course Technology.